



БИБЛИОТЕКА ЦЕНТРА ИССЛЕДОВАНИЙ ПЛАТЕЖНЫХ СИСТЕМ И РАСЧЕТОВ

НАЦИОНАЛЬНАЯ ПЛАТЕЖНАЯ СИСТЕМА



КНОРУС • МОСКВА • 2013

KnorusMedia
электронные версии книг

УДК 336.71
ББК 65.262.1
Н48

Авторский коллектив:

В.В. Адрианов, М.Я. Букирь, С.А. Бутенко, В.Б. Голованов, Д.Д. Давыдов, С.П. Карчевский, В.Ю. Копыгин, С.Б. Кузнецов, А.П. Курило, В.А. Лопатин, А.В. Пайкин, А.В. Пухов, А.Г. Сабанов, Е.В. Синельникова-Мурылева, К.Т. Сумманен, П.В. Трунин, М.И. Чапанов

Редактор-составитель А.С. Воронин

Национальная платежная система. Бизнес-энциклопедия / коллектив
Н48 авторов ; ред.-сост. А.С. Воронин. — М. : КНОРУС : ЦИПСИР, 2013. — 424 с.
ISBN 978-5-406-02526-0

Методология строительства и организации функционирования платежных систем национального масштаба на основе мирового опыта, особенности функционирования SWIFT в России, описание и опыт международных карточных систем, платежная система Банка России и коммерческих банков, расчеты на рынке ценных бумаг, комментарии специалистов к Федеральному закону «О национальной платежной системе» и многие другие темы — все это есть в предлагаемой бизнес-энциклопедии «Национальная платежная система».

Книга ориентирована на специалистов, работающих в различных сферах, — сотрудников банков, платежных систем, специалистов по ценным бумагам, сотрудников процессинговых центров, а также на всех, кто интересуется тематикой функционирования платежных систем в мире и в России. Авторский коллектив книги — специалисты-практики: сотрудники коммерческих банков, других коммерческих структур — участников платежного рынка, государственных регулирующих органов, российских и мировых платежных систем, финансовых институтов.

УДК 336.71
ББК 65.262.1

НАЦИОНАЛЬНАЯ ПЛАТЕЖНАЯ СИСТЕМА
Бизнес-энциклопедия

Изд. № 5160. Подписано в печать 23.07.2012. Формат 70 90/16.
Гарнитура «BalticaС». Печать офсетная.

Усл. печ. л. 26,5. Уч.-изд. л. 16,5. Тираж 1500 экз. Заказ №

ООО «Центр Исследований Платежных Систем и Расчетов».

E-mail: info@paysyscenter.ru <http://www.paysyscenter.ru>

ООО «КноРус».

129085, Москва, проспект Мира, д. 105, стр. 1.

Тел.: (495) 741-46-28.

E-mail: office@knorus.ru <http://www.knorus.ru>

Отпечатано в полном соответствии с качеством
предоставленного издательством электронного оригинал-макета
в ГУП «Брянское областное полиграфическое объединение».

241019, г. Брянск, пр-т Ст. Димитрова, 40.

© ООО «Центр Исследований
Платежных Систем и Расчетов», 2013
© ООО «КноРус», 2013

ISBN 978-5-406-02526-0

ОГЛАВЛЕНИЕ

| | |
|--|------------|
| Предисловие | 5 |
| Глава 1. Банк международных расчетов о национальных платежных системах | 7 |
| 1.1. Банк международных расчетов. Европейские международные финансовые институты | 8 |
| 1.2. Понятие и структура национальной платежной системы | 11 |
| 1.3. Развитие национальных платежных систем | 20 |
| 1.4. Платежные системы для крупных сумм | 39 |
| 1.5. Розничные платежные системы | 47 |
| Глава 2. Национальные платежные системы и SWIFT | 56 |
| 2.1. Использование SWIFT в национальных платежных системах | 56 |
| 2.2. Стандарты SWIFT | 59 |
| 2.3. Использование SWIFT в России | 61 |
| 2.4. Организационная структура российских пользователей SWIFT — РОССВИФТ | 62 |
| 2.5. Осуществление платежей и расчетов в рублях с использованием SWIFT. | 64 |
| 2.6. Доступ корпораций в SWIFT | 65 |
| 2.7. Коллективное подключение к SWIFT. | 67 |
| Глава 3. Национальные платежные системы и международные карточные платежные системы | 69 |
| 3.1. Международные карточные платежные системы. | 69 |
| 3.2. Интеграция МПС и НПС | 91 |
| Глава 4. Платежные и расчетные системы Российской Федерации | 103 |
| 4.1. Банковская система Российской Федерации | 103 |
| 4.2. Платежи и расчеты в Российской Федерации | 106 |
| 4.3. Денежные переводы и платежные агенты | 109 |
| 4.4. Платежная система Банка России. | 111 |
| 4.5. Частные платежные системы. | 114 |
| 4.6. Платежная система Сбербанка России | 118 |
| 4.7. Платежная система Федерального казначейства | 123 |
| 4.8. Платежная система Почты России | 125 |
| Глава 5. Платежные инструменты и технологии | 128 |
| 5.1. Денежные средства и платежные инструменты | 128 |
| 5.2. Наличные деньги | 130 |
| 5.3. Расчетные документы | 136 |
| 5.4. Платежные карты | 142 |
| 5.5. Электронные деньги | 146 |
| 5.6. Мобильные платежные технологии. | 151 |
| Глава 6. Расчетная система организованного рынка ценных бумаг | 157 |
| 6.1. Понятие и структура ОРЦБ. | 158 |
| 6.2. Правовое положение расчетного центра ОРЦБ | 164 |
| 6.3. Ограничение рисков в деятельности РЦ ОРЦБ | 167 |

| | |
|--|------------|
| 6.4. Правовое положение участника РЦ ОРЦБ | 168 |
| 6.5. Структура договорных отношений на ОРЦБ | 171 |
| 6.6. Виды банковских и внутрибанковских счетов, используемых в расчетах на ОРЦБ, и их режимы | 174 |
| 6.7. Внутрибанковские счета | 178 |
| 6.8. Торговые и клиринговые банковские счета | 179 |
| 6.9. Особенности проведения расчетов на рынке государственных ценных бумаг. | 182 |
| 6.10. Организация расчетов на фондовом рынке. | 185 |
| 6.11. Участие РЦ ОРЦБ в проведении расчетов на валютном рынке | 191 |
| 6.12. Перспективы построения платежной системы, предусматривающей переводы денежных средств по сделкам, совершенным на организованных торгах | 193 |
| Глава 7. Электронные деньги и мобильные платежи — методология использования внутри коммерческого банка | 195 |
| 7.1. Порядок деятельности оператора электронных денежных средств | 196 |
| 7.2. Порядок предоставления клиентам ЭСП и осуществления перевода | 197 |
| 7.3. Противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма | 202 |
| Глава 8. Безопасность и надежность функционирования платежных технологий | 211 |
| 8.1. Парадигма информационной безопасности для национальной платежной системы. | 211 |
| 8.2. Принципы обеспечения информационной безопасности национальной платежной системы. | 229 |
| 8.3. Модельные решения и стандарты обеспечения информационной безопасности | 238 |
| 8.4. Организационная основа безопасности и надежности НПС | 268 |
| Глава 9. Технологии аутентификации для обеспечения безопасности платежей | 271 |
| 9.1. Вопросы идентификации и аутентификации. | 273 |
| 9.2. Перспективные решения. Мобильный банкинг | 280 |
| Глава 10. Закон о НПС: структура и комментарии | 287 |
| 10.1. Что представляет собой НПС с точки зрения Закона | 287 |
| 10.2. Комментарии к статьям Закона об НПС. | 301 |
| Глава 11. Развитие национальной платежной системы в долгосрочной перспективе | 323 |
| 11.1. Тенденции развития и современное состояние НПС. | 323 |
| 11.2. Дизайн и функциональность НПС | 324 |
| 11.3. Архитектура НПС. | 330 |
| 11.4. О средствах дистанционного доступа к сервисам | 332 |
| 11.5. Национальная система электронных взаимодействий. | 337 |
| 11.6. Национальная инвойсинговая система (НИС) | 340 |
| 11.7. Национальная система розничных платежей | 346 |
| Глава 12. Эволюция правового обеспечения применения инновационных технологий в российской НПС | 357 |
| Приложение. ФЗ от 27.06.2011. № 161-ФЗ «О национальной платежной системе» | 363 |

ПРЕДИСЛОВИЕ

Бизнес-энциклопедия «Национальная платежная система» ориентирована на специалистов, работающих в различных сферах, — сотрудников банков, платежных систем, специалистов по ценным бумагам, сотрудников процессинговых центров, а также на всех, кто интересуется тематикой функционирования платежных систем в мире и в России. Авторский коллектив книги — специалисты-практики: сотрудники коммерческих банков, других коммерческих структур — участников платежного рынка, государственных регулирующих органов, российских и мировых платежных систем, финансовых институтов. Методологии строительства и организации эффективного функционирования платежных систем национального масштаба на основе мирового опыта, особенности функционирования SWIFT в России, описание и опыт международных карточных систем, платежная система Банка России и коммерческих банков, расчеты на рынке ценных бумаг, комментарии специалистов к Федеральному закону от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» и многие другие темы — все это есть в настоящем издании. Авторский коллектив книги рассчитывает, что книга будет интересна и полезна не только действующим специалистам, но и более широкому кругу читателей, интересующихся проблематикой функционирования платежных систем, в том числе студентам вузов. Бизнес-энциклопедия «Национальная платежная система» — редкое по широте охвата темы, глубине подачи материала, профессиональности подхода ко всем рассматриваемым вопросам издание.

Мы представляем читателям авторский коллектив бизнес-энциклопедии «Национальная платежная система» с указанием тех глав книги, которые написаны каждым из авторов (некоторые главы написаны в соавторстве, о чем указывается дополнительно).

Адрианов В.В. (ООО «Научно-производственная фирма „Кристалл“») — «Безопасность и надежность функционирования платежных технологий» (в соавторстве с В.Б. Головановым и А.П. Курило);

Букирь М.Я. (ООО «Банкир.Ру») — «Закон о НПС: структура и комментарии» (в соавторстве с С.А. Бутенко);

Бутенко С.А. (Платежная система «КредитПилот») — «Закон о НПС: структура и комментарии» (в соавторстве с М.Я. Букирь);

Голованов В.Б. (ООО «Научно-производственная фирма „Кристалл“») — «Безопасность и надежность функционирования платежных технологий» (в соавторстве с В.В. Адриановым и А.П. Курило);

Давыдов Д.Д. (РОССВИФТ) — «Национальные платежные системы и SWIFT» (в соавторстве с С.Б. Кузнецовым);

Карчевский С.П. (НКО ЗАО «Национальный расчетный депозитарий») — «Расчетная система организованного рынка ценных бумаг» (в соавторстве с А.В. Пайкиным);

Копытин В.Ю. (ГУ Банка России по Ростовской области, Южный федеральный университет) — «Платежные и расчетные системы Российской Федерации», «Платежные инструменты и технологии»;

Кузнецов С.Б. (РОССВИФТ) — «Национальные платежные системы и SWIFT» (в соавторстве с Д.Д. Давыдовым);

Курило А.П. (Банк России) — «Безопасность и надежность функционирования платежных технологий» (в соавторстве с В.В. Адриановым и В.Б. Головановым);

Лопатин В.А. (ВЭБ) — «Банк международных расчетов о национальных платежных системах»;

Пайкин А.В. (НКО ЗАО „Национальный расчетный депозитарий“) — «Расчетная система организованного рынка ценных бумаг» (в соавторстве с С.П. Карчевским);

Пухов А.В. (Банк) — «Электронные деньги и мобильные платежи — методология использования внутри коммерческого банка»;

Сабанов А.Г. (ЗАО «Аладдин Р.Д.») — «Технологии аутентификации для обеспечения безопасности платежей»;

Синельникова-Мурылева Е.В. («Институт экономической политики им. Е.Т. Гайдара») — «Национальные платежные системы и международные карточные платежные системы» (в соавторстве с П.В. Труниным);

Сумманен К.Т. (ОАО «Банк ВТБ») — «Развитие национальной платежной системы в долгосрочной перспективе»;

Трунин П.В. («Институт экономической политики им. Е.Т. Гайдара») — «Национальные платежные системы и международные карточные платежные системы» (в соавторстве с Е.В. Синельниковой-Мурылевой);

Чапанов М.И. (Аппарат Комитета ГД РФ по финансовому рынку) — «Эволюция правового обеспечения применения инновационных технологий в российской НПС».

В целях удобства читателей книги в приложении размещен текст ФЗ от 27.06.2011. № 161-ФЗ «О национальной платежной системе».

ГЛАВА 1

БАНК МЕЖДУНАРОДНЫХ РАСЧЕТОВ О НАЦИОНАЛЬНЫХ ПЛАТЕЖНЫХ СИСТЕМАХ

Национальная платежная система (НПС) является неотъемлемой частью финансовой системы любого государства. В соответствии со своим названием НПС обеспечивает осуществление платежей, создавая условия для оборота денежных средств, управления денежной массой, регулирования курса национальной валюты, осуществления инвестиционных программ и т.д. В конечном счете эффективная НПС способствует экономическому росту и процветанию национальной экономической системы.

В то же время практика построения и развития национальных платежных систем отличается от государства к государству, находясь в сильной зависимости от множества национальных факторов, включая уровень экономического развития, культурные и правовые традиции, уровень образования и многое другое. Как результат, национальные платежные системы отличаются по платежной структуре, по качеству и количеству платежных услуг, по степени интеграции и т.д.

Такие различия мешают развитию экономических отношений между странами, создавая разнообразные преграды на пути денежных потоков в виде несовместимых правил осуществления трансграничных переводов, правил возмещения убытков, стандартов передачи сообщений, интерфейсов технических устройств и т.д.

Чтобы повысить уровень взаимодействия между национальными платежными системами, на международном уровне предпринимается большое количество усилий в области унификации и стандартизации элементов платежных систем, в том числе путем выявления и распространение среди заинтересованных государств наиболее эффективных институциональных и инфраструктурных решений.

Наиболее активно такие усилия предпринимают Банк международных расчетов¹, Европейский центральный банк², Всемирный банк³ и Международный валютный фонд⁴.

¹ Bank for International Settlements (BIS), www.bis.org

² European Central Bank (ECB), www.ecb.int

³ World Bank (WB), www.worldbank.org

⁴ International Monetary Fund (IMF), www.imf.org

В данной главе обсуждаются вопросы построения и развития национальных платежных систем, в том числе отдельных элементов этих систем, которые отражены в документах Комитета по платежным и расчетным системам Банка международных расчетов, который был создан специально для организации взаимодействия национальных центральных банков по вопросам национальных платежных систем и является, по-видимому, наиболее авторитетным международным институтом по вопросам национальных платежных систем.

1.1. БАНК МЕЖДУНАРОДНЫХ РАСЧЕТОВ. ЕВРОПЕЙСКИЕ МЕЖДУНАРОДНЫЕ ФИНАНСОВЫЕ ИНСТИТУТЫ

Банк международных расчетов (БМР) является старейшим международным финансовым институтом, главной задачей которого является обеспечение взаимодействия национальных центральных банков по основным направлениям финансовой и денежной политики.

БМР был создан в 1930 г. на основе межправительственного соглашения шести государств (Бельгии, Великобритании, Германии, Италии, Франции, Японии) и конвенции этих государств со Швейцарией, на территории которой функционирует Банк. Он был учрежден в связи с необходимостью сбора, администрирования и распределения выплат Германии по Версальскому договору в рамках второго репарационного плана (плана Янга), что и определило название банка.

БМР начал работу в мае 1930 г. в Базеле, Швейцария. Банк имеет структуру акционерной компании, хотя не является субъектом швейцарского кредитного законодательства и учрежден как международная организация, деятельность которой регулируется международным правом.

До 2001 года 13,73% капитала БМР принадлежали не центральным банкам, а частным акционерам, но последние не имели права голоса. В сентябре 2000 г. Совет директоров БМР принял решение об изменении устава банка и выкупе акций у частных акционеров. С этого момента только центральные банки могут быть владельцами акций БМР.

До 90-х годов прошлого века в БМР было сильно влияние стран Западной Европы, что вызывало недовольство других государств. В связи с этим в сентябре 1996 г. было принято решение о расширении представительства центральных банков и приеме новых стран — членов БМР. В частности, в 1996 г. в члены БМР был принят Центральный банк Российской Федерации (Банк России) (далее — ЦБ РФ, Банк России). На сегодняшний день членами БМР являются центральные банки 56 государств¹.

¹ 81st Annual Report. 1 April 2010 — 31 March 2011. BIS, 26 June 2011.

ДЕЯТЕЛЬНОСТЬ БАНКА МЕЖДУНАРОДНЫХ РАСЧЕТОВ

Сегодня деятельность БМР сосредоточена в области сотрудничества центральных банков и других заинтересованных институтов по вопросам обеспечения финансовой и денежной стабильности. БМР организует регулярные встречи руководителей и экспертов центральных банков (с привлечением экспертов из других организаций), проводит исследования в области денежных и финансовых вопросов экономики, собирает, сводит в единые отчеты и распространяет среди центральных банков статистические данные по основным направлениям финансовой и денежной политики.

Наряду с организацией сотрудничества БМР выполняет традиционные банковские функции, регулярно осуществляя банковские операции по поручению центральных банков, а также агентские функции и функции доверительного собственника, кроме того, предоставляет или организует предоставление финансирования в целях поддержки международной финансовой системы.

В рамках БМР функционирует ряд комитетов, в том числе Базельский комитет по банковскому надзору BCBS (Basel Committee on Banking Supervision), Комитет по глобальным финансовым системам CGFS (Committee on the Global Financial System), Комитет по платежным и расчетным системам CPSS (Committee on Payment and Settlement Systems), Комитет Ирвинга Фишера IFC (Irving Fisher Committee) и Институт финансовой стабильности FSI (Financial Stability Institute).

КОМИТЕТ ПО ПЛАТЕЖНЫМ И РАСЧЕТНЫМ СИСТЕМАМ

Основные компетенции БМР в части НПС сосредоточены в Комитете по платежным и расчетным системам (КПРС), который является одной из наиболее авторитетных структур в своей области. КПРС ведет огромную работу по изучению и обобщению практики построения, развития и интеграции НПС в целом, а также отдельных институциональных и инфраструктурных элементов.

КПРС был создан в 1990 г. главами банков из группы десяти G10 (Group of Ten)¹ с целью продолжения и расширения деятельности Группы экспертов по платежным системам GEPS (Group of Experts on Payment Systems), созданной в рамках G10 в 1980 г., и для завершения работы, начатой Комитетом по межбанковским схемам неттинга CINS (Committee on Interbank Netting Schemes), созданным в рамках G10 в 1989 г.

КПРС функционирует под эгидой БМР и начиная с 2009 г. отчитывается о своей работе перед председателем Собрания по глобальной экономике GEM (Global Economy Meeting), которое объединяет руководителей центральных бан-

¹ Группа десяти (Group of ten, G10) — объединение, созданное в рамках Международного валютного фонда. Членами группы являются центральные банки следующих стран: Бельгия, Великобритания, Германия, Италия, Канада, Нидерланды, США, Франция, Швеция, Япония и Швейцария.

ков 30 стран — членов Базельского соглашения (акционеров БМР), включая руководителя Банка России. Банк России входит в эту тридцатку.

Деятельность КПРС направлена на совершенствование инфраструктуры финансового рынка с позиций совершенствования платежных и расчетных систем.

В рамках КПРС осуществляются мониторинг и анализ достижений развития платежных, расчетных и клиринговых систем отдельных стран, а также систем трансграничных и мультивалютных расчетов. Исследования и публикации КПРС способствуют стандартизации, кодификации и широкому распространению лучших практик.

Наиболее известными публикациями КПРС являются¹:

- «Глоссарий терминов, используемых в платежных и расчетных системах» [4];
- «Общее руководство по развитию национальной платежной системы» [9];
- «Новые разработки в платежных системах для крупных сумм» [7];
- «Механизмы клиринга и расчета розничных платежей в некоторых странах» [1];
- «Взаимозависимости платежных и расчетных систем» [11];
- «Наблюдение центрального банка за платежными и расчетными системами» [8];
- «Обзор новаций в области электронных денег и платежей, совершаемых с использованием мобильных средств связи и Интернета» [6] и др.

В настоящее время Банк России ведет огромную работу по переводу и публикации документов КПРС в журнале «Платежные и расчетные системы»².

ЕВРОПЕЙСКИЕ МЕЖДУНАРОДНЫЕ ИНСТИТУТЫ

Активным участником процессов развития и интеграции национальных платежных систем является Европейский центральный банк (European Central Bank — ЕСВ), который был учрежден в 1998 г. как преемник Европейского валютного института (European Monetary Institute — ЕМИ).

Наряду с национальными центральными банками ЕСВ входит в Европейскую систему центральных банков (European System of Central Banks — ЕСЦБ), которая была создана в соответствии с условиями Маастрихтского договора и Статута Европейской системы центральных банков (далее — ЕСЦБ) и Европейского центрального банка (далее — ЕЦБ).

Главным направлением деятельности ЕСВ являются вопросы монетарной политики, поэтому в официальных документах вопросы платежных систем в документах ЕСВ обычно тесно увязаны с вопросами стабильности финансовой системы Европейского союза.

¹ В квадратных скобках — номер в Перечне основных публикаций КПРС БМР, приведенный в конце текста главы.

² Журналы находятся в открытом доступе на сайте Банка России www.cbr.ru в разделе «Издания Банка России», подразделе «Платежные и расчетные системы».

В частности, это видно на примере электронных денег, изучению и регулированию которых ЕСВ уделяет много внимания. Уже в самой первой своей публикации по вопросам электронных денег в 1998 г.¹ ЕСВ выделил основные проблемные вопросы функционирования электронных денег, которые актуальны по сегодняшний день.

Одновременно ЕСВ проводит изучение текущего состояния национальных и международных платежных систем Евросоюза, включая обобщение лучших практик в области предоставления платежных услуг. Наиболее известной официальной публикацией ЕСВ в этой области является Синяя книга (Blue Book), посвященная платежным системам и системам расчета по ценным бумагам, функционирующим в рамках Евросоюза.

Наиболее известной неофициальной публикацией ЕСВ, посвященной платежным системам, является книга «Платежная система. Платежи, ценные бумаги и производные и роль Евросистемы», выпущенная в 2010 г. под редакцией Тома Коколы.

Еще одним известным европейским институтом является Европейский платежный совет (European Payment Council — ЕРС). ЕРС создан в 2002 г. европейской банковской индустрией для координации и принятия совместных решений в области платежных услуг. Основным направлением деятельности ЕРС является поддержка и продвижение Единого европейского платежного пространства (Single European Payment Area — SEPA).

ЕРС разрабатывает платежные схемы и структуры, необходимые для реализации интегрированного рынка платежей в евро. В частности, ЕРС вырабатывает позиции для сотрудничества в области платежных услуг, определяет стратегию в области стандартизации, разрабатывает правила, лучшие практики и стандарты, а также осуществляет поддержку и мониторинг процесса реализации принятых решений.

1.2. ПОНЯТИЕ И СТРУКТУРА НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ

Национальная платежная система является подсистемой финансовой системы государства, которая обеспечивает экономических субъектов платежными услугами. При этом НПС не является платежной системой национального масштаба, а представляет собой совокупность всех платежных элементов национальной финансовой системы, включая все государственные и коммерческие платежные и расчетные системы.

Как правило, каждое государство подходит к понятию НПС исходя из национального опыта, сложившегося под воздействием национальных культурных, экономических и политических традиций. Тем не менее в последние десятилетия расширение сотрудничества национальных центральных банков в рамках международных организаций позволило выработать общие принципы построения и развития НПС, в том числе найти общий подход к понятию НПС.

¹ Report on Electronic Money. European Central Bank, August 1998.

ТЕРМИН «НАЦИОНАЛЬНАЯ ПЛАТЕЖНАЯ СИСТЕМА»

В глоссарии к публикации КППРС «Общее руководство по развитию национальной платежной системы» определение термина «национальная платежная система» дано в следующем варианте:

«Национальная платежная система — институциональные и инфраструктурные механизмы финансовой системы, используемые при инициации и переводе денежных требований в форме обязательств центрального банка и коммерческих банков» [9].

Можно дать и несколько более общее определение данного термина, которое учитывает, что система — это совокупность взаимосвязанных элементов, а также тот факт, что денежные требования могут существовать в форме обязательств учреждений электронных денег:

«Национальная платежная система — совокупность взаимосвязанных институциональных и инфраструктурных механизмов финансовой системы, используемых при инициации и переводе денежных требований в форме обязательств центрального банка, коммерческих банков и учреждений электронных денег».

Заметим, что прилагательное «платежная» в названии НПС не случайно: согласно определению КППРС [4], платеж — это «перевод денежного требования плательщиком стороне, приемлемой для получателя». В связи с этим НПС можно рассматривать как совокупность механизмов, обеспечивающих осуществление платежей.

Учитывая, что платежи — это основа экономической и финансовой систем, НПС играет важную роль в жизни любого государства.

Во-первых, НПС создает на территории государства условия для хозяйственного оборота имущества и имущественных прав, предоставляя возможность осуществления платежей по сделкам в рамках функционирования хозяйственных единиц (в том числе при производстве и продаже товаров, выполнении работ, предоставлении услуг и т.п.).

Во-вторых, НПС обеспечивает реализацию экономической и финансовой политики государства, в том числе:

- денежно-кредитной политики (платежи на денежном рынке и рынке ценных бумаг в рамках управления денежной массой и процентными ставками);
- бюджетно-налоговой политики (платежи в рамках процедур сбора налогов и распределения бюджета);
- валютной политики (платежи на валютном рынке в рамках управления курсом национальной валюты);
- инвестиционной политики (платежи в рамках реализации государственных инвестиционных проектов) и т.д.

Кроме того, НПС дает возможность осуществлять и другие платежи, находящиеся за рамками хозяйственного оборота и выполнения государственных задач (предоставление безвозмездной помощи, оплата штрафов и т.д.).

При этом эффективность осуществления платежей определяется следующими факторами:

- способностью НПС быстро и эффективно обрабатывать крупные и мелкие платежи;
- устойчивостью НПС к флуктуациям ликвидности и дефолтам экономических субъектов;
- способностью НПС обеспечивать безопасность, надежность и конфиденциальность процессов осуществления платежей;
- способностью НПС обеспечивать непрерывное функционирование платежной инфраструктуры и ее быстрого восстановления в случае сбоев и т.д.

Совершенно очевидно, что перечисленные особенности НПС непосредственно воздействуют на результаты финансовой деятельности субъектов экономики и, как следствие, оказывают значительное влияние на агрегированные показатели макроэкономических достижений государства. В связи с этим большинство государств уделяют вопросам построения и развития НПС большое внимание, стараясь поддерживать на современном уровне национальные платежные институты и национальную платежную инфраструктуру.

СТРУКТУРА НПС

Рассмотрим, что представляет собой структура НПС и в частности — институциональные и инфраструктурные механизмы, о которых идет речь в определении НПС. Воспользуемся еще одной цитатой из вышеупомянутой публикации КПРС, согласно которой НПС «включает в себя следующие основные элементы:

- платежные инструменты, используемые для инициирования и направления перевода денежных средств со счетов плательщиков на счета получателей в финансовых институтах;
- платежную инфраструктуру для исполнения и клиринга платежных инструментов, обработки и передачи платежной информации, а также перевода денежных средств между институтами-плательщиками и получателями;
- финансовые институты, предоставляющие счета для осуществления платежей, платежные инструменты и услуги потребителям, а также предприятия и организации, являющиеся операторами сетей операционных, клиринговых и расчетных услуг по платежам для этих финансовых институтов;
- рыночные механизмы, такие как договоренности, обязательные предписания и договоры по созданию различных платежных инструментов и услуг, формированию цен на них, а также их предоставлению и приобретению;
- законы, стандарты, правила и процедуры, установленные законодательными, судебными и регулирующими органами, которые определяют и регулируют механизм перевода платежей и рынки платежных услуг.

Платежная инфраструктура включает в себя все отдельные операционные, клиринговые и расчетные системы по платежам, действующие в стране, даже

если их головные офисы находятся за ее пределами. Некоторые элементы инфраструктуры могут быть специально разработаны для конкретных видов платежных инструментов. Институциональные механизмы включают в себя рыночные механизмы для различных видов платежных услуг, а также финансовые институты и другие организации, предоставляющие платежные услуги пользователям, а также правовую и нормативную базу для организации и функционирования рынка и механизмы консультации и координации между основными заинтересованными сторонами. Институциональная структура функционально связывает заинтересованные стороны в рамках инфраструктурных механизмов в национальную платежную систему».

Заметим, что английские слова *institutional and infrastructure arrangements* переведены как «институциональные и инфраструктурные механизмы», что отличается от подхода Банка России, который предпочитает говорить об «институциональном и инфраструктурном взаимодействии» [9], тем самым подчеркивая взаимодействие отдельных элементов в рамках каждого механизма. Однако представить НПС как систему, состоящую из одного только взаимодействия, достаточно трудно, поэтому в данной главе будет использоваться первый вариант перевода, причем всякий раз будет предполагаться, что речь идет о совокупности взаимосвязанных институциональных и инфраструктурных элементов.

Учитывая рассмотренные выше определения НПС, в общем случае можно выделить следующие элементы системы:

- плательщики и получатели денежных средств;
- денежные требования по обязательствам центрального и коммерческих банков;
- платежные инструменты и платежные услуги;
- финансовые институты и счета в финансовых институтах;
- операционные, клиринговые и расчетные системы;
- рыночные механизмы;
- механизмы консультаций и координации;
- правовая и нормативная база.

На рисунке 1.1 показана структура НПС в том виде, как ее рассматривает КПРС. Структура включает несколько логических блоков:

а) элементы НПС, непосредственно вовлеченные в перевод денежных требований в виде обязательств центрального и коммерческих банков, — наличные и депозитные деньги, плательщик и получатель средств (верхний пунктирный прямоугольник);

б) элементы НПС, обеспечивающие перевод денежных требований (нижний пунктирный прямоугольник);

в) системы по ценным бумагам¹.

¹ Включение систем по ценным бумагам в состав НПС блока вызывает некоторые вопросы, так как далеко не все элементы систем по ценным бумагам относятся к механизмам финансовой системы, используемым при инициации и переводе денежных требований.



Рис. 1.1. Схема национальной платежной системы в документах КПРС

Кроме того, на рис. 1.1 в нижнем пунктирном прямоугольнике показан блок институциональной структуры, взаимодействующий с блоком (внутренний пунктирный прямоугольник), в который входят платежные инструменты и платежная инфраструктура, а также показана взаимосвязь между блоком платежных инструментов и блоком платежной инфраструктуры.

ПЛАТЕЖНЫЕ ИНСТРУМЕНТЫ

В соответствии с позицией КПРС платежный инструмент представляет собой «любой инструмент, предоставляющий держателю (пользователю) возможность для перевода денежных средств» [4]. Причем «перевод» означает «перевод денежного требования плательщиком стороне, приемлемой для получателя», с уточнением, что «как правило, требования принимают форму банкнот или остатков на счетах, открытых в финансовом учреждении или в центральном банке» [4].

Как правило, в состав платежных инструментов включают наличные платежные инструменты (наличные деньги), а также следующие безналичные платежные инструменты:

- кредитовый перевод;
- прямой дебет;

- платежные карты;
- платежные чеки;
- электронные деньги.

Кредитовый перевод представляет собой «платежное поручение или, возможно, последовательный ряд платежных поручений, переданных с целью предоставить денежные средства в распоряжение бенефициара» [4].

Инициатором такого платежного поручения является плательщик, который дает платежные инструкции банку плательщика. Далее платежные инструкции (и указанные в них денежные средства) перемещаются из банка плательщика в банк бенефициара. При этом на пути между двумя этими банками платежные инструкции и денежные средства могут проходить через несколько банков-посредников.

В отличие от кредитового перевода **прямой дебет** — это «предварительно разрешенное дебетование банковского счета плательщика, инициированное получателем» [4].

Бенефициар (получатель средств) может направить платежные инструкции для прямого дебетования счета плательщика как напрямую плательщику, так и через банк бенефициара в банк плательщика. При этом предварительное разрешение плательщика на платеж может быть дано заранее или в ответ на запрос банка плательщика.

Среди платежных карт различают кредитные и дебетовые карты.

Кредитная карта — это «карта, свидетельствующая о том, что ее держателю предоставлена кредитная линия». Такая карта «дает держателю возможность совершать покупки и (или) снимать наличность в пределах заранее установленного лимита», причем «предоставленный кредит может быть погашен полностью по окончании определенного периода или частично, при этом остаток рассматривается как расширенный кредит». Кроме того, «с суммы любого расширенного кредита взимаются проценты, а с держателя иногда взимается годовая комиссия» [4].

Дебетовая карта — это «карта, дающая возможность держателю оплачивать покупки напрямую за счет денежных средств на его счете в депозитном учреждении», причем такая карта «иногда может совмещаться с другой функцией, например с функцией карты по выдаче наличных или карты гарантии чека» [4].

На сегодняшний день платежные карты — это самый популярный платежный инструмент на розничном рынке. Безопасность платежей обеспечивается за счет соответствующих процедур идентификации и аутентификации платежных карт, а авторизация — после проверки наличия у держателя карты соответствующих денежных средств (остатка на счете или неиспользованного кредита).

Платеж с помощью платежной карты обычно занимает доли минут и осуществляется в режиме онлайн, путем обмена сообщениями между POS-терминалом (при оплате товаров и услуг в торговых точках) или банкоматом (при снятии и зачислении наличных либо осуществлении платежей), с одной стороны, и процессинговым центром соответствующей платежной системы — с другой.

Чек представляет собой «письменное поручение одной стороны (чекодателя) другой стороне (чекодержателю, как правило банку), обязывающее чекодержателя выплатить определенную сумму по требованию чекодателя или третьей стороны, указанной чекодателем», при этом «чеки могут использоваться для погашения долгов и для снятия денег в банках» [4].

Различают именные чеки (выписываются на определенное лицо), ордерные (выписываются на определенное лицо со специальным указанием «или его приказу»), которые могут передаваться с помощью индоссамента, и чеки на предъявителя (выписываются на предъявителя).

В отношении чеков может применяться обычное и специальное кроссирование: обычное кроссирование (две параллельные линии на лицевой стороне чека) запрещает выдавать денежные средства по чеку наличными денежными средствами и используется только для зачисления денежных средств на банковский счет получателя, а специальное кроссирование (две параллельные линии и между ними наименование банка получателя средств) — в целях ограничения дальнейших передач чека.

Наконец, **электронные деньги** определяются КППС как «стоимость, хранящаяся электронным способом в устройстве, таком как карта с микропроцессором или жесткий диск персонального компьютера» [4].

Электронные деньги могут храниться в электронном кошельке, электронном бумажнике или иным способом. При этом электронным кошельком называется «перезагружаемая многоцелевая предоплаченная карта, которая может использоваться для небольших розничных и других платежей вместо монет» [4].

Электронный бумажник — «компьютерное устройство, используемое в некоторых системах электронных денег, которое может включать в себя карту с интегральной схемой или в которое могут быть встроены карты с интегральной схемой и которое может выполнять больше функций, чем карта с интегральной схемой» [4].

В последнее время все большее количество систем электронных денег строится по аналогии с электронными системами депозитных денежных средств, с тем отличием, что в первом случае учет денежных средств ведется на виртуальных счетах оператора электронных денег, а во втором — на банковских счетах кредитных организаций.

ИНСТИТУЦИОНАЛЬНАЯ СТРУКТУРА

В общем случае институциональная структура НПС включает в себя законы, практику и организационные механизмы, способствующие осуществлению переводов денежных требований. В частности, в рамках институциональной структуры можно выделить следующие элементы:

- рыночные механизмы;
- правовую и нормативную базу;

- механизмы консультаций и координации действий между заинтересованными сторонами;
- финансовые институты и другие организации, предоставляющие платежные услуги пользователям.

Рыночные механизмы включают рыночные соглашения о создании платежных инструментов, стандарты форматов платежных инструментов, стандарты и процедуры ведения бизнеса, соглашения и процедуры формирования цен на использование платежных инструментов, порядок разработки типовых договоров по оказанию платежных услуг, регламенты предоставления и приобретения платежных инструментов и т.д.

Правовая и нормативная база включает общую и специальную правовую базу, а также иные нормативные документы, регулирующие деятельность субъектов НПС.

В правовую базу общего применения, как правило, входят законы и нормативные акты, регулирующие правоотношения в области вещного, договорного и корпоративного права, законодательство о конкуренции и банкротстве, а также другие акты, оказывающие воздействие на платежную систему.

Специальные законы и нормативные акты обычно включают законодательство и принятые в соответствии с ним регламенты о национальной платежной системе, о платежах и платежных услугах, о неттинге и взаимозачете, об операционной, клиринговой и расчетной деятельности, о трансграничных платежах и т.д.

Кроме того, правовую и нормативную базу НПС составляют законодательные и судебные механизмы по принятию, применению и толкованию законов и нормативных актов, а также по процедурам вынесения по ним судебных решений и принудительного исполнения вынесенных решений.

Механизмы консультаций и координации действий между заинтересованными сторонами включают механизмы консультаций по вопросам развития НПС и рынка платежных услуг, координации действий при достижении общих и индивидуальных целей участников рынка, механизмы координации наблюдения и регулирования НПС и т.д.

Как правило, механизмы консультаций и координации предполагают создание различных совместных органов и рабочих групп из числа заинтересованных сторон, а также утверждение процедур обсуждения, планирования и реализации совместных действий.

В частности, механизмы консультаций и координации действий участников рынка платежных услуг (включая контролирующие и регулирующие органы власти) оказывают существенную помощь при выстраивании баланса индивидуальных и общих целей участников рынка. С одной стороны, они способствуют сохранению высокого уровня конкуренции, обеспечивающей появление и развитие новых платежных инструментов и услуг; с другой стороны, обеспечивают стабильность, безопасность и эффективность платежных операций за счет выра-

ботки совместных решений по внедрению лучших практик, стандартов, типовых договоров, кодексов поведения и т.д.

Финансовые институты и другие организации, участвующие в предоставлении платежных услуг, являются главными организационными механизмами институциональной структуры НПС. Они обеспечивают реализацию стандартных управленческих функций (мониторинг, прогнозирование, планирование, организация, руководство, регулирование, контроль и т.д.) в процессе функционирования и совершенствования других элементов институциональной структуры, а также элементов платежной инфраструктуры.

При этом финансовые институты (и другие организации) как организационные механизмы необходимо отличать от финансовых институтов (и других организаций) как элементов платежной инфраструктуры, когда речь идет о технологической составляющей их деятельности (технической инфраструктуре, технологических процедурах и т.д.).

ПЛАТЕЖНАЯ ИНФРАСТРУКТУРА

В общем случае в изложении КПРС платежная инфраструктура представляет собой «совокупность сетевого оборудования, технологий и процедур для осуществления доступа и операций с платежными инструментами, а также для обработки, клиринга и расчета по соответствующим платежам» [2].

КПРС включает в платежную инфраструктуру следующие инфраструктурные элементы:

- операционную инфраструктуру;
- клиринговую инфраструктуру;
- расчетную инфраструктуру.

К операционной инфраструктуре относится та часть платежной инфраструктуры, которая задействована в предоставлении услуг по созданию, подтверждению и передаче платежных инструкций. Такие услуги, в частности, включают следующие процедуры:

- идентификацию и аутентификацию сторон, участвующих в платежной операции, в том числе с использованием технологий шифрования;
- проверку и подтверждение соответствия используемого платежного инструмента стандартам и другим системным требованиям;
- проверку и подтверждение платежеспособности плательщика, в том числе с учетом механизмов обеспечения ликвидности;
- авторизацию перевода денежных средств между финансовыми учреждениями получателя и плательщика;
- учет, хранение и предоставление платежной информации, обрабатываемой в рамках операционной инфраструктуры;
- распространение информации между учреждениями в соответствии с правилами платежных систем.

Клиринговая инфраструктура обеспечивает предоставление услуг по передаче, согласованию и (в некоторых случаях) подтверждению платежных инструкций между финансовыми учреждениями, а также к вычислению межбанковских расчетных позиций. В рамках клиринговой инфраструктуры осуществляются:

- сортировка и сверка платежных инструкций, относящихся к тем или иным финансовым учреждениям, участвующим в осуществлении платежей;
- сбор, обработка и группировка данных, связанных с осуществлением платежей, по каждому финансовому учреждению;
- подготовка и хранение отчетности по платежам и передача ее каждому финансовому учреждению;
- вычисления позиций по валовому или нетто-расчету (сумм денежных средств, подлежащих уплате или получению) по каждому финансовому учреждению.

Расчетная инфраструктура используется для предоставления услуг по межбанковскому переводу денежных средств. Она обеспечивает:

- сбор денежных требований, в соответствии с которыми должны осуществляться расчеты, и проверку их полноты;
- проверку наличия денежных средств на счетах финансовых учреждений в расчетном банке, необходимых для проведения расчета;
- осуществление расчета в соответствии с требованиями путем перевода денежных средств по счетам финансовых учреждений в расчетном банке;
- выполнение учетных записей, относящихся к расчету, и доведение информации об этих записях до сведения заинтересованных финансовых учреждений.

1.3. РАЗВИТИЕ НАЦИОНАЛЬНЫХ ПЛАТЕЖНЫХ СИСТЕМ

В общем случае под развитием системы подразумевается такое изменение системы, которое характеризуется переходом системы из менее развитого в более развитое состояние. Как правило, развитие системы подразумевает наличие четырех элементов:

- шкалы развития, на которой упорядочены положения состояний системы от менее развитых к более развитым;
- метода оценки состояния системы по шкале развития;
- способа изменения состояния системы по шкале развития;
- движущей силы развития.

Например, развитие системы можно оценивать по количеству элементов, шкалу развития можно упорядочить от меньшего количества элементов к большему, а механизмом движения можно считать добавление к системе новых элементов. Причем движущей силой такого развития может быть инициатива индивида, корпоративная политика, рыночная конкуренция, государственная политика и т.п.

Совершенно очевидно, что шкал развития, методов оценок, механизмов и движущих сил движения может быть много, а тот или иной выбор носит субъективный характер.

Все сказанное выше имеет прямое отношение к НПС, когда каждое государство руководствуется своим пониманием шкалы развития НПС, методов оценки состояния НПС по этой шкале, приемлемых способов изменения состояний НПС и движущих сил такого изменения. Причем такое понимание формируется под воздействием большого количества национальных особенностей, которые определяются политическими, экономическими, социальными, культурными и другими факторами.

Как правило, национальные особенности глубоко проникают как в теоретическое обоснование развития НПС, так и в практический опыт построения институтов и инфраструктуры. В связи с этим процессу развития НПС может существенно мешать недостаток знаний, ограниченное концептуальное видение, а также отсутствие механизмов изучения и внедрения зарубежного опыта.

Сегодня существует целый ряд международных институтов, которые изучают и сравнивают те или иные элементы НПС разных государств, а также выявляют и обосновывают лучшие институциональные и инфраструктурные механизмы. Как результат, появилась возможность координации позиций государств в вопросах понимания шкалы развития НПС, методов оценок и механизмов движения.

КПРС является наиболее авторитетным международным органом по вопросам развития НПС. КПРС на постоянной основе собирает информацию и изучает опыт построения и развития НПС разных государств, что позволяет ему выявлять и распространять среди заинтересованных государств наиболее эффективные правила, технологии и схемы взаимодействия.

ФАКТОРЫ, ТЕНДЕНЦИИ И ПРИНЦИПЫ РАЗВИТИЯ НПС

КПРС выделяет следующие факторы, влияющие на построение и развитие НПС:

а) факторы среды, которые определяют вероятность поддержки реформ:

- демографические факторы, включая численность и структуру населения,
- географические факторы, включая уровень и распределение природных ресурсов,
- социальные и культурные ценности и нормы;

б) экономические факторы, которые в том числе определяют потребности государства в платежных услугах и его ресурсные возможности в части реализации реформ:

- уровень и стабильность экономического роста в целом,
- факторы распределения национального богатства,
- уровень и квалификация рабочей силы, а также наличие возможностей для повышения квалификации,

- развитие отраслевой инфраструктуры, в частности телекоммуникационных и транспортных систем,
- темпы инновационных и технологических изменений;

в) финансовые факторы, которые могут стимулировать спрос и предложение новых платежных инструментов и услуг:

- финансовые издержки, риски и выгоды платежных услуг,
- инициативы по совершенствованию платежных услуг, направленные на снижение издержек и рисков и повышение выгод для пользователей и провайдеров;

г) факторы государственной политики, которые непосредственно влияют на институциональные механизмы:

- законы и государственная политика в отношении рынка и финансовых институтов,
- государственная политика в области образования, промышленности, торговли, защиты прав потребителей и т.д.,
- государственная политика в отношении макроэкономических показателей.

Считается, что все эти факторы влияют на развитие НПС в основном через механизм спроса и предложения платежных услуг, а также через рыночные механизмы оказания платежных услуг. При этом КПРС выделяет следующие характеристики спроса и предложения платежных услуг:

а) спрос на платежные услуги:

- степень доступности и возможности выбора платежных инструментов и услуг,
- наличие информации об относительных выгодах и издержках пользователей, а также о рисках в отношении различных инструментов и услуг,
- уровень издержек пользователей,
- уровень взаимодействия между конкурирующими операционными сетями в отношении аналогичных платежных инструментов,
- уровень правового риска и степени информационной безопасности.

В частности, спрос на платежные услуги увеличивается при справедливом доступе к платежным услугам, низким издержкам при осуществлении платежей, быстром и предсказуемом предоставлении услуг, безопасности платежных операций и т.д.;

б) предложение платежных услуг:

- уровень новых технологий в области обработки информации, телекоммуникаций и транспортировки для передачи и перевода платежных инструкций и инструментов,
- степень совместимости механизмов обработки транзакций в системах банкоматов¹, терминалов электронного перевода денежных средств в пункте продаж² и платежей через Интернет,

¹ Automated Teller Machine (ATM).

² Electronic Funds Transfer at Point of Sale (EFTPOS).

- степень расширения деятельности финансовых и нефинансовых институтов за счет предоставления новых услуг и вторжения на новые рынки.

В частности, увеличению предложения на рынке платежных услуг способствуют интеграция клиринговых и расчетных систем, совершенствование регламентов (включая законодательство) в области организации, управления и функционирования платежной инфраструктуры, проведение реформ, направленных на снижение операционного риска при осуществлении сетевых операций, и т.д.

КПРС отмечает, что в общем случае развитие направлено на повышение системной надежности и эффективности НПС в целом. В то же время можно выделить некоторые вполне определенные тенденции:

- постепенное расширение перечня платежных инструментов и услуг;
- облегчение доступа финансовых институтов к дешевым кредитам под расчеты;
- улучшение механизмов платежных систем, ответственных за экономию ликвидности;
- повышение уровня совместимости, взаимодействия и устойчивости инфраструктуры обработки платежей, сделок с ценными бумагами и конверсионных операций с целью облегчения сквозной обработки транзакций¹;
- внесение изменений в платежную инфраструктуру для снижения правовых, операционных и финансовых рисков участников платежных и расчетных систем, а также для повышения эффективности платежных операций с точки зрения издержек;
- совершенствование режима регулирования НПС и развитие функции наблюдения за НПС в рамках центрального банка;
- повышение эффективности, стабильности и организованности рынков, ответственных за предоставление платежных услуг и формирование цен на платежные услуги.

Проведение реформ, как правило, сталкивается с огромным количеством проблемных вопросов, которые тормозят развитие НПС. В частности, по мнению КПРС бесперебойному и эффективному проведению реформ мешают:

- неправильные представления участников процесса о предметной области;
- ограниченное концептуальное видение и руководство процессом;
- ограниченная информация о возникающих потребностях и системных возможностях;
- недостаточное вовлечение заинтересованных лиц в процесс консультаций и, как следствие, слабая поддержка и приверженность реформам с их стороны;
- ограниченные ресурсы для реализации проекта развития;
- законодательные, политические и рыночные барьеры, мешающие осуществлению непрерывного процесса развития НПС.

¹ *Straight Through Processing (STP)*.

Для преодоления указанных ограничений КПРС разработал 14 руководящих принципов, направленных на поддержание усилий государств по развитию НПС, которые фактически стали отраслевым стандартом.

Все принципы сгруппированы в четыре раздела, которые посвящены:

- участию в развитии НПС банковской системы;
- планированию и реализации проекта развития НПС;
- развитию институциональных механизмов НПС;
- развитию инфраструктурных механизмов НПС.

При этом подчеркивается ключевая роль центрального банка в реализации этих принципов, в том числе путем исполнения ролей оператора собственной платежной системы, органа наблюдения в отношении ключевых платежных механизмов, пользователя платежных услуг и катализатора процесса реформирования НПС.

УЧАСТИЕ БАНКОВСКОЙ СИСТЕМЫ В РАЗВИТИИ НПС

Банковская система принимает непосредственное участие в функционировании НПС. Во-первых, одной из основных функций банков и аналогичных им финансовых институтов является предоставление платежных инструментов и платежных услуг индивидуальным потребителям и компаниям. Во-вторых, межбанковские расчеты на финансовом рынке (по конверсионным сделкам, по сделкам с ценными бумагами и т.д.) составляют большую часть всех платежных операций. Как следствие, развитие НПС тесно связано с развитием банковской системы.

Учитывая это, КПРС рекомендует применять следующие два руководящих принципа в отношении участия банковской системы в развитии НПС:

- сохранять за центральным банком главную роль;
- повышать роль устойчивой банковской системы.

Принцип сохранения за центральным банком главной роли

Принцип сохранения за центральным банком главной роли в процессе развития НПС основан на том, что качество функционирования НПС оказывает непосредственное влияние на качество национальной валюты, в том числе в части ее использования как средства платежа. Учитывая, что именно центральный банк отвечает за устойчивость национальной валюты и за ее эффективное использование в качестве средства платежа, он должен возглавить процесс развития НПС, причем рассматривать развитие НПС как приоритетное направление своей деятельности.

С точки зрения КПРС центральный банк может развивать НПС за счет следующих механизмов (в рамках выполнения указанных выше функций):

а) как оператор (провайдер) платежных услуг:

- эмитируя наличные деньги в качестве непосредственного платежного инструмента и депозитные требования в качестве расчетного актива для межбанковских платежей,

- владея, обрабатывая операции или участвуя в управлении системно значимыми клиринговыми и расчетными системами,
 - владея или обрабатывая операции в значимых (но не системно значимых) клиринговых и расчетных системах, возможно, участвуя в управлении такими системами,
 - предоставляя расчетные счета и обеспечивая кредитование (под внутридневные расчеты и для завершения расчетов в конце дня) для участников расчетной системы;
- б) как катализатор процесса развития:
- иницилируя, координируя, проводя исследования и консультируя по вопросам проектирования и функционирования платежных систем, включая вопросы политики,
 - консультируя и при необходимости разрабатывая законопроекты по вопросам НПС;
- в) как орган наблюдения:
- осуществляя мониторинг существующих и планируемых систем и оценивая их с точки зрения безопасности и эффективности,
 - консультируя, предлагая рекомендации и при необходимости настаивая на внесении изменений в технологию и операции платежных систем,
 - публикуя принципы, политику и основные направления деятельности в области наблюдения;
- г) как пользователь платежных услуг:
- используя для осуществления платежей (в том числе по поручению правительства и его агентов) системы, которыми владеют и которые процессируют третьи лица,
 - используя для осуществления собственных операций депозитарии и системы расчетов по ценным бумагам,
 - используя услуги корреспондентского банкинга других центральных банков и финансовых институтов.

При этом центральный банк должен прикладывать необходимые усилия для организации сбалансированного выполнения перечисленных функций (оператора, катализатора, органа наблюдения и пользователя) в рамках своей деятельности в качестве центрального банка. В том числе предполагается, что центральный банк уделяет особое внимание планированию и расстановке приоритетов развития этих функций, а также постоянно совершенствует знания и компетентность персонала.

Принцип повышения роли устойчивой банковской системы

Принцип повышения роли устойчивой банковской системы основан на том, что успешное развитие НПС во многом зависит от того, насколько банки и другие финансовые институты способны действовать совместно, как система, чтобы

обеспечить доверие к банковской системе в целом. При этом КПРС рассматривает банковскую систему как систему, которая включает в себя все финансовые институты, принимающие депозиты, предоставляющие кредиты или оказывающие платежные услуги конечным пользователям в качестве одной из своих бизнес-функций.

В соответствии с данным принципом институты банковской системы как основные поставщики платежных инструментов и услуг конечным пользователям должны развивать:

- предоставление услуг на всей территории государства и с применением инновационных технологий и процедур;
- системы управления внутренними счетами и системы обработки платежей;
- механизмы дистанционного доступа по сети для услуг платежной инфраструктуры.

Причем расширение доступа к банковским и платежным услугам в национальном масштабе по мнению КПРС можно стимулировать путем:

- расширения доступа к платежным счетам и услугам через филиальные и агентские сети, а также через сети электронного банкинга (банкоматы, интернет-банкинг и т.д.);
- инвестирования в системы информирования и управления объединенными счетами, создаваемые на основе систем сетевого (удаленного) доступа;
- интеграции систем управления внутренними счетами с другими системами с целью предоставления клиентам услуг инициирования и авторизации платежей;
- расширения перечня розничных платежных инструментов.

Другая совместная деятельность финансовых институтов, направленная на укрепление доверия к банковской системе, может быть нацелена на создание отраслевых стандартов в части платежных инструментов и услуг, в том числе на базе международных стандартов. Для этой цели необходимо поощрять финансовые институты к созданию отраслевых групп и форумов, способных разработать такие стандарты.

При этом центральный банк может активно сотрудничать с банковской системой, продвигая и даже возглавляя инициативы частного сектора. Например, в качестве провайдера платежных услуг центральный банк может влиять на принятие отраслевых стандартов, а в качестве катализатора он может помочь банковской системе в организации отраслевой группы, а также может проводить с этой группой консультации по вопросам платежной политики.

ПЛАНИРОВАНИЕ ИНИЦИАТИВ РАЗВИТИЯ НПС

Как правило, развитие НПС представляет собой непрерывный процесс, состоящий из большого числа параллельно и последовательно выполняемых проектов, масштаб которых может варьироваться от кардинальных реформ инсти-

туциональных и (или) инфраструктурных механизмов до внесения простых изменений в отдельные элементы НПС.

В связи с этим в рамках планирования процесса развития НПС КПРС предлагает следующие руководящие принципы:

- осознавать сложность процесса;
- концентрироваться на потребностях;
- устанавливать четкие приоритеты;
- считать реализацию ключевым этапом.

При этом важно, чтобы в процесс планирования инициатив развития НПС были вовлечены все заинтересованные стороны (индивидуально и в группах), причем центральные банки и банковское сообщество должны разделять как интерес, так и ответственность в части руководства этим процессом.

Принцип осознания сложности процесса

Принцип осознания сложности процесса планирования требует, чтобы планирование осуществлялось при наличии всестороннего понимания ключевых элементов НПС, а также основных факторов, влияющих на ее развитие.

Если реформы НПС проводятся без учета многочисленных связей между институциональными и инфраструктурными элементами НПС, развитие системы рано или поздно столкнется с ограничениями, вызванными неравномерным развитием отдельных элементов. Устойчивое развитие НПС предполагает, что на этапе планирования инициатив развития необходимо рассмотреть все основные элементы системы и связи между ними, включая рыночные механизмы, правовую и нормативную базу, процессы развития банковской системы, основные факторы развития и т.д.

По мнению КПРС, планирование инициатив должно быть основано на широком видении проблемных вопросов и направлено на создание комплексного плана развития, который должен учитывать все многообразие и сложность структуры взаимосвязей в НПС. Только это поможет избежать непредвиденных и непреднамеренных последствий реформирования НПС негативного содержания.

Основными инструментами реализации данного принципа являются проведение комплексного анализа текущего состояния и подготовка всеобъемлющего обзора функционирования ключевых элементов НПС, в которых должны быть отражены:

- платежные инструменты и средства;
- платежная инфраструктура и платежные институты;
- использование платежной системы в финансовых операциях;
- процессы развития, оказывающие воздействие на НПС;
- статистические данные по НПС и др.

В подготовку обзора должны быть вовлечены все заинтересованные стороны, причем выявление заинтересованных сторон и их позиций также является

предметом анализа текущего состояния НПС. Технически реализовать вовлечение сторон можно различными методами, включая анкетирование, интервью, консультации и т.д.

Как правило, катализатором процесса подготовки отчета выступает центральный банк, который вносит основной вклад в подготовку отчета за счет доступа к огромному массиву информации о деятельности финансовых институтов.

Принцип концентрации на потребностях

Принцип концентрации на потребностях требует выявлять и руководствоваться потребностями всех пользователей НПС, а также возможностями экономики. При этом предполагается, что развитие НПС направлено прежде всего на удовлетворение потребностей пользователей, в том числе государство и его агентов.

Возникающие платежные потребности обычно обусловлены тенденциями и процессами развития в коммерческом, промышленном и финансовом секторах экономики. В связи с этим информация о таких тенденциях и процессах очень полезна для оперативного выявления и глубокого понимания новых потребностей.

По мнению КПРС основным средством определения потребностей может стать так называемый анализ бизнес-требований, целью которого является описание возможной бизнес-практики, вытекающей из тех или иных инициатив развития. Такой анализ позволяет определить:

- тенденции спроса и предложения платежных инструментов и услуг;
- правовой и финансовый риски участников возникающих взаимоотношений;
- роли заинтересованных сторон в качестве пользователей и провайдеров услуг;
- позиции органов надзора или регулирования в соглашениях об оказании услуг и т.д.

Как правило, анализ бизнес-требований выявляет необходимость развития технологического потенциала и человеческих ресурсов страны (например, телекоммуникационных и информационных технологий для развития определенной платежной инфраструктуры или образовательных программ в области эксплуатации сложных платежных систем). В связи с этим в рамках планирования инициатив развития необходимо оценить экономические возможности реализации таких затратных проектов.

Принцип установления четких приоритетов

Принцип установления четких приоритетов основан на необходимости стратегического планирования и определения приоритетов развития НПС. При этом стратегический план позволяет задать направление, конечную точку и масштаб изменений, а приоритизация — эффективно распределить ограниченные ресурсы для реализации плана.

Стратегический план должен рассматривать НПС с максимально широкими позицией, охватывая ключевые институциональные и инфраструктурные элементы, а также ключевые факторы, влияющие на их развитие. Разработка плана должна включать достижение согласия по основным инициативам (особенно если они касаются фундаментальных и широкомасштабных изменений) на основе двусторонних и многосторонних консультаций со всеми заинтересованными сторонами.

Для определения полезных инициатив развития НПС и их приоритетности КПСР предлагает использовать два основных аналитических метода:

- метод анализа «разрыва» ;
- метод анализа «издержек-рисков-выгод».

Анализ «разрывов» направлен на выявление конкретных элементов НПС, требующих реформирования. Он состоит из двух частей. В первой части результаты анализа бизнес-требований сравниваются с результатами обзора текущего состояния НПС и выявляются «разрывы» между текущим и желаемым состояниями НПС в виде институциональных и инфраструктурных элементов, требующих изменения. Во второй части анализа эти «разрывы» оцениваются с точки зрения возможностей по их заполнению новыми платежными продуктами, технологиями и услугами.

Анализ «разрывов» помогает определить перечень необходимых реформ, но не дает рекомендаций, проводить реформы одновременно, последовательно или в некоторой комбинации. В связи с этим используется анализ «издержек-рисков-выгод», который помогает установить нужные приоритеты.

Согласно названию, анализ «издержек-рисков-выгод» направлен на оценку трех экономических параметров для каждой из выбранных инициатив, а также структуризацию всех инициатив в соответствии со значениями этих параметров. Окончательный выбор последовательности, в которой данные инициативы будут реализованы, — во многом субъективный процесс, основанный на предпочтении (приемлемости) того или иного сочетания издержек, риска и выгоды.

Такой субъективизм существенно осложняет поиск и согласование компромиссного варианта среди заинтересованных сторон. При этом структура консультаций по выработке окончательного решения может как усилить, так и сгладить возможные перекося.

Принцип ключевой роли этапа реализации

Принцип ключевой роли этапа реализации направлен на обеспечение эффективной реализации стратегического плана за счет хорошей организации и правильного управления процессом реализации.

В реализацию проекта обычно вовлекается множество заинтересованных лиц, которые в рамках процесса реализации играют разные роли и несут разную ответственность. В связи с этим одна из главных задач плана реализации — обес-

печить координацию и контроль деятельности разных участников с целью достижения заданных результатов при соблюдении временных и ресурсных ограничений.

С точки зрения КПРС эффективный план реализации должен содержать:

- эффективные механизмы управления проектом;
- измеримые параметры реализации этапов проекта;
- четко заданные конечные и промежуточные результаты;
- возможные отклонения и процедуры их устранения;
- продуманную стратегию внедрения результатов;
- реалистичную стратегию управления ресурсами и финансами.

В случае масштабного проекта организация проекта может иметь сложную структуру. Как правило, проекты реформирования НПС выполняются большими проектными группами, которые имеют координационный комитет, руководителя и управляющего проектом, координаторов проектных подгрупп для каждой проектной инициативы и т.д.

При реализации проектов реформирования НПС центральные банки часто выступают в роли лидеров и катализаторов проектов. По мере необходимости центральный банк может:

- выступать спонсором, организатором, консультантом и участником проектных групп;
- принимать участие в работе организационных и координационных комитетов;
- привлекать экспертные знания из национальных и международных источников;
- способствовать реализации проекта путем реформирования собственных процедур и политик и т.д.

РАЗВИТИЕ ИНСТИТУЦИОНАЛЬНЫХ МЕХАНИЗМОВ НПС

Хотя развитие НПС часто связывают с развитием ключевых инфраструктурных механизмов, в силу институционально-инфраструктурного взаимодействия развитие платежных институтов имеет в проведении реформ не менее важное значение. Более того, в большинстве случаев эффективная реализация проектов развития предполагает, что институциональные изменения предшествуют инфраструктурным.

В общем случае институциональная структура НПС включает в себя законы, практику и организационные механизмы, способствующие осуществлению платежей и переводов. В частности, к платежным институтам относятся:

- рыночные механизмы оказания платежных услуг;
- механизмы консультаций с заинтересованными сторонами;
- механизмы координации процессов наблюдения за НПС;
- правовые механизмы, включая юридические соглашения о платежах.

Каждому из перечисленных элементов институциональной структуры соответствует свой руководящий принцип развития НПС.

Принцип содействия развитию рынка

Принцип содействия развитию рынка направлен на совершенствование рыночных механизмов оказания платежных услуг и исходит из того, что эффективное и надежное рыночное взаимодействие имеет решающее значение для пользователей и провайдеров и, следовательно, для функционирования НПС в целом.

При этом к рыночным механизмам относят те механизмы взаимодействия, которые обеспечивают координацию и формирование цен на платежные инструменты и услуги, а также предоставление платежных инструментов и услуг пользователям. В основном они включают процедуры, соглашения, нормативные акты и договоры, которые регулируют отношения между пользователями и провайдерами услуг при оказании платежных услуг и выполнении платежных операций.

Развитие НПС обычно сопровождается расширением круга платежных инструментов и услуг, включенных в рыночное взаимодействие, а также расширением круга провайдеров и пользователей этих инструментов и услуг. В этой связи по мере развития НПС структура рыночного взаимодействия обычно становится все более и более разнообразной и сложной, причем как в организационном, так и функциональном плане.

Как минимум услуги и рынки услуг обычно разделяют на два типа:

- платежные услуги «оптового» рынка для провайдеров платежных услуг;
- платежные услуги розничного рынка для конечных пользователей

При этом оптовый и розничный рынок во многом взаимосвязаны, так как многие финансовые институты являются пользователями услуг на одном рынке и провайдерами на другом. Кроме того, предоставление услуг на одном рынке может быть обусловлено услугами на другом рынке. Например, предоставление розничных услуг конечным пользователям часто влечет за собой предоставление клиринговых и расчетных услуг провайдерам услуг.

Реализация принципа содействия развитию рынка предполагает создание:

- механизмов рыночной координации;
- условий для эффективного рыночного ценообразования;
- механизмов рыночного информирования и прозрачности;
- условий для надлежащего доступа на рынок.

Механизмы рыночной координации позволяют пользователям и провайдерам услуг принять, отвергнуть или договориться об условиях оказания услуг. К ним относятся механизмы взаимодействия между отдельными пользователями и провайдерами, а также взаимодействия на уровне групп банков, компаний и индивидуальных пользователей.

Основная проблема такого взаимодействия — противоречие между целями конкуренции и сотрудничества. Если механизмы рыночного взаимодействия

препятствуют конкуренции, то снижается потенциал основной движущей силы развития, хотя одновременно увеличиваются возможности для сотрудничества.

В свою очередь сотрудничество на рынке может развиваться за счет:

- создания отраслевых кодексов ведения бизнеса и защиты прав потребителей;
- стандартизации форматов платежных инструментов;
- координации планов между провайдерами при создании платежных систем;
- разработки типовых договоров по оказанию платежных услуг и т.д.

Эффективное рыночное ценообразование является ключевым элементом функционирования и совершенствования НПС. При этом эффективные стратегии в области ценообразования отражают:

- затраты по созданию и предоставлению платежных инструментов или услуг;
- цену субститутов (заменителей) с учетом их удобства и качества;
- воздействие положительных и отрицательных сетевых факторов и др.
- В частности, схемы ценообразования могут включать:
- фиксированные комиссии за доступ к сети;
- пооперационные комиссии или комиссии за объем;
- дифференциацию комиссий для различных участников и т.п.

Заметим, что при неспособности рынка обеспечить эффективное ценообразование развитие НПС может потребовать внесения изменений в политику органов власти.

Механизмы рыночного информирования и прозрачности направлены прежде всего на то, чтобы заинтересовать пользователей новыми инструментами и услугами, а также информировать их о свойствах этих инструментов и услуг. Делая информацию доступной и ясной, такие механизмы способствуют созданию конкурентной среды и повышению уровня рыночной дисциплины.

Как правило, в базовые информационные материалы о новых инструментах и услугах включают:

- сведения о порядке оказания услуг;
- новые отличительные качества услуг в части удобства, стоимости и безопасности;
- ответственность пользователей в случае неправильного использования услуг и т.д.

Другой важной для рынка информацией является:

- законодательство о конкуренции и защите прав потребителей;
- стандарты договоров об оказании платежных услуг;
- специфические условия договоров конкретных финансовых институтов;
- отраслевые кодексы поведения и практика;
- статистические данные о функционировании различных инфраструктурных единиц;
- статистические данные об использовании платежных инструментов и т.д.

Создание условий для надлежащего доступа на рынок предполагает поиск оптимального варианта доступа, на который влияют два встречных процесса:

- 1) расширение круга участников и снижение барьеров для доступа с целью увеличения уровня конкуренции;
- 2) ограничение круга участников и увеличение барьеров для доступа с целью обеспечения устойчивости рынка.

Например, доступ к некоторым услугам, которые требуют распределения финансовых рисков, может быть ограничен кругом участников, в отношении которых действуют похожие правила пруденциального надзора. В частности, это относится к услугам в рамках клиринговых и расчетных соглашений, в которых обычно участвуют только банки и аналогичные финансовые институты.

Обычно в реализации принципа содействия развитию рынка активно участвует национальный центральный банк, который может включать вопросы развития рынка в программы своего сотрудничества с банковскими ассоциациями и другими отраслевыми группами. При этом деятельность центрального банка, как правило, направлена на продвижение политики справедливой конкуренции среди провайдеров услуг, раскрытие информации при оказании услуг, создание эффективных механизмов разрешения споров и принудительного исполнения решений и т.д. Одновременно центральный банк может способствовать развитию рынка путем выдвижения инициатив по совершенствованию законодательства (антимонопольного, о защите прав потребителей и т.д.).

Принцип вовлечения заинтересованных сторон

Принцип вовлечения заинтересованных сторон направлен на обеспечение поддержки процесса развития НПС со стороны потенциальных участников путем проведения эффективных консультаций.

Основными заинтересованными сторонами процесса развития, как правило, являются:

- центральный банк;
- банковские и платежные ассоциации;
- ассоциации по ценным бумагам;
- организации финансовой инфраструктуры (операторы платежных систем, операторы систем расчетов по ценным бумагам и т.д.);
- потребительские и розничные ассоциации;
- ассоциации казначейств в частном и государственном секторах и т.д.

Консультации с указанными сторонами могут проводиться как в структурированных группах, так и в рамках неформальных встреч. При этом основным инструментом достижения согласия по целям и направлениям реформ, как правило, являются структурированные двусторонние и многосторонние консультации.

Среди консультативных групп можно выделить стратегические консультативные группы, деятельность которых обычно направлена:

- на структуризацию исходной информации и проведение исследований по вопросам платежных систем;
- разработку инициатив, консультирование и поиск решений по проблемным вопросам платежных систем.

Но большая часть консультативных групп обычно фокусируется на конкретных элементах НПС и процесса развития НПС:

- на стратегическом и текущем планировании;
- платежных технологиях и стандартах;
- механизмах развития рынков;
- управлении рисками и т.д.

Организатором многих консультативных форумов обычно является центральный банк, в котором, как правило, сосредоточены обширные экспертные знания и который способен продвигать в консультативных группах культуру концептуального видения, вовлеченности и направленности действий.

Принцип сотрудничества в целях эффективного наблюдения

Принцип сотрудничества в целях эффективного наблюдения требует от центрального банка организации плодотворного сотрудничества с другими органами власти с целью развития НПС в части создания эффективных механизмов наблюдения за НПС.

Прежде всего к таким органам власти относятся:

- органы банковского надзора (если эти функции не выполняет центральный банк);
- органы регулирования по ценным бумагам;
- органы регулирования в сфере конкуренции;
- министерство финансов (казначейство и другие департаменты);
- органы по делам потребителей и т.д.

Цели механизмов сотрудничества могут включать:

- выявление тенденций, проблем и инициатив развития НПС и элементов НПС;
- выявление правовых проблем в рамках действующих и планируемых законов и иных нормативных актов;
- координацию действий по регулированию и наблюдению за НПС и т.д.

При этом особую важность приобретает задача объединения экспертных знаний центрального банка по специфике платежной системы с экспертными знаниями других органов власти по соответствующим аспектам операционной деятельности и рыночного поведения финансовых институтов, что может существенно улучшить качество политики в области наблюдения за НПС.

Принцип обеспечения правовой определенности

Принцип обеспечения правовой определенности направлен на создание прозрачной, полной и стабильной правовой базы, в рамках которой существует и развивается НПС.

Правовая база НПС представляет собой совокупность правовых норм, регулирующих права и обязанности субъектов НПС, а также процедуры перевода денежных средств и разрешения споров в отношении инструментов, услуг, окончательного расчета и т.д. Эти правовые нормы могут быть включены в один или несколько законов или в иные обязательные к исполнению нормативные акты, а также быть частью общего права.

Как правило, правовая база НПС должна включать:

- законы общего применения (право вещное, договорное, корпоративное, банковское, финансовое и т.д.);
- специальные законы о платежной системе (о платежных инструментах, неттинге, окончательности платежа и т.д.);
- законодательные и судебные механизмы по принятию и толкованию законов, а также вынесению и исполнению судебных решений.

При реализации принципа обеспечения правовой определенности КПРС рекомендует:

- адаптировать правовую базу к развитию НПС;
- проводить разработку правовой базы на основе консультаций;
- сделать правовую базу прозрачной и доступной.

Состояние правовой базы должно соответствовать уровню развития НПС. КПРС рекомендует реформировать правовую базу на основе типовых законов, разработанных международными правовыми организациями. Причем отдельно необходимо обращать внимание на то, чтобы правовая база обеспечивала выполнение международных соглашений страны по вопросам, связанным с осуществлением платежей.

Особенно чувствительны к уровню развития правовой базы системно значимые платежные системы и системы расчетов по ценным бумагам, так как подверженность риску убытков на сумму большую, чем ликвидность и капитал, одновременно подвергает их риску системного неисполнения обязательств в случае возникновения правовых проблем.

Реформа правовой базы должна сопровождаться консультациями со всеми заинтересованными сторонами (провайдерами услуг, пользователями и др.), а также с регулирующими и законодательными органами, чтобы ограничить риск непреднамеренных негативных последствий в результате изменений правовой базы.

При этом законы и иные нормативные документы правовой базы должны быть физически доступны всем желающим (в бумажном или электронном виде), причем содержание документов должно быть достаточно прозрачным, чтобы быть доступным для восприятия всем заинтересованным лицам.

РАЗВИТИЕ ИНФРАСТРУКТУРНЫХ МЕХАНИЗМОВ НПС

Инфраструктура НПС включает операционную, клиринговую и расчетную инфраструктуру платежных и расчетных систем, в том числе провайдеров соответствующих услуг, технологическое оснащение (специализированное оборудо-

вание, компьютерные программы, информационные сети и т.д.) и операционные процедуры.

Как уже упоминалось в параграфе «Понятие и структура НПС», к услугам платежной инфраструктуры относятся:

а) в части операционной инфраструктуры: услуги по созданию, подтверждению и передаче платежных инструкций, включая:

- идентификацию и аутентификацию участников операции,
- подтверждение соответствия платежного инструмента установленным требованиям,
- проверку платежеспособности плательщика,
- авторизацию перевода денежных средств между финансовыми институтами,
- учет и обработку платежной информации,
- передачу информации финансовым институтам;

б) в части клиринговой инфраструктуры: услуги по передаче, согласованию и подтверждению платежных инструкций между финансовыми институтами, а также по вычислению межбанковских расчетных позиций, включая:

- сортировку и сверку платежных инструкций,
- сбор, обработку и группировку платежных данных,
- хранение и передачу отчетности по платежам,
- вычисления позиций по валовому или нетто-расчету;

в) в части расчетной инфраструктуры: услуги межбанковского перевода денежных средств, включая:

- сбор и проверку целостности расчетных требований,
- проверку достаточности денежных средств на счетах финансовых институтов в расчетном банке для проведения расчета,
- проведение расчета на основе расчетных требований путем перевода денежных средств по счетам финансовых институтов в расчетном банке,
- учет операций по расчету и доведение учетной информации до сведения соответствующих финансовых институтов.

Конкретный провайдер услуг платежной инфраструктуры той или иной платежной системы предоставляет свой набор услуг из общего перечня услуг.

По мнению КПРС развитие инфраструктуры НПС должно включать:

- расширение доступности розничных платежных систем;
- развитие платежных систем для крупных сумм;
- совместное развитие платежных систем и систем по ценным бумагам;
- координацию расчета в розничных платежных системах, платежных системах для крупных сумм и системах по ценным бумагам.

Обычно развитие инфраструктуры подразумевает изменение технологической основы обработки и обмена информации и только потом — изменение процедур осуществления операций. Тем не менее во многих случаях улучшение платежной инфраструктуры может быть достигнуто за счет изменения структуры и содержания процедур.

Принцип расширения доступности розничных платежных услуг

Принцип расширения доступности розничных платежных услуг подчеркивает необходимость развития инфраструктуры розничного сегмента НПС с целью развития эффективных и безопасных платежных инструментов и услуг для индивидуальных потребителей, компаний и государственных органов.

Инициативы в области развития инфраструктуры розничных платежных систем могут быть направлены:

а) в части развития операционной инфраструктуры:

- на повышение доступности платежных инструментов,
- расширение номенклатуры стандартизованных платежных инструментов,
- повышение уровня безопасности платежных инструментов,
- совершенствование взаимодействия между операционными сетями и т.д.;

б) в части развития клиринговой и расчетной инфраструктуры:

- на совершенствование взаимосвязи региональных клиринговых систем,
- совершенствование механизмов клиринга на национальном уровне,
- внедрение интегрированных систем управления расчетными системами региональных отделений центрального банка,
- стандартизацию платежных инструментов и клиринговых процедур и т.д.

В частности, развитие инфраструктуры розничных платежных систем может включать:

- внедрение электронных технологий дистанционного доступа к счетам и услугам с помощью пластиковых карт, Интернета и мобильной связи;
- внедрение технологий электронного документооборота, включая технологии преобразования бумажных платежных инструментов в электронную форму;
- объединение или интеграцию операционных сетей на базе единых форматов платежных инструментов и процедур их обработки и т.д.

Необходимо отметить, что эффективное развитие инфраструктуры розничных платежных систем невозможно без одновременного развития институциональных механизмов, обеспечивающих взаимодействие между участниками розничных платежных систем, а также между платежными системами в рамках НПС. В частности, правовая база НПС должна давать возможность использования электронного документооборота, средств шифрования и удостоверения электронной подписи, обмена документов по публичным сетям и т.д. (основные вопросы построения и развития розничных платежных систем рассмотрены в параграфе 1.5 «Розничные платежные системы»).

Принцип развития платежных систем для крупных сумм

Принцип развития платежных систем для крупных сумм (ПСКС) нацелен на развитие таких систем в соответствии с потребностями участников финансового рынка и в соответствии с изменением требований к критичным по времени межбанковским платежам.

Появление данного принципа связано с тем, что ПСКС обычно используются для осуществления межбанковских переводов, причем среди этих переводов (по мере развития финансового рынка) растет доля платежей на крупные суммы по сделкам на финансовом рынке. Такие платежи, как правило, являются критичными по времени платежами, так как воздействуют на открытые денежные позиции финансовых институтов (особенно это касается открытых позиций внутрисдневной ликвидности).

Реализация принципа развития платежных систем для крупных сумм в соответствии с потребностями финансового рынка требует:

- сокращения времени окончательного расчета по платежам;
- реализации технологий поддержания и экономии ликвидности;
- обеспечения надлежащего уровня безопасности и конфиденциальности и т.д.

Основные вопросы построения и развития ПСКС рассмотрены в параграфе 1.4 «Платежные системы для крупных сумм».

Принцип совместного развития платежных систем и систем по ценным бумагам

Принцип совместного развития платежных систем и систем по ценным бумагам направлен на координацию процессов развития систем по ценным бумагам и ПСКС.

Системы по ценным бумагам обычно включают в себя целый ряд инфраструктурных единиц, в том числе следующие системы:

- заключение сделок по ценным бумагам;
- регистрация прав на ценные бумаги;
- управление счетами хранения ценных бумаг;
- клиринг требований по ценным бумагам и деньгам;
- расчет по денежным требованиям.

Причем системы по ценным бумагам и ПСКС обычно взаимозависимы, так как:

- ПСКС обычно используются для проведения платежей по сделкам, заключенным в системах по ценным бумагам;
- сделки с ценными бумагами в системах по ценным бумагам обычно используются для поддержания ликвидности финансовых институтов в ПСКС.

Все это приводит к необходимости постоянно координировать не только текущее функционирование систем по ценным бумагам и ПСКС, но и их совершенствование. Причем реализация принципа совместного развития двух систем требует (в части развития НПС):

- повышения уровня операционного взаимодействия;
- повышения уровня технической интеграции;
- повышения уровня устойчивости и непрерывности бизнеса и т.д.

Как правило, платежные системы для крупных сумм развиваются быстрее систем по ценным бумагам в силу большей потребности в таких системах. В связи с этим при проектировании систем по ценным бумагам необходимо встраиваться в существующую ПСКС, а также закладывать возможности взаимодействия систем при развитии ПСКС.

Принцип координации расчета в платежных системах

Принцип координации расчета в платежных системах направлен на координацию процессов расчета в розничных платежных системах, платежных системах для крупных сумм и системах по ценным бумагам.

В общем случае платежные процессы в этих платежных системах осуществляются по своему временному графику с использованием собственных механизмов поддержания ликвидности и управления рисками. В то же время они сильно взаимосвязаны, так как при оказании услуг участвуют одни и те же финансовые институты (в одних случаях — в качестве провайдеров услуг, в других — в качестве пользователей).

В связи с этим возникает целый ряд вопросов, которые могут быть решены за счет координации расчета в этих системах:

- экономии ликвидности за счет согласования временных графиков расчета;
- снижения риска за счет согласования механизмов управления рисками;
- снижения издержек за счет согласования бизнес-процессов расчета и т.д.

В частности, координация касается согласования операционных правил и стандартов расчетных систем с целью обеспечения сквозной обработки платежных инструкций; операционных часов платежных систем и рынков ликвидности; графиков операций на денежном рынке и переводов обеспечения по внутридневному кредиту; вопросов распределения рисков при сбое в работе одной из систем и т.д.

1.4. ПЛАТЕЖНЫЕ СИСТЕМЫ ДЛЯ КРУПНЫХ СУММ

Платежные системы для крупных сумм занимают центральное место в структуре национальных платежных систем, так как обеспечивают в денежном выражении основной объем платежных операций. По этой причине ПСКС относятся, как правило, к классу системно значимых платежных систем, а их операторами являются центральные банки.

Участниками ПСКС в большинстве случаев являются банки и другие крупные субъекты национального финансового рынка, причем окончательные расчеты между ними, как правило, осуществляются деньгами центрального банка (депозитными денежными средствами, хранящимися на счетах участников ПСКС в центральном банке) [7].

ПЛАТЕЖНЫЙ ПРОЦЕСС ПСКС

Платежный процесс ПСКС использует операционный, клиринговый и расчетный механизмы и при некотором упрощении может быть представлен в виде следующей последовательности действий:

- проверка условий безопасности;
- ввод платежных инструментов;
- проверка платежных инструментов;
- помещение платежных инструментов в очередь;
- обработка платежей в очереди в соответствии с алгоритмом ПСКС (на валовой основе, на основе неттинга (взаимозачета) и т.п.);
- проведение окончательного расчета;
- предоставление информации участникам ПСКС.

Проверка условий безопасности осуществляется при обращении участника ПСКС в систему за платежными услугами. Учитывая, что современные ПСКС, как правило, используют дистанционное обслуживание участников, в момент подключения участников к программно-аппаратному комплексу (ПАК) ПСКС с использованием публичных или частных сетей осуществляются идентификация и аутентификация участников, а также проверка их полномочий и доступных им сервисов.

При этом проверка условий безопасности осуществляется не только в первоначальный момент, при входе участника в систему, но и при наступлении некоторых других событий. Например, при возобновлении активности, при использовании сервисов (управление очередью, кредитование и т.п.), при осуществлении ошибочных действий и т.д.

Ввод платежных инструментов в систему обычно осуществляется дистанционно в одном из следующих режимов:

- одноразовый пакетный режим;
- многократный пакетный режим;
- режим реального времени.

ПСКС предыдущего поколения обычно использовали одноразовый или многократный пакетный режим ввода платежных инструментов, так как алгоритм обработки таких ПСКС основывался на одноразовом или многократном неттинге (взаимозачете).

Сегодня, когда ПСКС широко используют обработку платежей на валовой и гибридной основе, при вводе платежных инструментов в основном используется многократный пакетный режим и (или) режим реального времени (в зависимости от алгоритма работы интерфейса между корпоративным ПАК участника и ПАК платежной системы).

Проверка платежных инструментов по форме и содержанию (верификация) осуществляется на предмет соответствия структуры платежных инструментов и содержащихся в них данных национальному законодательству, принятым

стандартам и правилам ПСКС, а также на предмет непротиворечивости и полноты указанных данных.

Правила заполнения полей платежных инструментов обычно делятся на обязательные и рекомендованные. Нарушение обязательных правил является основанием для возврата (аннулирования) платежного инструмента без исполнения, а нарушение рекомендованных правил может повлиять на скорость обработки платежа, возможность использования тех или иных сервисов ПСКС, применение к платежам базовых (льготных) тарифов и т.п.

Заметим, что в рамках ПСКС обычно используется очень ограниченный набор платежных инструментов: в основном это кредитовый и дебетовый переводы, причем с огромным перевесом в пользу первого.

Помещение платежных инструментов в очередь платежей. Платежные инструменты, прошедшие верификацию, обычно помещаются для дальнейшей обработки в очередь платежей. При этом очередь платежей может иметь достаточно сложное устройство, зависящее от алгоритма работы ПСКС.

В частности, в рамках очереди платежей могут быть организованы подчиненные очереди (по участникам, по видам инструментов, по уровню приоритета и т.д.), причем по отношению к каждой такой очереди может предлагаться разный набор сервисов.

В простейшем случае, при одноразовом неттинге (взаимозачете) платежей, участники ПСКС обычно не имеют никаких рычагов воздействия на очередь (за исключением, возможно, повторного ввода пакета). Однако современные ПСКС, как правило, предоставляют широкий спектр услуг по управлению очередями, в том числе по изменению приоритета платежа, разбиению платежа на более мелкие, отзыву платежа из очереди и т.д.

Одним из последних достижений в этой области стал сервис по установлению индивидуальных и агрегированных лимитов на платежи, стоящие в очереди.

Обработка платежей в очереди платежей направлена на подсчет позиций участников ПСКС, необходимых для выполнения окончательного расчета, и осуществляется в соответствии с алгоритмом ПСКС. Как правило, могут использоваться:

- одноразовая обработка на валовой основе;
- обработка на базе одноразового неттинга (взаимозачета);
- обработка на базе многоразового неттинга (взаимозачета);
- непрерывная обработка на валовой основе;
- обработка на основе гибридного алгоритма.

Заметим, что во всех случаях обработка начинается с установления расчетных позиций участников равными остатками на счетах в расчетном банке. При этом сумма овердрафта, доступная каждому участнику, используется автоматически по мере необходимости.

В случае одноразовой обработки на валовой основе платежи обрабатываются один раз по окончании операционного дня, последовательно, в порядке установ-

ленной очереди, на двусторонней основе, путем увеличения расчетной позиции получателя средств и уменьшения позиции плательщика.

При этом могут использоваться как однопроходные, так и многопроходные алгоритмы. В первом случае очередь обрабатывается один раз, и все платежи, которые не могут быть исполнены из-за недостатка средств на счете, перемещаются в рамках очереди на несколько позиций назад (количество позиций зависит от используемого алгоритма). Во втором случае такие платежи пропускаются, а затем очередь обрабатывается повторно (фактически однопроходный алгоритм с перемещением платежа в конец очереди).

Обработка на базе неттинга (взаимозачета) использует сложные алгоритмы поиска групп взаимных платежей участников, которые в той или иной степени компенсируют друг друга без возникновения отрицательных расчетных позиций. В частности, могут использоваться алгоритмы:

- двустороннего (многостороннего) неттинга (взаимозачета);
- циклического (периодического) неттинга (взаимозачета);
- неттинга (взаимозачета) с полным (неполным) охватом очереди и т.д.

Естественно, все алгоритмы учитывают структуру очереди, в частности, в первую очередь обрабатываются платежи с более высоким приоритетом.

Заметим, что неттинг и взаимозачет несколько отличаются по методу формирования расчетных позиций: при неттинге увеличение (уменьшение) позиций осуществляется только на результирующую сумму по каждому участнику из группы, а в случае взаимозачета — на сумму каждого платежа каждого участника из группы.

Одноразовый неттинг (взаимозачет) обычно осуществляется один раз, по окончании операционного дня, а многоразовый — многократно в течение операционного дня и еще раз по окончании операционного дня. При этом многоразовый неттинг (взаимозачет) может осуществляться циклически, с непрерывным повторением циклов, каждый раз охватывая всю очередь или ее часть.

Непрерывная обработка на валовой основе осуществляется в течение операционного дня, причем платежи, которые приводят к отрицательным позициям, не выполняются, а перемещаются на некоторое количество позиций в конец очереди (количество позиций зависит от используемого алгоритма).

Наконец, гибридные алгоритмы используют совместную обработку и на валовой основе, и на основе неттинга (взаимозачета). Например, система может в течение операционного дня осуществлять обработку на валовой основе, а по окончании дня — на основе неттинга (взаимозачета). Или система сначала может пытаться обработать платежи на валовой основе, а если не получается — включается алгоритм неттинга (взаимозачета).

Проведение окончательного расчета осуществляется путем увеличения (уменьшения) остатков денежных средств на счетах участников ПСКС в расчетном банке в соответствии с данными о расчетных позициях, полученных на этапе обработки платежей в очереди.

Увеличение (уменьшение) остатков на счетах участников может осуществляться:

- на двусторонней основе, путем перевода денежных средств со счетов одних участников на счета других;
- через промежуточный счет расчетного банка, путем увеличения (уменьшения) остатков на счетах участников в корреспонденции с уменьшением (увеличением) остатка на промежуточном счете.

При этом отражение позиций на счетах в расчетном банке может осуществляться непосредственно после расчета позиций многократно в течение операционного дня или один раз после окончательного расчета позиций на валовой основе или на основе неттинга (взаимозачета) по завершении операционного дня.

Предоставление информации участникам осуществляется в соответствии с национальным законодательством и правилами ПСКС, которые могут определять время, формат, объем и способ передачи таких данных. При этом участники системы обычно получают не только данные об остатках и оборотах по счетам, но и электронные копии платежных документов, на основании которых такие обороты сформированы.

ХАРАКТЕРИСТИКИ ПСКС

Основными характеристиками ПСКС являются:

- момент безотзывности платежа;
- момент окончательности платежа;
- скорость обработки платежа;
- уровень кредитного риска;
- уровень издержек ликвидности;
- сервис поддержания ликвидности.

Момент безотзывности платежа характеризует момент времени, начиная с которого участник ПСКС не может отменить платеж. Момент безотзывности платежа обычно регулируется национальным законодательством и (или) правилами ПСКС и может определяться:

- моментом поступления платежа в ПСКС;
- моментом верификации платежа в ПСКС;
- моментом помещения платежа в очередь платежей;
- началом обработки платежа на основе неттинга (взаимозачета);
- началом обработки платежа на валовой основе.

Заметим, что при определенных обстоятельствах «безотзывный» статус платежа может измениться на «отзывный». Например, в некоторых ПСКС, использующих циклический неттинг (взаимозачет), участник ПСКС может отзываться платежи из очереди платежей. В этом случае на время обработки платежа на базе неттинга (взаимозачета) он становится безотзывным, но если неттинг (взаимозачет) не состоялся, платеж возвращается в очередь (активируется в очереди) и может быть отозван.

Момент окончательности платежа характеризует момент времени, когда наступают безотзывность и безусловность платежа. Этот момент может регулироваться национальным законодательством и (или) правилами ПСКС и обычно привязан к моменту завершения расчетов по платежу (но иногда может наступать раньше).

С моментом окончательности платежа связана другая характеристика — **скорость обработки платежа**, которая определяется периодом времени с момента поступления платежа в систему и до момента окончательного расчета по платежу.

Как правило, чем раньше наступает момент окончательности платежа, тем меньше возможность возникновения непредвиденных кредитных рисков в процессе расчетов. В связи с этим развитие ПСКС при прочих равных обстоятельствах обычно ориентировано на достижение более раннего момента окончательности платежа.

Долгое время ПСКС проектировались с условием, что окончательный расчет должен наступить не позднее начала следующего операционного дня после поступления в систему платежных инструментов, в связи с чем клиринг и расчеты могли осуществляться один раз в день, после окончания текущего операционного дня.

Однако по мере развития компьютерных систем появилась возможность существенно сократить время обработки платежной информации, и сегодня ПСКС предоставляют участникам платежных систем возможность осуществления платежей начиная от режима пакетной обработки один раз в день до режима онлайн.

Заметим, что скорость обработки платежей является одной из важнейших характеристик ПСКС, так как платежи на крупные суммы практически всегда критичны по времени. В соответствии с этим ПСКС считаются платежной системой не только для крупных сумм, но и для срочных платежей (в том числе на небольшие суммы).

Уровень кредитного риска определяется риском неисполнения участниками платежной системы своих обязательств по переводу денежных средств в связи с недостатком средств на счетах, а **уровень издержек ликвидности** — с издержками поддержания значительных остатков на счетах для завершения расчетов.

Как упоминалось выше, чем раньше наступает момент окончательности платежа, тем меньше возможность реализации непредвиденных кредитных рисков. Кроме того, если окончательные расчеты начинают осуществляться при меньшем остатке на счетах участников, то издержки ликвидности становятся меньше (причем они становятся еще меньше, если участники ПСКС могут финансировать свои счета за счет кредитования).

Таким образом, изменяя дизайн ПСКС за счет внедрения инфраструктурных и институциональных инноваций, можно изменять в лучшую сторону баланс между совокупными рисками и издержками ликвидности.

В зависимости от алгоритма работы платежной системы к участникам ПСКС могут предъявляться разные требования по поддержанию остатков на счетах.

Самые жесткие требования к величине остатка на счете предъявляют системы валовых расчетов, в которых платежи осуществляются по очереди, в порядке поступления, без применения механизмов неттинга (взаимозачета).

В то же время в таких системах можно существенно снизить кредитный риск, оставив без исполнения платежи, для которых остаток средств на счете оказался недостаточным. При этом платежи, оставшиеся без исполнения, могут быть либо аннулированы, либо повторно поставлены в очередь платежей.

Существенно более мягкие требования к величине остатка средств на счете предъявляют системы платежей на базе неттинга (взаимозачета), когда суммы платежей со счета могут компенсироваться суммами платежей, зачисляемых на счет. При этом чем больше сумм участвует в неттинге (взаимозачете) (чем реже окончательный расчет), тем меньше требования к остатку на счете.

Однако при попытке окончательного расчета по результатам неттинга (взаимозачета) может выясниться, что на счетах одного или нескольких участников недостает средств, что вызовет невозможность окончательного расчета.

Сервис поддержания ликвидности может включать:

- возможность пополнения счета;
- возможность получения кредита;
- возможность управления очередью платежей.

Возможность пополнения счета позволяет участникам ПСКС оперативно пополнять счета в ходе операционного дня ПСКС (в любой момент или в заданные периоды времени) до момента окончательного расчета, с тем чтобы он реально состоялся.

Такой сервис относительно легко реализовать, если оператор платежной системы одновременно выступает в качестве расчетного банка, и трудно, если это разные субъекты национальной платежной системы (особенно, если окончательный расчет осуществляется в деньгах центрального банка).

Возможность получения кредита для завершения расчетов является сервисом, который широко распространен среди ПСКС. Как правило, кредит предоставляется автоматически, в форме овердрафта и может различаться:

- а) по сроку кредитования:
 - внутридневной, до окончания текущего операционного дня (intraday),
 - до начала следующего операционного дня (overnight),
 - на более длительный срок;
- б) по форме обеспечения:
 - необеспеченный, в пределах лимита,
 - под залог ценных бумаг, в пределах лимита,
 - под залог ценных бумаг, сверх лимита.

Внутридневной intraday-кредит предоставляется для обеспечения окончательного расчета в течение операционного дня и автоматически погашается (при наличии средств на счете) или при недостатке средств на счете переходит в кредит на более длительный срок (обычно вида overnight) по окончании операционного дня.

Кредит вида *overnight* предоставляется для обеспечения расчетов по итогам клиринга платежных инструментов, если он осуществляется по завершении операционного дня, либо для переоформления кредита вида *intraday* при недостатке средств на счете.

Возможность управления очередью платежей (если такой сервис предоставляет ПСКС) используется для изменения последовательности обработки платежей (путем изменения приоритетов платежей или очередности платежей в рамках заданного приоритета) или для расщепления крупного платежа на несколько более мелких.

Такой сервис может применяться для поддержания ликвидности участника ПСКС, если окончательные расчеты по платежам осуществляются непрерывно или периодически в течение операционного дня ПСКС.

ОСНОВНЫЕ ВИДЫ ПСКС

К основным видам ПСКС относятся:

- системы отложенных нетто-расчетов;
- системы валовых расчетов в реальном времени;
- гибридные платежные системы.

Системы отложенных нетто-расчетов (СОНР) были доминирующей формой ПСКС в 1980-х гг. В таких системах ввод платежных инструментов осуществляется на основе пакетной передачи, обработка платежей — на основе одноразового неттинга (взаимозачета) по окончании операционного дня, а расчет по результирующим суммам позиций — один раз по окончании неттинга (взаимозачета).

Так как в рамках СОНР окончательные расчеты проводятся в соответствии с итоговыми расчетными позициями, требования к остаткам на счетах участников (а следовательно, и издержки ликвидности) минимальны.

В то же время окончательность расчета в таких системах наступает поздно, в конце дня, поэтому кредитный риск в таких системах достаточно высок: недостаток средств на счете одного участника системы способен по цепочке привести к риску последующего невыполнения обязательств другими участниками.

Системы валовых расчетов в реальном времени (СВРРВ или RTGS¹) были созданы почти в каждой стране в 1990-х гг. В таких системах:

- ввод платежных инструментов может осуществляться как в многоканальном пакетном режиме, так и в режиме реального времени;
- обработка платежей осуществляется на валовой основе, непрерывно в течение операционного дня;
- окончательный расчет по каждому платежу осуществляется непосредственно после его обработки.

В связи с этим при наличии достаточного количества денежных средств на счете (или доступности соответствующего кредита) окончательность платежа в таких

¹ RTGS — Real Time Gross Settlement System.

системах наступает практически сразу после ввода платежного инструмента в систему, т.е. в режиме реального времени, что сводит кредитный риск к минимуму.

Естественно, недостатком СВРРВ является потребность в существенно большем остатке на счете в расчетном банке (или в большем кредите), чем в режиме СОНР.

Гибридные платежные системы (ГПС) появились в связи с необходимостью снижения требований к остаткам на счетах, которые предъявляли СВРРВ. Они стали результатом развития СВРРВ на основе заимствования некоторых особенностей СОНР.

Сначала в платежный процесс СВРРВ были встроены процедуры неттинга (взаимозачета), которые стали выполняться несколько раз в течение операционного дня. В таких системах платежи помещаются в централизованную очередь, и их неттинг (взаимозачет) осуществляется через определенные промежутки времени. Причем, если по итогам неттинга (взаимозачета) нет отрицательных расчетных позиций, окончательный расчет по платежам производится немедленно.

С одной стороны, по сравнению с СВРРВ такие системы уменьшают потребность в ликвидности за счет неттинга (взаимозачета), а с другой — по сравнению с СОНР снижают риск, связанный с расчетами, обеспечивая окончательный расчет по итогам каждого цикла неттинга (взаимозачета).

Затем в ГПС были объединены функции неттинга (взаимозачета) с расчетами в реальном времени. В результате ГПС сначала стремится произвести платеж на валовой основе, а если это невозможно вследствие недостаточности средств на счете, то проверяет возможность осуществления взаимозачета одного или нескольких двусторонних или многосторонних платежей. При этом используются различные методы оптимизации: относительно простые двусторонние алгоритмы применяются в режиме реального времени, более сложные многосторонние — периодически, через короткие промежутки времени.

1.5. РОЗНИЧНЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ

Розничные платежные системы (РПС) наряду с платежными системами для крупных сумм составляют основу НПС каждого государства. Они обеспечивают использование денег как средства обмена при розничных сделках, и от того, насколько эффективно и безопасно функционируют такие системы, зависит доверие граждан государства ко всей НПС.

В отличие от платежных систем для крупных сумм розничные платежные системы нацелены на обработку платежей среднего и малого размера, причем таких платежей, которые не столь критичны по времени исполнения.

По количеству операций объем платежей в розничных платежных системах обычно существенно превышает объем платежей в платежных системах для крупных сумм, однако в денежном выражении ситуация прямо противоположная.

Розничные платежные системы имеют и другие особенности. По сравнению с платежными системами для крупных сумм в РПС обычно наблюдается:

- большее количество участников;
- большой набор платежных инструментов;
- в большей степени используются услуги частных провайдеров.

В частности, в розничных платежных системах используются не столько кредитовые и дебетовые переводы (это типично для платежных систем для крупных сумм), сколько кредитные и дебетовые платежные карты, чеки и электронные деньги. Причем последние используются не только как электронные кошельки и электронные бумажники, но и более традиционным образом: как виртуальные счета, расчеты по которым осуществляются с использованием других платежных инструментов.

Платежный процесс в розничных платежных системах более строго структурирован с точки зрения инфраструктурных механизмов и обычно включает три подчиненных взаимосвязанных процесса (каждый подчиненный процесс соответствует реализации соответствующего инфраструктурного механизма):

- операционный процесс;
- клиринговый процесс;
- расчетный процесс.

Как правило, три указанных процесса разворачиваются с некоторым временным сдвигом относительно друг друга, причем величина сдвига зависит от используемых платежных инструментов, механизмов инфраструктуры и правил платежной системы.

На рисунке 1.2 представлена схема, приведенная КПРС в работе [1], с условным изображением потоков информационных и платежных инструкций между сторонами, участвующими в переводе денежных средств в рамках розничной платежной системы: плательщиком, финансовым институтом плательщика, получателем и финансовым институтом получателя.

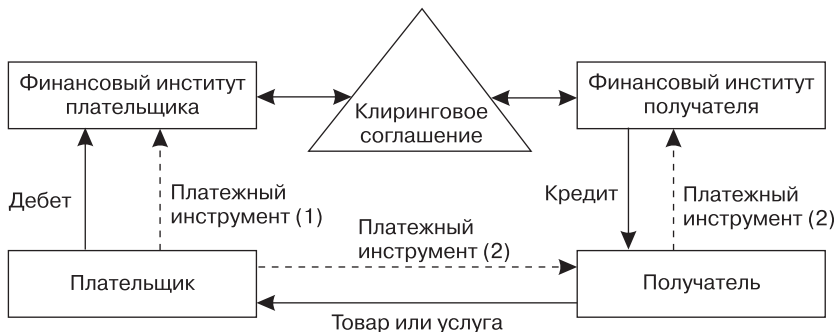


Рис. 1.2. Схема потоков информационных и платежных инструкций между сторонами, участвующими в переводе денежных средств

На схеме показаны два типа платежных инструментов, которые используются при осуществлении переводов денежных средств. В случае (1) используется кредитовый платежный инструмент, который представляется плательщиком в финансовый институт плательщика (например, кредитовый перевод); в случае (2) используется дебетовый платежный инструмент, который представляется получателем в финансовый институт получателя.

Обмен указанными платежными инструментами между финансовыми институтами плательщика и получателя средств осуществляется в рамках клирингового соглашения (взаимодействие между финансовыми институтами в рамках расчетного соглашения на схеме не показано).

ОПЕРАЦИОННЫЙ ПРОЦЕСС

Операционный процесс розничной платежной системы обеспечивает инициирование, подтверждение и перевод платежа. В общем случае операционный процесс включает [1]:

- проверку подлинности сторон, участвующих в операции;
- подтверждение правильности оформления платежного инструмента;
- проверку платежеспособности плательщика;
- авторизацию перевода денежных средств финансовыми институтами плательщика и получателя;
- передачу информации финансовым институтом плательщика в финансовый институт получателя;
- проведение операции.

В каждом конкретном случае состав и последовательность операционного процесса могут различаться в зависимости от используемого платежного инструмента и платежной инфраструктуры (платежная инфраструктура специфична для каждой конкретной розничной платежной системы).

Проверка подлинности сторон, участвующих в операции, осуществляется путем применения специальных процедур идентификации и аутентификации пользователей. Например, при выполнении платежей с помощью платежной карты идентификация пользователя может осуществляться на основе реквизитов, эмбоссированных на пластике карты, а аутентификация — с помощью процедуры ввода и верификации ПИН-кода.

Подтверждение правильности оформления платежного инструмента заключается в проверке соответствия формы и содержания платежного инструмента некоторым заранее установленным стандартам. Например, в случае чека это может быть проверка соответствия структуры чека заданному стандарту, а также проверка правильности заполнения полей чека. При этом проверка, как правило, осуществляется с использованием тех или иных средств автоматизации.

Проверка платежеспособности плательщика включает проверку достаточности средств на счете плательщика, а при недостатке средств — проверку нали-

чия неиспользованных лимитов кредитования для покрытия недостающей суммы. В зависимости от вида платежного инструмента такая проверка может проводиться как непосредственно после представления платежного инструмента провайдеру услуг (например, при представлении плательщиком в банк кредитового перевода), так и существенно позже (например, после получения чека банком чекодателя).

Авторизация перевода денежных средств финансовыми институтами плательщика и получателя представляет собой одобрение соответствующих платежных инструкций, которое обуславливает их направление на исполнение.

Передача информации финансовым институтом плательщика в финансовый институт получателя представляет собой передачу авторизованных платежных инструкций и иной информации (необходимой в соответствии с правилами платежной системы).

Проведение операции включает осуществление в рамках операционного процесса процедур, необходимых для перевода денежных средств (также определяются правилами платежной системы).

Заметим, что передача информации финансовым институтом плательщика в финансовый институт получателя, а также действия по проведению операции осуществляются не только в рамках операционного процесса, но и в рамках других процессов (клирингового и расчетного). Причем далеко не всегда можно точно сказать, какие действия относятся к какому процессу.

В документах КПРС различаются две разновидности аутентификации и авторизации:

- 1) немедленные аутентификация и авторизация: выполняются финансовыми институтами плательщиков в начале операционного процесса;
- 2) отложенные аутентификация и авторизация: выполняются финансовыми институтами плательщиков в конце операционного процесса по запросу финансового института получателя, обрабатывающего платежную информацию.

Немедленные аутентификация и авторизация выполняются, например, при кредитовых переводах и платежах с использованием карт.

В частности, при кредитовых переводах финансовый институт плательщика устанавливает личность плательщика и достаточность средств на его текущем счете непосредственно после получения платежных инструкций, а затем направляет необходимую информацию финансовому институту получателя. При этом аутентификация и авторизация кредитовых переводов могут выполняться как в электронном виде (путем автоматической проверки электронной цифровой подписи и ввода уполномоченным лицом установленных компьютерных команд), так и путем обработки документа на бумажном носителе (проверка личности и окончательное согласие на перевод осуществляются посредством проверки и проставления подписей на операционном документе).

При операциях с платежными картами аутентификация и авторизация в большинстве случаев происходят автоматически, путем соединения терминала в точке продажи (POS) или банкомата с финансовым институтом, участвующим

в операции (либо с организацией, которой финансовый институт поручил осуществление таких операций) в режиме реального времени. При этом используется телекоммуникационный и компьютерный обмен информацией о карте и счете между торговой точкой и финансовым институтом держателя карты (либо вышеупомянутой организацией).

Отложенные аутентификация и авторизация выполняются, например, при прямом дебетовании и платежах с использованием чеков.

При прямом дебетовании финансовый институт плательщика получает платежный документ от получателя средств или от его финансового института, причем авторизацию платежа он осуществляет после получения согласия (акцепта) плательщика, которое может быть предоставлено как предварительно, так и по запросу финансового института.

В случае платежа с использованием чека финансовый институт плательщика также получает платежный документ от получателя средств или от его финансового института, причем авторизацию платежа он осуществляет на основании информации о достаточности средств на чековом счете.

ПРОЦЕСС КЛИРИНГА

Клиринговый процесс розничной платежной системы обеспечивает обмен платежными инструментами и другой необходимой платежной информацией между финансовыми институтами плательщика и получателя, а также вычисление платежных требований, необходимых для проведения расчета.

Обмен платежными инструментами или платежной информацией в рамках клирингового процесса состоит из нескольких шагов:

- сверка операций;
- сортировка операций;
- сбор и проверка данных;
- агрегирование данных;
- отправка информации.

Как и в случае операционного процесса, перечень шагов может значительно различаться в зависимости от характеристик платежных инструментов.

Процедуры вычисления требований для проведения расчета могут включать вычисления требований на валовой основе и (или) на агрегированной основе (на основе неттинга).

Результатом процесса вычисления требований является полностью обработанный и готовый к проведению расчета платеж, включая подтверждение требования института получателя к институту плательщика.

КПРС выделяет четыре типа клиринговых механизмов:

1) внутренний клиринговый механизм, в рамках которого обмен информацией и вычисление клиринговых позиций осуществляются в рамках одного финансового института (в котором ведутся дебетуемые и кредитуемые счета);

2) двусторонний клиринговый механизм, в соответствии с которым сортировка и обработка платежей между двумя финансовыми институтами производятся самими институтами;

3) трехсторонний клиринговый механизм, когда финансовые институты привлекают для клиринга третий финансовый институт, известный как корреспондент (как правило, такие корреспонденты предоставляют свои услуги другим финансовым институтам на основе двусторонних договоров);

4) многосторонний клиринговый механизм, организуемый специальным клиринговым институтом, в ходе которого финансовые институты по единым правилам представляют данные и обмениваются ими и (или) документами, связанными с переводом денежных средств.

В последнем случае в качестве клирингового института могут выступать клиринговая палата, клиринговая ассоциация и т.п. Клиринговая палата, управляющая централизованным механизмом клиринга, при расчете платежных обязательств (в рамках многостороннего неттингового соглашения) выступает также в качестве центрального контрагента. Клиринговые ассоциации обычно не располагают обрабатывающими мощностями и не выступают при расчете в качестве центрального контрагента.

Наряду с четырьмя базовыми клиринговыми механизмами могут использоваться комбинации из базовых механизмов. Например, корреспондент в трехстороннем клиринговом механизме может передавать платежные инструкции в клиринговую палату от имени своих клиентов (финансовых институтов). Другим примером является перекрестное членство финансовых институтов в клиринговых палатах, когда член одной клиринговой палаты может выступать в качестве корреспондента для членов другой палаты. Кроме того, клиринговая палата сама может быть членом другой клиринговой палаты или участвовать в соглашении об обмене с другими клиринговыми палатами.

Многосторонний клиринговый механизм считается наиболее эффективным механизмом обработки большого количества платежей. Во-первых, за счет координации обмена платежными инструкциями, а также использования коммуникационных сетей и процессинговых центров можно существенно повысить эффективность обработки платежных инструкций. Во-вторых, в рамках многостороннего клирингового механизма можно использовать механизм многостороннего неттинга, что позволяет участникам клирингового процесса существенно минимизировать ликвидность, необходимую для расчета.

ПРОЦЕСС РАСЧЕТА

Расчетный процесс розничной платежной системы обеспечивает исполнение финансовыми институтами плательщика платежных требований финансовых институтов получателей посредством отражения позиций, вычисленных в результате клирингового процесса, на расчетных счетах финансовых институтов.

В общем случае процесс расчета включает следующие шаги:

- сбор предназначенных для проведения расчета платежных требований и проверку их подлинности;
- проверку достаточности для расчета денежных средств на расчетных счетах финансовых институтов;
- урегулирование требований между финансовыми институтами посредством отражения денежных сумм на расчетных счетах;
- регистрацию информации о результатах расчетного процесса и передачу данной информации заинтересованным финансовым институтам.

При этом используются следующие виды расчетных счетов:

- корреспондентские счета, которые финансовые институты ведут друг у друга;
- корреспондентские счета, которые финансовые институты ведут в третьем финансовом институте, выступающем в качестве расчетного банка.

Финансовый институт, который имеет расчетный счет в другом финансовом институте и рассматривает остаток денежных средств на этом счете в качестве актива, называет этот счет счетом НОСТРО, а финансовый институт, предоставляющий расчетный счет и рассматривающий остаток на этом счете в качестве своего обязательства, называет его счетом ВОСТРО¹. При наличии такого счета два указанных финансовых института, связанные двусторонним клиринговым соглашением, могут осуществить расчет путем отражения на данном счете результатов клиринга.

Многосторонний клиринговый механизм обычно подразумевает наличие расчетного банка, в котором ведутся индивидуальные расчетные счета участников клирингового соглашения. Информация об остатках на этих счетах обычно используется в процессе клиринга, а сами счета используются для отражения расчетных обязательств по итогам клиринга.

Как отмечалось выше, в платежных системах для крупных сумм расчет, как правило, производится деньгами центрального банка. В розничных платежных системах расчет может производиться деньгами как коммерческого финансового института, так и центрального банка. В последнем случае доступ к расчетным счетам центрального банка может быть предоставлен либо всем прямым участникам клиринговых соглашений, либо ограниченному кругу институтов, которые отвечают установленным требованиям. Причем финансовые институты, не имеющие счетов в центральном банке, производят расчет по своим платежам на балансе прямого участника, имеющего счет в центральном банке.

Платежные системы для крупных сумм и розничные платежные системы являются основными платежными системами любой НПС. Но наряду с ними в рам-

¹ В России вместо термина ВОСТРО часто используется термин ЛОРО, хотя в международной практике счет ЛОРО — это обычно счет третьего банка в банке-корреспонденте данного финансового института.

ках НПС существуют и другие виды платежных систем: платежные системы для ценных бумаг, платежные системы для производных финансовых инструментов, платежные системы на рынке Forex и др. Всем им КПРС также уделяет значительное внимание, что отражено в его публикациях.

Кроме того, большое внимание в публикациях КПРС уделяется вопросам политики центральных банков в области платежных систем, наблюдения за платежными и расчетными системами, управления рисками в платежных и расчетных системах и т.д. И хотя выше эти вопросы подробно не обсуждались, все они имеют большое значение для стабильного и эффективного функционирования НПС.

Приложение к главе 1

Перечень основных публикаций КПРС БМР

1. Clearing and settlement arrangements for retail payments in selected countries. CPSS BIS, September, 2000 / Пер.: Механизмы клиринга и расчета розничных платежей в некоторых странах. ЦБ РФ // Платежные и расчетные системы. 2008. Вып. 13.

2. Core Principles for Systemically Important Payment Systems. CPSS BIS, January, 2001 / Пер.: Ключевые принципы для системно значимых платежных систем. ЦБ РФ // Платежные и расчетные системы. 2010. Вып. 23.

3. Recommendations for securities settlement systems. CPSS BIS, November, 2001 / Пер.: Рекомендации для систем расчета по ценным бумагам. ЦБ РФ // Платежные и расчетные системы. 2008. Вып. 8.

4. A glossary of terms used in payments and settlement systems. CPSS BIS, March, 2003 / Пер.: Глоссарий терминов, используемых в платежных и расчетных системах. ЦБ РФ // Платежные и расчетные системы. 2007. Вып. 1.

5. Policy issues for central banks in retail payments. CPSS BIS, March, 2003 / Пер.: Политика центральных банков в области розничных платежей. ЦБ РФ // Платежные и расчетные системы. 2008. Вып. 5.

6. Survey of developments in electronic money and internet and mobile payments. CPSS BIS, March, 2004 / Пер.: Обзор новаций в области электронных денег и платежей, совершаемых с использованием мобильных средств связи и Интернета. ЦБ РФ // Платежные и расчетные системы. 2008. Вып. 6—7.

7. New developments in large-value payment systems. CPSS BIS, May, 2005 / Пер.: Новые разработки в платежных системах для крупных сумм. ЦБ РФ // Платежные и расчетные системы. 2008. Вып. 4.

8. Central bank oversight of payment and settlement systems. CPSS BIS, May, 2005 / Пер.: Наблюдение центрального банка за платежными и расчетными системами. ЦБ РФ // Платежные и расчетные системы. 2007. Вып. 2.

9. General guidance for national payment system development. CPSS BIS, January, 2006 / Пер.: Общее руководство по развитию национальной платежной системы. ЦБ РФ // Платежные и расчетные системы. 2008. Вып. 3.

10. General principles for international remittance services CPSS BIS, January, 2007 / Пер.: Общие принципы оказания услуг по международным переводам денежных средств. ЦБ РФ // Платежные и расчетные системы. 2008. Вып. 10.

11. The interdependencies of payment and settlement systems. CPSS BIS, June, 2008 / Пер.: Взаимозависимости платежных и расчетных систем. ЦБ РФ // Платежные и расчетные системы. 2008. Вып. 14.

12. Payment, clearing and settlement systems in the CPSS countries — Volume 1. CPSS BIS, September 2011 / Пер. (частично): Платежные, клиринговые и расчетные системы России. ЦБ РФ // Платежные и расчетные системы. 2011. Вып. 29.

ГЛАВА 2

НАЦИОНАЛЬНЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ И SWIFT

2.1. ИСПОЛЬЗОВАНИЕ SWIFT В НАЦИОНАЛЬНЫХ ПЛАТЕЖНЫХ СИСТЕМАХ

Создание современных национальных платежных систем, позволяющих контролировать финансовые и расчетные риски, особенно при проведении крупных платежей, является одной из главных задач, стоящих перед национальными банками. Комитет по платежным и расчетным системам Банка международных расчетов, о деятельности которого было подробно рассказано в предыдущей главе, организовал Рабочую группу с целью разработки принципов, которые должны лежать в основе структуры и функционирования платежных систем во всех странах. Банк России активно участвует в работе Комитета по платежным и расчетным системам и является членом Рабочей группы по принципам и практическим аспектам создания платежных систем. Итогом деятельности Рабочей группы стала публикация рекомендаций Банка международных расчетов «Ключевые принципы для системно значимых платежных систем».

В данном документе подчеркивается роль центрального банка при организации национальной системы расчетов, которая состоит в том числе в определении необходимых параметров платежной системы, обеспечения ее функционирования, совершенствования и развития. Международный опыт показывает, что важную роль при практической реализации национальных платежных систем играет SWIFT¹ как инфраструктура, обеспечивающая гарантированную быструю и качественную доставку сообщений.

Созданное в 1973 г. кооперативное сообщество SWIFT является ведущим международным объединением в сфере передачи финансовых сообщений. В настоящее время пользователями SWIFT являются более 9000 крупнейших банков (включая

¹ SWIFT (Society for Worldwide Interbank Financial Telecommunication) — Сообщество всемирных интербанковских финансовых телекоммуникаций.

центральные (национальные) банки), финансовых организаций (инвестиционные компании, брокерские фирмы, биржи, депозитарии) и ведущих корпораций из 209 стран. Ежедневно по сети SWIFT передается около 15 млн сообщений.

Причинами столь широкого использования сети SWIFT являются следующие особенности.

Надежность. SWIFT принимает на себя финансовую ответственность за точную, полную и своевременную доставку сообщений. Ни одна другая организация, предоставляющая сеть для передачи данных, не может этого гарантировать. Справедливости ради следует отметить, что за время существования сеть SWIFT ни разу не была взломана.

Безопасность. Комбинирование физических и логических мер безопасности, а также применение различных видов шифрования исключают возможность изменения сообщения в процессе его передачи по сети SWIFT. Никому, кроме отправителя и получателя сообщения, не доступно его содержание.

Скорость. Доставка сообщений производится за несколько секунд, причем проверка и подтверждение подлинности осуществляются полностью автоматически.

Эффективность. Стандарты и технология SWIFT предоставляют возможность создавать прикладные программы для автоматической обработки сообщений. Благодаря этому увеличивается производительность и уменьшаются затраты на ручную обработку сообщений. Кроме того, финансовые организации могут использовать один и тот же комплекс связи SWIFT для обмена внутренними и международными сообщениями, таким образом создавая «единое окно» для всех потоков сообщений. Сервисные центры обеспечивают пользователям круглосуточную специализированную поддержку семь дней в неделю (в том числе на русском языке). SWIFT предоставляет также специальное оборудование и программное обеспечение для работы в сети.

Рентабельность. Помимо расчетов с крупнейшими иностранными банками технологии SWIFT позволяют кредитным учреждениям организовать автоматизированную и безопасную связь, использующую все возможности сети SWIFT, для своих филиалов и дочерних банков. В связи с этим при подключении к SWIFT пользователи получают в свое распоряжение надежную, защищенную и высокоэффективную финансовую сеть, позволяющую существенно снизить расчетные и финансовые риски, удешевить стоимость сообщений и расширить спектр услуг для своих клиентов.

Международное сообщество SWIFT создало высоконадежную сеть передачи финансовой информации, гарантирующую точную и оперативную ее доставку, с документальным подтверждением времени отправления и получения. При этом SWIFT принимает на себя финансовую ответственность за идентичность, безопасность и своевременность доставки финансовых сообщений.

На базе SWIFT реализованы системы платежей и расчетов более 50 стран мира, в том числе системы всех стран Евросоюза, а также такие инфраструктур-

ные проекты, как Европейская система трансграничных платежей TARGET, мировая валютообменная система CLS и др.

Принципиально важно, что из входящих в «Большую семерку» промышленно развитых стран мира пять государств — Великобритания, Германия, Италия, Канада и Франция — построили национальные платежные системы на базе сети SWIFT. В то же время среди стран, выбравших SWIFT в качестве инфраструктуры для реализации платежной системы, есть и такие, которые относительно недавно создали собственную расчетную сеть: Босния и Герцеговина, Латвия, Хорватия. Отдельно следует отметить Азербайджан — первую страну СНГ, создавшую национальную платежную систему на основе SWIFT.

Центральный банк РФ и Федеральная резервная система США выбрали несколько иной путь. В этих странах SWIFT в национальной платежной системе RTGS будет использоваться в качестве параллельного канала наряду с расчетной сетью регулятора. Применительно к России это означает, что коммерческие банки смогут выбирать, каким образом осуществлять взаимодействие в системе банковских электронных срочных платежей (БЭСП) — через расчетную сеть Банка России или через сеть SWIFT.

Разработанный Банком России подход — использование двух каналов доступа — существенно повышает устойчивость и эффективность системы БЭСП. Как и при использовании расчетной сети Банка России, при задействовании SWIFT для организации доступа в БЭСП кредитным организациям не придется делать дополнительных капиталовложений для участия в системе. Они смогут использовать уже существующий у них комплекс SWIFT как для участия в национальной системе RTGS, так и для расчетов на основе прямых корреспондентских отношений, межфилиальных расчетов и расчетов с клиентами. Таким образом повышается окупаемость уже действующего комплекса SWIFT в финансовой организации.

Применение форматов и сети SWIFT в БЭСП позволит использовать уже существующие современные высокотехнологичные решения в области платежных и расчетных систем, основанные на принципах надежности, транспарентности и безопасности. Это обеспечит при необходимости возможность интеграции российской платежной системы в международные платежные и расчетные системы.

Система БЭСП Банка России обеспечивает многократный рост оборачиваемости денежных средств, повышает эффективность управления ликвидностью и способствует минимизации рисков участников расчетов. Использование международных стандартов и инфраструктуры SWIFT в БЭСП позволит российским банкам эффективно использовать имеющуюся у них инфраструктуру, а для иностранных инвесторов создаст четкие и понятные правила осуществления расчетов.

Это обеспечит выход России на качественно новый уровень развития, характеризующийся устойчиво растущей экономикой, эффективной и современной

платежной системой. Таким образом, совершенствуемая Банком России система БЭСП повысит конкурентоспособность российской экономики и будет содействовать увеличению роста ВВП России, как это наблюдалось в других странах при реализации аналогичных проектов.

Кроме того, поскольку национальные (центральные) банки стран — участниц Таможенного союза и ЕврАзЭС являются членами SWIFT, можно использовать инфраструктуру SWIFT для интеграции экономического пространства СНГ. Создание трансграничной системы платежей TARGET было осуществлено Европейским союзом именно на основе сети SWIFT в силу рентабельности и эффективности данного решения.

2.2. СТАНДАРТЫ SWIFT

Реализованные SWIFT концепция, форматы и правила передачи финансовой информации приобрели статус общепринятого международного стандарта. SWIFT является уполномоченным органом Международной организации по стандартизации (ISO) по ведению стандартов ISO 9362 (Банковские идентификационные коды BIC), ISO 13616 (международный код банковского счета IBAN), ISO 15022 (Сообщения рынков ценных бумаг), ISO 20022 (Словарь финансовых терминов) и др. Стандарты SWIFT были разработаны финансовыми организациями — членами сообщества SWIFT совместно с Международной организацией по стандартизации (ISO¹), Международной торговой палатой (ICC²), Организацией по промышленной стандартизации торговых коммуникаций (ISITC³) и другими международными объединениями. На протяжении более четырех десятилетий стандарты SWIFT непрерывно развиваются, отражая все потребности современного электронного финансового документооборота.

Финансовые сообщения SWIFT подразделяются на следующие категории.

0. Системные сообщения.
 1. Клиентские переводы и чеки.
 2. Переводы финансовых организаций.
 3. Рынки денежных средств — форекс, депозиты и производные.
 4. Инкассо и кассовые письма.
 5. Рынки ценных бумаг.
 6. Драгоценные металлы и синдицирование.
 7. Аккредитивы и гарантии.
 8. Дорожные чеки.
 9. Управление денежными средствами и статус клиента.

¹ International Organization for Standardization.

² International Chamber of Commerce.

³ Industry Standardization for Institutional Trade Communication.

Внутри каждой категории насчитывается установленное число стандартизированных типов сообщений, сформированных на основе требований рынка, — каждому из этих сообщений соответствует определенная финансовая операция.

Сообщение любого типа состоит из заголовка, текста и трейлера. Заголовок и трейлер образуют так называемый конверт для пересылки сообщения и используются для управления системой и маршрутизации сообщений. В заголовке указываются идентификаторы получателя и отправителя, коды защиты и контроля, а также код-идентификатор самого сообщения и его приоритет. В трейлере ставятся код аутентификации и различные предупреждения для получателя. Использование заголовков и трейлеров позволяет осуществлять установку очередности сообщений, обеспечивать гарантированную доставку сообщения и получения подтверждения о получении, хранение сообщений в архиве.

Текст сообщения строго регламентирован и состоит из полей, каждое из которых обозначено двузначным цифровым кодом. Информация заносится в поля в определенной для каждого поля последовательности, при этом существуют обязательные и необязательные поля для заполнения.

Унификация не ограничивается применением стандартов для финансовых сообщений: стандарты SWIFT подразумевают использование кодов BIC¹ (стандарт ISO 9362), BEI² и IBAN³ (стандарт ISO 13616) — идентификаторов финансовых учреждений, нефинансовых организаций и счета клиента соответственно. Кроме того, при обмене данными используются коды ISO для обозначения стран (ISO 3166) и валют (ISO 4217).

Основным сервисом хранения и передачи сообщений в сети SWIFT является сервис FIN. Данный сервис предоставляет финансовым организациям большой выбор типов сообщений для быстрой и защищенной передачи информации по финансовым транзакциям и расчетам. Сообщения определяются трехзначным номером, отражающим общую сферу использования (категория), функцию (группу) и конкретные детали (формат). Например, клиентский перевод обозначается MT 103. Защищенные передача, доставка и хранение сообщений, шифрование данных внутри сети SWIFT, а также проверка сообщений на подлинность обеспечивают конфиденциальность, целостность и подлинность сообщений сервиса FIN. Сервис FIN используют все российские банки, подключенные к SWIFT.

В соответствии с требованиями времени SWIFT уделяет большое внимание обеспечению требований по противодействию легализации доходов, полученных преступным путем, и финансированию терроризма (Anti Money Laundering). Для этого используется специальное программное обеспечение, работающее со списками FATF⁴ и др.

¹ Bank Identifier Codes — банковский идентификационный код.

² Business Entity Identifier — идентификатор юридического лица.

³ International Bank Account Number — международный номер банковского счета.

⁴ Financial Action Task Force — Группа разработки финансовых мер борьбы с отмыванием капиталов.

2.3. ИСПОЛЬЗОВАНИЕ SWIFT В РОССИИ

На 1 января 2011 г. пользователями SWIFT являются более 540 ведущих кредитных и финансовых учреждений и корпораций. География пользователей охватывает 69 городов в девяти временных зонах России. Таким образом, в настоящее время в SWIFT представлена практически половина российских кредитных организаций, являющихся крупнейшими финансовыми институтами и осуществляющих более 80% расчетов в стране.

По количеству пользователей SWIFT Россия занимает второе место в мире, уступая по данному показателю только США. Крупнейшим пользователем SWIFT в Российской Федерации является Сбербанк России, который входит в первую сотню лидеров по трафику SWIFT в мире (во второй сотне — Банк ВТБ).

Количество российских пользователей SWIFT

| Год | Количество пользователей | Год | Количество пользователей |
|------|--------------------------|------|--------------------------|
| 1995 | 229 | 2003 | 389 |
| 1996 | 255 | 2004 | 413 |
| 1997 | 250 | 2005 | 448 |
| 1998 | 247 | 2006 | 475 |
| 1999 | 256 | 2007 | 496 |
| 2000 | 271 | 2008 | 517 |
| 2001 | 293 | 2009 | 530 |
| 2002 | 344 | 2010 | 541 |

Наибольшее количество российских пользователей SWIFT сосредоточено в Москве, на втором месте — Санкт-Петербург, далее следуют Екатеринбург, Казань и Новосибирск.

В 2010 году суммарный трафик SWIFT составил более 4,0 млрд сообщений. Количество же отправленных российскими пользователями сообщений превысило 31,4 млн. И если в 2009 г. снижение российского трафика по сравнению со снижением суммарного трафика SWIFT происходило удвоенными темпами, то в 2010 г. ситуация зеркально изменилась — рост российского трафика составил 15,6% на фоне роста общемирового трафика SWIFT на 7,2%.

По-прежнему наибольший вес в структуре российского трафика имеют платежи — 78,3% (рост 15,4%), далее идут операции с ценными бумагами — 10,8% (рост 13,2%). Операции на финансовых рынках занимают третью строчку таблицы с показателем 8,9% (рост 25,0%). Отрадно отметить, что в целом по объему отправленного трафика Россия поднялась на 22-е место в мире.

Доля внутреннего трафика составила 58,4% (рост 13,0%). По данному показателю наша страна занимает 10-е место в мире. Вслед за Россией по степени убывания наши пользователи наиболее часто отправляют сообщения в США (11,7%), Германию (6,9%), Великобританию (5,8%), Беларусь (3,0%) и Украину (2,6%).

Трафик России

| Год | Количество сообщений | Год | Количество сообщений |
|------|----------------------|------|----------------------|
| 1995 | 3 179 346 | 2003 | 12 450 561 |
| 1996 | 3 783 823 | 2004 | 15 281 128 |
| 1997 | 5 463 857 | 2005 | 17 810 861 |
| 1998 | 5 517 072 | 2006 | 20 532 533 |
| 1999 | 4 479 650 | 2007 | 24 429 961 |
| 2000 | 6 642 263 | 2008 | 28 819 790 |
| 2001 | 8 309 709 | 2009 | 27 437 545 |
| 2002 | 9 964 562 | 2010 | 31 632 539 |

Трафик SWIFT, %

| Распределение трафика SWIFT | В мире | В России |
|-------------------------------|--------|----------|
| Платежи | 49,4 | 78,3 |
| Ценные бумаги | 43,4 | 10,8 |
| Операции на финансовых рынках | 5,8 | 8,9 |
| Финансирование торговли | 1,1 | 0,4 |
| Системные сообщения | 0,3 | 1,6 |

2.4. ОРГАНИЗАЦИОННАЯ СТРУКТУРА РОССИЙСКИХ ПОЛЬЗОВАТЕЛЕЙ SWIFT – РОССВИФТ

Согласно Уставу SWIFT, в каждой стране, представленной в Сообществе, создаются Национальная группа членов SWIFT и Группа пользователей SWIFT, объединяющие всех пользователей сети. В Российской Федерации организацией, представляющей интересы обеих групп и действующей от их имени, является Российская национальная ассоциация SWIFT (РОССВИФТ), которая была создана в мае 1994 г. и представляет собой негосударственную некоммерческую организацию.

В настоящее время более 550 ведущих российских банков и организаций являются пользователями SWIFT. Высшим органом Ассоциации является общее собрание. В перерывах между собраниями руководство Ассоциацией осуществ-

вляется комитетом. Комитет избирается собранием из числа членов Ассоциации в соответствии с утвержденными собранием принципами. Комитет возглавляет председатель комитета РОССВИФТ. Текущее управление деятельностью Ассоциации осуществляет исполнительная дирекция.

Основные направления деятельности Ассоциации.

- Координация деятельности российских пользователей SWIFT и оказание им правовой, организационной, консультативной и иной помощи; защита их прав и интересов в государственных органах Российской Федерации, оказание им помощи в целях повышения эффективности их деятельности.
- Осуществление сотрудничества с Советом директоров и Администрацией SWIFT по вопросам планирования и развития SWIFT в Российской Федерации; проверка соответствия российских пользователей критериям, выработанным Ассоциацией, исходя из решений Совета директоров и Администрации SWIFT.
- Представление от имени российских финансовых организаций — членов SWIFT кандидатуры в Совет директоров SWIFT, а также рекомендация специалистов для деятельности в рабочих группах и других органах SWIFT.
- Информирование российских пользователей SWIFT о решениях органов власти и управления, налоговых органов и прочих организаций по вопросам, имеющим отношение к деятельности SWIFT в Российской Федерации.
- Формирование рабочих групп для решения конкретных задач Ассоциации в интересах ее членов; руководство деятельностью группы пользователей SWIFT Российской Федерации, обеспечение деятельности групп пользователей интерфейсов и рабочих групп по разработке стандартов.
- Осуществление ввоза на территорию Российской Федерации криптографического оборудования для подключения к сети SWIFT и организация замены неисправного оборудования.
- Организация обучения персонала и подготовка документации, включая рекомендации по использованию сети SWIFT для осуществления рублевых платежей и перевод Руководства пользователей SWIFT на русский язык.
- Организация собраний, конференций, семинаров, участие в проведении выставок.

Начиная с 2000 г. российские пользователи SWIFT имеют за своими плечами успешный опыт реализации двух пятилетних концепций развития. Практически все задачи данных документов успешно выполнены, по ряду направлений продуктивная работа продолжается.

Опыт SWIFT широко используется для совершенствования стандартов российской финансовой индустрии. Данному процессу, в частности, способствуют:

- Меморандум о взаимопонимании между Банком России и SWIFT касательно построения в России системы валовых расчетов в режиме реального времени (RTGS), подписанный в 2004 г.;

- Соглашение между ФСФР России и SWIFT о сотрудничестве в области использования международных стандартов финансовых сообщений участниками российского фондового рынка, подписанное в 2006 г.

В 2009 году Председатель Правительства России утвердил План мероприятий по созданию Международного финансового центра в Российской Федерации. Данные мероприятия включают, в частности, внедрение форматов электронных сообщений платежной системы Банка России для обеспечения их совместимости с форматами SWIFT для осуществления расчетов в рублях и соответствующую доработку системы БЭСП. В этой связи Банком России подготовлен проект нового расчетного документа и создается специализированный интерфейс для проведения расчетов в системе БЭСП с использованием SWIFT.

По итогам 2010 г. по количеству пользователей SWIFT Россия занимает второе место в мире после США, трафик страны растет опережающими мировые показатели темпами. Банк России приступил к опытной эксплуатации обеспечения возможности доступа кредитных организаций в национальную систему крупных (высокоприоритетных) платежей БЭСП через SWIFT.

Концепция развития SWIFT в России до 2015 г. традиционно уделяет максимальное внимание практической реализации задач, поставленных российскими пользователями. Основными направлениями Концепции являются «эффективная локализация» развития SWIFT в России, содействие созданию в Москве Международного финансового центра и обеспечению российскому рублю статуса региональной резервной валюты, а также формирование условий для вхождения представителя страны в совет директоров SWIFT. Документ в том числе включает в себя план реализации принципов, изложенных в Концепции развития платежной системы Банка России на период до 2015 г. и в Стратегии SWIFT 2015.

2.5. ОСУЩЕСТВЛЕНИЕ ПЛАТЕЖЕЙ И РАСЧЕТОВ В РУБЛЯХ С ИСПОЛЬЗОВАНИЕМ SWIFT

Для осуществления платежей и расчетов в рублях с использованием SWIFT совместно с Банком России подготовлен специальный документ — Рекомендации SWIFT-RUR. Фактически Рекомендации SWIFT-RUR — это набор правил STP, полностью соответствующих стандартам SWIFT и отвечающих требованиям российского законодательства по проведению расчетов в национальной валюте. Именно Рекомендации SWIFT-RUR были взяты за основу для обеспечения конвертируемости форматов платежных сообщений Банка России и стандартов SWIFT при построении системы БЭСП Банка России.

Фактически в Рекомендациях SWIFT-RUR отражены правила формирования сообщений SWIFT при операциях с российскими рублями, а также правила и таблицы транслитерации, которые позволяют производить однозначное кодирование и декодирование символов русского алфавита в тексте сообщений SWIFT.

Такой подход позволяет учитывать особенности организации расчетов в различных кредитных организациях и дает возможность использовать единые технологии для автоматизации обработки финансовых сообщений при операциях как в российских рублях, так и в иностранных валютах. Применение Рекомендаций SWIFT-RUR в значительной степени способствует тому, что на протяжении многих лет на внутренний трафик российских пользователей приходится более 50% отправляемых российскими пользователями сообщений SWIFT.

Следует отметить, что рекомендации SWIFT-RUR в свое время были утверждены SWIFT в качестве правил сквозной обработки данных (STP Rules) при использовании стандартов SWIFT для передачи финансовых сообщений в российских рублях и рекомендуются как дополнение к соответствующим томам Руководства пользователя SWIFT. Порядок применения рекомендаций SWIFT-RUR определяется Дополнительным соглашением об использовании стандартов SWIFT-RUR для совершения операций в валюте Российской Федерации в системе SWIFT, являющимся приложением к договорам о корреспондентских соглашениях. Обо всех изменениях действующей версии стандартов SWIFT-RUR пользователи извещаются не позднее чем за три месяца до предполагаемой даты их введения.

В целях унификации использования сообщений SWIFT при взаимодействии участников российского рынка ценных бумаг были созданы и утверждены Рекомендации SWIFT-RUS. Данный документ содержит набор правил и примеров, учитывающих специфику российского рынка и требования регулятора (ФСФР). Рекомендации SWIFT-RUS охватывают расчеты по ценным бумагам и активно используются депозитариями и кастодианами.

Рекомендации SWIFT-RUR и SWIFT-RUS находятся в открытом доступе на сайте РОССВИФТ (www.rosswift.ru).

2.6. ДОСТУП КОРПОРАЦИЙ В SWIFT

В последние годы пользователями SWIFT стали более 300 ведущих мировых корпораций (Arcelor, General Electric, EADS, Microsoft, «ЛУКОЙЛ» и др.).

Решения SWIFT для корпораций позволяют обмениваться финансовой информацией (платежи, подтверждения и расчеты на денежном рынке и по ценным бумагам, отчетность) со всеми своими финансово-кредитными организациями, используя при этом хорошо известные преимущества транспортной сети SWIFT. Реализуя физическое подключение к сети SWIFT, корпорация получает возможность использовать принцип «единого окна» для взаимодействия со своими банками, что является хорошей альтернативой по поддержке многочисленных банков-клиентов. Наличие единых стандартов финансовых сообщений со всеми расчетными банками позволяет упростить бизнес-процессы корпорации, а также управлять потоками денежных средств и другими активами более эффективно, реализуя на практике идею Payment Factory.

В свое время на Совете директоров SWIFT были утверждены три категории для корпораций при вступлении в сообщество SWIFT:

- контрагент по операциям на денежных рынках (Treasury Counterparty);
- участник закрытой группы пользователей под руководством члена SWIFT (Participant within MA-CUG);
- корпорация (Corporate) в рамках SCORE.

РОССВИФТ разработал критерии для определения категории членства, что позволило, по сути, упростить процедуру вступления в сообщество SWIFT российским корпорациям.

Ниже приводится краткое описание категорий членства в SWIFT для корпораций.

Treasury Counterparty

Категория «Контрагент по операциям на денежных рынках (Treasury Counterparty)» не дает возможности корпорациям передавать расчетные инструкции или получать отчетность по сети SWIFT. Данная категория позволяет корпорациям обмениваться с любой финансовой организацией — пользователем сети SWIFT сообщениями исключительно третьей категории, в которую входят подтверждения форексных сделок и сделок на денежных рынках. Требованием со стороны SWIFT является прохождение корпорацией аудиторской проверки на регулярной основе по международным стандартам.

Participant within Member Administered Closed User Group (MACUG)

Обмен сообщениями в данной категории ограничивается рамками закрытой группы пользователей (CUG). Функции администрирования берет на себя расчетный банк корпорации. Он же может устанавливать дополнительные правила при приеме в свою закрытую группу. Потенциально любая корпорация подходит под данную категорию.

Corporate for Standardised Corporate Environment (SCORE)

Вступление в сообщество SWIFT в данной категории освобождает корпорацию от необходимости создавать многочисленные закрытые группы пользователей со всеми своими расчетными банками. Единоразы зарегистрировавшись в SCORE, корпорация сможет обмениваться трафиком с любой финансовой организацией, подписавшейся на SCORE. Администрирование закрытой группы, действующей по принципу SCORE, осуществляет сам SWIFT. Критерии по доступу корпораций в данной категории являются достаточно жесткими со стороны SWIFT:

- акции корпорации котируются на фондовых биржах, зарегистрированных в странах, входящих в группу FATF, или
- наличие рекомендации от банка — участника SCORE, который в свою очередь зарегистрирован в стране — члене FATF. Данная рекомендация долж-

на содержать согласие банка на обмен финансовой информацией с этой корпорацией по сети SWIFTNet.

Для всех трех категорий членства корпораций в сообществе SWIFT действует следующее ограничение: трафик «корпорация — корпорация» запрещен.

РОССВИФТ согласовал с Банком России использование сети и стандартов SWIFT для обмена финансовой информацией корпорации и банка при отражении соответствующего положения в договоре. На регулярной основе проводятся рабочие встречи с крупнейшими российскими банками и корпорациями для выявления и анализа проблем, затрудняющих взаимодействие банков и их корпоративных клиентов по сети SWIFT. Среди российских пользователей SWIFT такие известные российские корпорации, как «ЛУКОЙЛ», Роснефть.

2.7. КОЛЛЕКТИВНОЕ ПОДКЛЮЧЕНИЕ К SWIFT

При подключении к международной системе SWIFT для кредитно-финансовой организации основополагающими факторами являются эффективность использования SWIFT и стоимость подключения. Аспекты уменьшения расходов на эксплуатацию комплекса SWIFT также интересуют и уже работающие в SWIFT организации.

Существуют два основных способа подключения к сети SWIFT: собственное подключение и коллективный доступ.

Собственное подключение к SWIFT предполагает наличие у пользователя сложной собственной технической инфраструктуры, дорогостоящих специализированных каналов связи, квалифицированного персонала для осуществления целого ряда регламентных процедур обслуживания, а также определенных лицензий, связанных с использованием шифровальных средств.

Коллективный доступ к SWIFT предоставляется специализированной организацией (сервис-бюро), прошедшей соответствующую процедуру сертификации в SWIFT. Используя коллективный доступ к SWIFT через специализированное сервис-бюро, пользователь значительно сокращает расходы на собственную техническую инфраструктуру, каналы связи, а также дополнительно получает квалифицированное обслуживание специалистов сервис-бюро. Коллективный доступ к SWIFT имеет широкое распространение во всем мире, поскольку обеспечивает эффективный способ использования сервисов SWIFT с минимальными собственными затратами, что особенно важно в текущей экономической ситуации.

В России в настоящее время более половины всех работающих в SWIFT финансовых организаций используют коллективное подключение. Подключение к сети SWIFT через сервис-бюро предоставляет кредитно-финансовым организациям следующие преимущества:

- упрощение технической инфраструктуры и, как следствие, значительное снижение единовременных расходов на подключение к SWIFT;

- снижение ежемесячных расходов на содержание технической и штатной инфраструктуры;
- техническая и консультационная поддержка высококвалифицированными специалистами сервис-бюро;
- возможное снижение стоимости каналов связи в SWIFT;
- возможность оперативно предоставлять филиалам полный доступ к SWIFT под контролем центрального учреждения;
- возможность подключать дополнительные сервисы SWIFT с минимизацией расходов;
- высокая надежность и отказоустойчивость соединения со SWIFT без дополнительных расходов;
- существенное снижение расходов при смене местонахождения узла SWIFT;
- возможность последующего перехода на самостоятельное подключение.

В настоящее время сервис-бюро предлагает своим пользователям широкий спектр услуг, в полной мере отвечающих потребностям новых и уже работающих в SWIFT организаций, индивидуальный выбор графика работы в сети, а также бесплатные телефонные консультации по техническим вопросам. Получая доступ к сети SWIFT, клиент сервис-бюро потенциально становится пользователем большого количества услуг, что представляет собой реализацию концепции «единого окна», активно внедряемой SWIFT.

Крупнейшим в России является сервис-бюро «Безопасность финансовых коммуникаций» (БФК), созданное в 2002 г., ставшее одним из ведущих сервис-бюро в мире. БФК предоставляет своим клиентам возможность использования всех существующих сервисов SWIFT. На 1 января 2012 г. около 250 финансовых организаций из России, СНГ и стран дальнего зарубежья подключены через сервис-бюро БФК, а суммарный трафик сообщений, проходящих через инфраструктуру сервис-бюро, составляет около 20 тыс. сообщений в день.

ГЛАВА 3

НАЦИОНАЛЬНЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ И МЕЖДУНАРОДНЫЕ КАРТОЧНЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ

3.1. МЕЖДУНАРОДНЫЕ КАРТОЧНЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ

ИСТОРИЯ

Появление рынка платежных карт связано с основанием в 1950 г. компании Diners Club, выпустившей первую в истории многофункциональную платежную карту, что привело к значительным изменениям в сфере розничных платежей¹. Примечательно, что первые платежные карты были сделаны из картона² и принимались к оплате исключительно в некоторых ресторанах. Схема функционирования карты была проста: клиент посещал ресторан, его счет в ресторане оплачивала компания Diners Club, после этого клиент возмещал соответствующую сумму компании Diners Club. За первый год число держателей карт достигло 42 тыс. Такой успех объяснялся прежде всего ростом числа городов в США, в которых карты начали принимать к оплате. Уже в 1953 г. Diners Club становится международной платежной картой: ее начинают принимать в Великобритании, Канаде, Мексике и на Кубе. Спустя два года платежная карта начинает распространяться в Европе, Азии и на Ближнем Востоке через сеть франчайзинговых компаний. К 1959 году число держателей карт достигло миллиона человек, а акциями платежной компании стали торговать на Нью-Йоркской фондовой бирже. В 1967 году карта Diners Club принималась в качестве средства платежа уже в 130 странах,

¹ <http://www.dinersclubinternational.com>

² Первая пластиковая карта была выпущена в 1959 г. компанией American Express. Способ оплаты при помощи такой карты остался прежним, однако благодаря прочности материала, из которого она была сделана, карта American Express заняла нишу престижного платежного продукта.

а в 1969 и 1980 гг. она стала первой платежной картой, принимаемой в России и в Китае соответственно. В 1970-х годах платежная карта Diners Club была наиболее популярной международной картой, однако со временем компания потеряла свои лидирующие позиции. Тем не менее сегодня платежные карты компании Diners Club, принадлежащей банку Citibank, принимаются более чем в 185 странах и территориях по всему миру: картами платежной сети Diners Club можно воспользоваться в миллионах торговых точек, а также более чем в 800 тыс. банкоматов и других пунктах получения наличности¹.

На сегодняшний день абсолютными лидерами в области международных карточных платежей являются компании Visa и MasterCard — небанковские институты, принадлежащие банкам. При этом компания Visa занимает первое место по объему проводимых платежей. В дальнейшем при изложении различных аспектов функционирования международных карточных платежных систем будем опираться на опыт и устройство именно этих сетей, что объясняется их доминирующим положением.

Другими участниками на рынке международных платежных карт являются небанковские американские компании American Express (Amex), Discover, Diners Club. Кроме того, на данном рынке также заметно присутствие японской платежной системы JCB (Japan Credit Bureau) и китайской системы CUP (China Union-Pay).

VISA

История компании Visa² началась в 1958 г., когда Bank of America запустил свою первую кредитную карту общего назначения — проект BankAmericard, в рамках которого клиентам предоставлялась инновационная услуга «возобновляемого (револьверного) кредита». Новый продукт также представлял собой обычную картонную карточку с кредитным лимитом 300 дол. США. Первые кредитные карты не только предлагались уже существующим клиентам банка, но и рассылались по почте случайным людям, давая им возможность совершать покупки в кредит. Принцип работы и расчетов по карте BankAmericard аналогичен принципу работы с кредитной картой Diners Club.

В 1973 году National BankAmericard Inc. (NBI), управляемая рядом банков-эмитентов кредитных карт BankAmericard и созданная тремя годами ранее, запускает первую электронную систему авторизации (BASE I), а спустя год — предвестника современной операционной платформы VisaNet (BASE II), т.е. электронную клиринговую и расчетную систему. Первая дебетовая карта компании была выпущена в 1975 г., а через год BankAmericard изменил свое название на Visa, являющееся более удобным и одинаково произносимым на большинстве языков (знаковые события в развитии Visa — табл. 3.1).

¹ <http://www.dinersclubinternational.com>

² <http://corporate.visa.com> (см. также документ: Visa Inc. Corporate Overview).

Таблица 3.1

Основные события в развитии МПС Visa за период 1983–2011 гг.

| Год | Событие |
|-----------|---|
| 1983 | У держателей карт Visa появляется возможность круглосуточного доступа к наличности в банкоматах банков – участников платежной системы Visa во всем мире |
| 1986 | Visa становится первой карточной платежной системой, позволяющей финансовым институтам осуществлять расчеты и клиринг не в одной, а в разных валютах, что существенно повысило удобство и скорость совершаемых транзакций |
| 1989 | Введена возможность электронной подписи (после приобретения Visa компанией Interlink) |
| 1993 | Visa первой применяет новейшую технологию нейронной сети (neural network) в сфере платежей – нововведение, направленное на снижение уровня мошенничества с картами |
| 1995 | Visa совместно с MasterCard и Europay начинает участвовать в разработке платежной карты с чипом стандарта EMV (Europay/MasterCard/Visa), призванного обеспечить работу всех чиповых карт на всех терминалах, приспособленных для считывания информации с чипов |
| 1999 | Visa проводит первую транзакцию в валюте евро с использованием платежной карты |
| 2004 | Visa начинает использовать передовую технологию Advanced Authorization, позволяющую отслеживать и анализировать каждую транзакцию в режиме реального времени |
| 2007 | Visa запустила платформу для мобильных платежей и вспомогательных услуг. В этом же году заканчивается глобальная реорганизация компании, приведшая к появлению Visa Inc |
| 2010–2011 | Visa активно совершенствует свои возможности по совершению мобильных и бесконтактных платежей, в частности покупает компании PlaySpan Inc., Fundamo, а также заключает соглашение о долгосрочном сотрудничестве с компанией Monitise – лидирующим поставщиком решений для финансовых организаций в области «мобильных» денег (mobile money) |

На сегодняшний день Visa Inc. является компанией, позволяющей экономическим агентам более чем в 200 странах и территориях совершать платежи с использованием электронных денег. К основным направлениям деятельности компании Visa относятся:

- предоставление услуг по совершению транзакций финансовым институтам и коммерческим организациям на базе централизованной операционной платформы VisaNet. Кроме того, Visa дополнительно предоставляет своим клиентам некоторые услуги, в частности юридические, услуги по управлению рисками и т.д.;

- предоставление финансовым организациям широкого набора платежных инструментов, которые они далее предлагают своим клиентам в форме кредитных, дебетовых, предоплаченных продуктов и программ по доступу к наличности.

Visa Inc.¹ является наиболее крупной сетью, в которой совершаются розничные электронные платежи. По состоянию на 30 июня 2011 г. в обращении находилось 1,9 млрд карт платежной системы Visa, которые принимаются в миллионах магазинов и в 1,9 млн банкоматов по всему миру (за IV квартал 2010 г. — III квартал 2011 г. было проведено 76 млрд транзакций). Процессинговая платформа VisaNet функционирует на базе четырех операционных центров, расположенных на трех континентах.

MASTERCARD

История платежной сети MasterCard², первоначально носившей название Master Charge, начинается в 1966 г. с основания Interbank Card Association (ICA). В 1969 году Master Charge была приобретена California Bank Association и спустя десять лет была переименована в MasterCard (основные этапы развития — табл. 3.2).

Таблица 3.2

Основные этапы развития MasterCard за период с 1985 по 2011 г.

| Год | Событие |
|------------|---|
| 1985, 1988 | Приобретение доли в EuroCard (предшественнике EuroPay International) и в сети банкоматов Cirrus |
| 1991 | Запуск самостоятельного бренда (платежной сети) Maestro, которая стала первой всемирной дебетовой сетью |
| 2002 | MasterCard окончательно объединилась с Europay International |
| 2008 | Приобретение компании Orbiscom Ltd — лидера на рынке программного обеспечения в сфере платежей для финансовых организаций; начало использования международной платежной платформы IPS (Integrated Processing Solution) для дебетовых и предоплаченных продуктов |
| 2010 | Приобретение компании DataCash Group plc |
| 2011 | Завершение поглощения одного из подразделений компании Travelex по управлению предоплаченными картами (теперь эта программа носит название Access Prepaid Worldwide) |

По данным компании Mastercard, потребителями ее услуг являются приблизительно 22 тыс. организаций более чем в 210 странах и территориях. По состоянию на 31 декабря 2010 г. эмитентами было выпущено приблизительно 1,6 млрд

¹ Без учета Visa Europe.

² <http://www.mastercard.com> (см. также документы: Corporate Overview и MasterCard Annual Report 2010).

карт MasterCard и Maestro. Держатели карт могут воспользоваться ими более чем в 31 млн точек по всему миру. В основе платежной системы лежит операционная сеть MasterCard Worldwide Network, являющаяся, по данным MasterCard, самой высокоскоростной платформой в сфере карточных платежей и проводящая более 23 млрд транзакций в год. Средняя скорость ответа платежной системы составляет 0,13 с, что в 2 раза быстрее, чем у ближайшего конкурента компании¹. Подобно компании Visa платежная система MasterCard предлагает своим клиентам широкий набор кредитных, дебетовых, предоплаченных и прочих платежных продуктов на базе брендов MasterCard, Maestro, MasterCard PayPass и Cirrus.

Платежная сеть MasterCard географически поделена на следующие шесть регионов: США, Европа, Канада, страны Тихоокеанского бассейна, Ближний Восток и страны Африки, Латинская Америка и страны Карибского бассейна.

Платежная платформа MasterCard Worldwide Network является уникальной, поскольку сочетает в себе две традиционные операционные структуры:

1) децентрализованную (distributed), т.е. «пиринговую» сеть, в рамках которой осуществляется передача информации от одного самостоятельного равноправного узла к другому (peer-to-peer);

2) централизованную (centralized), т.е. имеющую центральный узел, связанных в второстепенными узлами (hub-and-spoke).

Передача данных с использованием децентрализованной сети является наиболее быстрой и надежной, поскольку происходит в тех пунктах платежной сети, которые находятся близко к месту совершения транзакции. В рамках децентрализованной сети обычно совершаются транзакции с использованием продуктов MasterCard PayPass. Централизованная передача данных осуществляется в режиме реального времени через центральный узел (hub). Таким образом, в рамках платежной системы для каждой транзакции выбирается оптимальный (наиболее быстрый и упрощенный) маршрут. Транзакции, требующие специализированной обработки, сначала анализируются на центральном узле сети, а затем направляются в подходящую финансовую организацию.

ПРОДУКТЫ

В целом в рамках международных карточных платежных систем предлагают услуги по совершению платежей с использованием следующих типов инструментов²:

1) традиционные карточные инструменты, включающие кредитные, дебетовые (в том числе банкоматные), расчетные, предоплаченные и иные типы карт;

2) развивающиеся формы платежей, к которым относятся, например, платежи, совершаемые с использованием мобильных телефонов.

¹ Подразумевается платежная сеть Visa.

² <http://www.mastercard.com> (см. документ: MasterCard Annual Report 2010).

Самым распространенным карточным платежным инструментом являются карты общего назначения, т.е. платежные карты с некоторым отличительным знаком (логотипом), позволяющим использовать ее в определенной стране, регионе или по всему миру. Отличительные свойства карт общего назначения зависят от типа счета, к которому привязана карта. Кредитные или расчетные карты обычно открывают доступ к кредитному счету. При этом в рамках расчетной карты требуется выплата полной суммы долга в течение определенного периода, в то время как кредитная карта предоставляет доступ к счету с возобновляемым кредитом. Дебетовые карты обычно связаны с чековым счетом, депозитным счетом до востребования или иным текущим счетом держателя карты. С помощью предоплаченных карт осуществляется использование предварительно внесенных на карту денежных средств.

В зависимости от вида используемой карты карточные платежи можно разделить на два типа транзакций:

1) офлайн-транзакции, т.е. транзакции, требующие в качестве подтверждения сделки подпись держателя карты¹;

2) онлайн-транзакции, т.е. транзакции, требующие введения персонального идентификационного номера (ПИН) держателя карты с целью удостоверения его личности.

Некоторые транзакции за пределами США могут совершаться с использованием чиповых карт, требующих введения ПИН-кода, однако при этом относятся к офлайн-транзакциям. Кроме того, в некоторые платежные карты встроены микрочипы с радиочастотной идентификацией (RFID, radio frequency identification), позволяющие совершать бесконтактные платежи, которые до определенной отдельно устанавливаемой суммы платежа не требуют ни подписи, ни ПИН-кода для подтверждения платежа. Введение ПИН-кода или подпись невозможны в случае, если покупка совершается через Интернет. Такие транзакции также классифицируются как офлайн-транзакции.

На протяжении длительного времени в США и на других крупных рынках под платежными картами понимались, скорее, кредитные и расчетные карты, т.е. карты, связанные с кредитным счетом держателя карты. Однако на сегодняшний день ситуация изменилась, и платежные системы предоставляют своим клиентам широкие возможности для выпуска дебетовых и предоплаченных карт, пользующихся большой популярностью у конечных потребителей.

Выпускаемые в настоящее время дебетовые карты можно условно разделить на три следующие категории²:

1) дебетовые карты, использование которых для совершения транзакции требует от держателя карты поставить свою подпись на товарном чеке, за исключением обстоятельств, в которых подпись не является обязательной. Например,

¹ Офлайн-транзакции на протяжении длительного времени представляли собой традиционную схему совершения платежа в наиболее крупных платежных сетях — Visa и MasterCard.

² <http://www.mastercard.com> (см. документ: MasterCard Annual Report 2010).

некоторые продавцы не требуют ставить подпись, если покупка совершена на небольшую сумму;

2) дебетовые карты, использование которых для совершения транзакции требует введения ПИН-кода на специальном терминале, установленном в пункте продаж;

3) карты, предоставляющие доступ только к наличным деньгам, в основном используются для получения наличных денег через банкоматы и требуют для этого введения ПИН-кода.

В целом основными конкурентами на рынке карточных платежей в США сегодня являются компании Visa, MasterCard, American Express и Discover. Однако основные участники рынка меняются в зависимости от карточного продукта. На рынке платежных карт общего назначения основную роль играют Visa (включая торговые марки Plus, Electron и Interlink), MasterCard (в том числе Maestro), American Express и Discover. На рынке дебетовых карт, используемых в основном для оплаты товаров и услуг в местах продаж и для снятия наличных денег через банкоматы, основными конкурентами в США являются различные сети компаний Visa и MasterCard, сеть Star, принадлежащая First Data Corporation, сеть NYCE, находящаяся в собственности FIS, а также сеть Pulse, принадлежащая Discover.

За пределами США существенную конкуренцию международным карточным платежным системам составляют национальные платежные операторы, зачастую поддерживаемые правительствами стран. Во многих странах основными игроками на рынке внутренних карточных платежей выступают именно национальные компании, а международные платежные сети обслуживают преимущественно трансграничные транзакции.

Примечательно, что зачастую финансовые организации эмитируют карты разных платежных сетей, например, как Visa, так и MasterCard повышают уровень конкуренции между международными платежными компаниями.

Компания Visa предлагает финансовым организациям широкий набор платежных продуктов. Кредитные продукты предоставляются на базе различных платформ, которые могут быть приспособлены под любой сегмент рынка, и в том числе под крупные корпорации. Эти платформы дополняются услугами, которые могут повысить использование этих продуктов клиентами и их лояльность. К таким дополнительным услугам можно отнести специальные поощрения, возможность срочной замены карты, помощь во время путешествий, страховку арендованной машины и т.д.

Дебетовые продукты компании Visa объединены в четыре торговые марки: Visa, Visa Electron, Interlink и Plus — и отвечают потребностям различных групп клиентов как с точки зрения их демографических и социальных характеристик, так и с точки зрения их географического месторасположения. Для сравнения MasterCard предлагает следующие дебетовые продукты: Debit MasterCard, Maestro и Cirrus.

Visa и MasterCard также предлагают множество prepaid-продуктов, которые удобны лицам, не пользующимся финансовыми услугами и не обслуживаемым в банках. Prepaid-карта выступает более надежной и удобной альтернативой наличности и чеку. Prepaid-продукты широко используются государством и фирмами¹ для распределения средств из фондов здравоохранения, для помощи безработным, с целью выплаты заработной платы и пособий. Можно привести следующие примеры использования prepaid-карт платежной сети MasterCard².

- По всему миру значительное число работников получают заработную плату на prepaid-карты.
- В Перу prepaid-карты используются для получения государственных талонов на продукты не в форме традиционных бумажных карточек, а в форме пластиковых карт.
- В Италии пополняемые карты используются для осуществления социальных выплат 1 млн человек; эта программа является самой крупной карточной программой социальных выплат в Европе.
- В России платежные карты MasterCard также используются для выплаты пособий по социальному обеспечению гражданам, не обслуживаемым в банках.
- Министерство финансов США планирует полностью отказаться от бумажных чеков к 2013 г. Клиринг одного чека в среднем обходится американской экономике в 1 дол., и такой переход на электронные платежи позволит сэкономить более 1 млрд дол. в течение десяти лет. С момента запуска программы Direct Express Debit MasterCard в 2008 г. министерство финансов перевело на электронную форму получения выплат более 1,5 млн человек.

Платежные компании также предлагают отдельные платежные продукты для бизнеса. В рамках платежной сети Visa для малых фирм такими продуктами являются Visa Business credit, Visa Business debit, а также Visa Business line of credit access cards. Для фирм среднего размера, крупных корпораций и государств Visa Inc. предлагает продукты Visa Corporate, Visa Purchasing, Visa Commercial, Visa Meetings, Visa Fleet, Visa Distribution, B2B, а также продукты и услуги по управлению цепями поставок. В рамках платежной сети MasterCard предлагаются следующие программы для бизнеса: MasterCard Payment Gateway, MasterCard Smart Data OnLine, MasterCard inControl. Кроме того, подобно компании Visa компания MasterCard предлагает широкий набор карточных платежных программ для фирм в зависимости от их размеров.

¹ <http://usa.visa.com> (см. документы VITA program uses Visa® Prepaid cards to speed tax refunds and empower underbanked clients, State significantly reduces unemployment insurance disbursement costs and achieves 99,5% e-pay, Chicago Public Schools achieves 99,8% e-pay), а также <http://www.mastercard.us> (см. документ PAYROLL CARD SAVES TIME AND MONEY FOR OMNI HOTELS & RESORTS AND ITS ASSOCIATES).

² <http://www.mastercard.com> (см. документ: MasterCard Annual Report 2010).

Основным преимуществом использования платежных карт и программ для фирм является удобство контролирования расходов, а также возможность их последующего анализа. В рамках таких платежных программ возможно совершение не только карточных платежей, но и банковских переводов (electronic funds transfer)¹.

УЧАСТНИКИ ПЛАТЕЖНОЙ СИСТЕМЫ

Компания, стоящая во главе платежной системы (например, Visa или MasterCard), обычно призвана выполнять следующие основные функции. Во-первых, она является франчайзером, во-вторых, обрабатывает и передает информацию о транзакциях участникам системы и, в-третьих, она может выполнять функции консультанта по вопросам работы системы. Роль франчайзера состоит в том, что платежная компания распространяет свои товары и услуги через финансовые организации по всему миру. Однако ключевыми функциями платежной системы являются обработка и передача информации о транзакциях.

Для предоставления консультационных и информационных услуг в области платежей в компании MasterCard было создано специальное подразделение. Предоставляемые услуги обычно являются возмездными, однако в некоторых случаях они могут оказываться клиентам бесплатно в качестве поощрения по некоторым договорам.

Основу любой карточной платежной системы составляет операционная платформа. Помимо платежной компании, т.е. организации, предоставляющей операционную платформу для совершения транзакций, так называемая открытая платежная система состоит из четырех типов участников:

- продавец (merchant) — компания, уполномоченная принимать карточные платежные продукты в оплату за товары и услуги;
- эквайер (acquirer) — финансовая организация (чаще всего банк продавца) или другая компания, которая обслуживает сделки по оплате товаров или услуг со стороны продавца;
- держатель карты (cardholder) — авторизированный пользователь платежной карты или иного платежного продукта;
- эмитент (issuer) — финансовая или иная организация (чаще всего банк держателя карты), выпускающая платежные карты и взаимодействующая с держателями карт в рамках выставления счетов и оплаты транзакций.

Платежные компании Visa и MasterCard не являются эмитентами платежных карт, не предоставляют кредиты держателям карт и не устанавливают комиссии и тарифы для конечных потребителей платежных продуктов. Платежные компании также не определяют «торговый дисконт», т.е. комиссию, которую финансовое учреждение, обслуживающее пластиковую карту, взимает с продавца за каждую сделку, оплаченную картой. Обычно такая комиссия устанавливается

¹ <http://corporate.visa.com>, <http://www.mastercard.com>

в виде процента от суммы покупки, оплаченной с помощью карты. Все эти вопросы находятся в ведении финансовых институтов — непосредственных клиентов платежных компаний, которые в свою очередь предоставляют платежные продукты и услуги конечным потребителям.

Участие банков в открытых платежных системах может проходить в прямой и аффилированной (ассоциированной) форме. Прямые участники являются полноправными членами платежной системы и самостоятельно принимают решения, касающиеся их работы в рамках платежной системы. В частности, прямой участник может выпускать карты всех типов собственного дизайна, а также может заниматься эквайрингом карт. Для того чтобы стать аффилированным участником платежной системы, банк должен иметь «спонсорскую поддержку» от прямого участника системы. Другими словами, прямой участник системы представляет банк к участию в международной платежной системе (МПС). Ассоциированный участник может проводить свои транзакции через банк, являющийся его «спонсором», или же может организовать собственную процессинговую сеть, тем не менее связанную с сетью банка — прямого участника системы для обмена данными. Ассоциированное участие позволяет небольшим и новым финансовым организациям становиться членами международных платежных систем, не беря на себя чрезмерные обязательства и риски.

Помимо открытых, или четырехсторонних, карточных платежных систем существуют так называемые закрытые, или трехсторонние, платежные системы. К таким системам можно отнести American Express, Diners Club, JCB, которые преимущественно сами являются как эмитентами карт, так и эквайерами. Такие системы относятся к «частным» системам, поскольку владелец структуры также является собственником технической сети, используемой для клиринга и совершения транзакций.

ОСУЩЕСТВЛЕНИЕ ТРАНЗАКЦИИ

Далее будет рассмотрено осуществление типичной транзакции в рамках четырехсторонних международных карточных платежных систем, к которым относятся Visa и MasterCard. Схема осуществления типичной транзакции представлена на рис. 3.1. Держатель карты предъявляет продавцу платежную карту в качестве средства платежа. Информация, касающаяся номера счета и других данных, закодированных на магнитной полосе карты или на ее чипе, считывается при помощи специального терминала на месте продажи. Терминал переводит информацию о карте и сумме транзакции эквайеру, который переносит информацию по транзакции в авторизационный запрос и отправляет сформированный запрос в платежную систему. МПС переправляет запрос эмитенту карты для проверки. (В некоторых случаях, например если система эмитента недоступна или не отвечает, МПС может выполнить самостоятельную обработку и проверку данных и, как следствие, разрешить или отклонить транзакцию.) Эмитент направляет

ет в МПС ответ на запрос об авторизации, разрешая или отклоняя транзакцию. МПС переправляет ответ об авторизации эквайеру, который в свою очередь передает информацию об ответе платежной системы на терминал продавца.

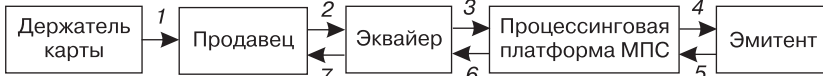


Рис. 3.1. Схема осуществления транзакции в четырехсторонней международной платежной системе

Типичная транзакция, проходящая через платежную систему, происходит в три стадии: авторизация, клиринг и расчет. Авторизация — процесс одобрения (санкционирования) или отклонения транзакции до момента окончательного совершения покупки или выдачи денег из банкомата. Под клирингом понимается процесс передачи итоговой информации о транзакциях от эквайеров эмитентам карт для дальнейшего учета данных о транзакции на счете держателя карты. Процесс клиринга также включает в себя подсчет комиссий, причитающихся эквайеру и эмитенту карты, которые были задействованы в совершении транзакции, а также перевод денежных средств в валюту, в которой должна быть совершена транзакция. Процесс расчета состоит в определении и передаче чистых итоговых позиций эмитентов карт и эквайеров по всем транзакциям, прошедшим клиринг.

Ни рисунок 3.2 показан процесс клиринга и расчета между эмитентом платежной карты и эквайером. Процесс клиринга можно разделить на три этапа:

- 1) на первом этапе продавец передает информацию о покупках эквайеру, в том числе номера счетов и суммы, на которые были совершены транзакции;
- 2) далее на основании полученной информации эквайер формирует клиринговое извещение (сообщение) и пересылает его в МПС;
- 3) МПС переправляет клиринговое извещение эмитенту, а также рассчитывает обязательства эмитента по расчетам и сумму, которая должна быть перечислена эквайеру (за вычетом комиссий).

Процесс расчета происходит следующим образом. Эмитент направляет средства в размере своих обязательств по расчетам в банк, выбранный МПС для совершения расчетов. По указанию МПС расчетный банк переводит средства эквайеру.

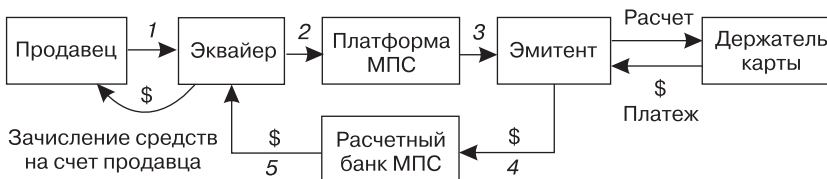


Рис. 3.2. Процесс клиринга и расчетов между эмитентом и эквайером для типичной транзакции в рамках МПС

В общем случае некоторые особенности осуществления транзакции в рамках платежной системы могут различаться в зависимости от того, является ли транзакция внутренней, т.е. осуществляется внутри одной страны, или транзакция является трансграничной, т.е. происходит между участниками платежной системы из разных стран. В случае если транзакция является внутренней, страна ее проведения также имеет значение, так как правила проведения транзакций в каждой конкретной стране определяются не только регламентами МПС, действующими для отдельных стран и регионов, но и национальным законодательством. Процесс осуществления транзакции также зависит от ее цели. Транзакция может быть направлена на оплату товаров и услуг в местах продаж или же на снятие наличности. Кроме того, транзакция может быть проведена непосредственно через сеть платежной компании или же через стороннюю платежную сеть. В случае если финансовая организация является одновременно и эмитентом платежной карты, и эквайером, обычно транзакция проводится ею самостоятельно.

КОМИССИИ

Источником доходов для платежных компаний служат преимущественно комиссии, которые платят банки или другие финансовые организации и которые зависят от объема платежей и транзакций, проходящих через платежную систему. Отдельным источником доходов для платежных компаний служат комиссии, которые выплачивают эмитенты карт и эквайеры за пользование дополнительными услугами платежных компаний. Кроме того, комиссия может также взиматься за присоединение к платежной системе. Размер комиссии за присоединение в общем случае зависит от следующих факторов:

- типа участия;
- набора услуг, используемых банком;
- деятельности, выполняемой банком (эмиссия карт или эквайеринг);
- объема активов нового участника и др.

Доход платежной компании формируется из следующих четырех источников:

1) внутренние отчисления (*domestic assessments*), т.е. комиссии, выплачиваются эмитентами карт и эквайерами и исчисляются исходя из объема операций по картам в случае, когда страна держателя карты совпадает со страной продавца, принимающего карту к оплате;

2) трансграничные комиссии (*cross-border volume fees*) уплачиваются эмитентами карт и эквайерами исходя из объема операций, совершенных по карте в случае, когда страна держателя карты не совпадает со страной продавца;

3) комиссии за обработку транзакций (*transaction processing fees*) взимаются как за внутренние, так и за трансграничные транзакции и зависят главным образом от числа сделок; комиссии за обработку транзакций взимаются отдельно за каждый этап ее совершения, т.е. за авторизацию, клиринг и расчет, и обычно выплачиваются эмитентами карт;

4) прочие доходы (*other revenues*) поступают за пользование дополнительными услугами, например услугами для держателей карт, консультационными и исследовательскими услугами, помощью в урегулировании споров; в прочие доходы также включены пени, плата за голограммы и публикации.

Чистая выручка платежной компании уменьшается на величину скидок и поощрений (*rebates and incentives*), которые выплачиваются участникам системы с целью стимулирования и повышения лояльности. В таблице 3.3 представлена динамика доходов компании MasterCard по источникам доходов в период с 2008 по 2010 г.

Таблица 3.3

Динамика доходов компании MasterCard за 2008—2010 гг., млн дол. США

| Доход | 2010 г. | 2009 г. | 2008 г. |
|----------------------------------|---------|---------|---------|
| Внутренние отчисления | 2 642 | 2 382 | 2 386 |
| Трансграничные комиссии | 1 927 | 1 509 | 1 547 |
| Комиссии за обработку транзакций | 2 198 | 2 042 | 1 777 |
| Прочие доходы | 791 | 784 | 751 |
| Общая выручка | 7 558 | 6 717 | 6 461 |
| Скидки и средства поощрения | (2 019) | (1 618) | (1 469) |
| Чистая выручка | 5 539 | 5 099 | 4 992 |

Источник: MasterCard Annual Report 2010.

Структура и динамика доходов компании Visa за тот же период представлена в табл. 3.4.

Таблица 3.4

Динамика доходов компании Visa за 2008—2010 гг., млн дол. США¹

| Доход | 2010 г. | 2009 г. | 2008 г. |
|----------------------------------|---------|---------|---------|
| Внутренние отчисления* | 3 497 | 3 174 | 3 061 |
| Трансграничные комиссии | 2 290 | 1 916 | 1 721 |
| Комиссии за обработку транзакций | 3 125 | 2 430 | 2 073 |
| Прочие доходы | 713 | 625 | 569 |
| Поощрительные выплаты** | (1 560) | (1 234) | (1 161) |
| Выручка | 8 065 | 6 911 | 6 263 |

Источник: Visa Annual Report 2010.

* В рамках отчетности Visa эти отчисления носят название *service revenues* или *service fees*.

** В рамках отчетности Visa эти выплаты носят название *Volume and support incentives*.

¹ Отчетный год оканчивается 30 сентября.

Ценообразование на различные продукты и услуги, предлагаемые в рамках платежной системы, зависит от природы и объемов транзакций, их типов, а также от того, какие другие продукты и услуги предлагаются платежной сетью своим клиентам. Можно выделить следующие основные факторы, влияющие на формирование цен:

- внутренний или трансграничный характер транзакции;
- подтверждение транзакции подписью или ПИН-кодом;
- многоуровневое (дифференцированное) ценообразование со снижающимися тарифами при увеличении объемов или числа транзакций, осуществляемых клиентами платежной системы;
- географический регион или страна;
- совершение розничной покупки или снятие наличности.

Существенная доля доходов международных платежных сетей поступает от трансграничных транзакций. Это объясняется не только числом и объемом таких операций, но и тем фактом, что проведение каждой трансграничной транзакции сопряжено с большим числом и величиной различных комиссий, чем внутренние транзакции. Например, основная выручка компании MasterCard поступает от транзакций, проведенных в следующих валютах: доллар США, евро, бразильский реал.

Аналогичным образом банки или иные финансовые организации получают доходы в виде комиссий с конечных потребителей платежных услуг, т.е. держателей карт и продавцов товаров и услуг.

Банковская комиссия за операцию (*interchange fees*) представляет собой разницу между суммой по платежной транзакции и суммой, которую эмитент выплачивает эквайеру, т.е. расчетной суммой. Другими словами, это комиссия, выплачиваемая обслуживающим банком банку — эмитенту платежной карты при осуществлении операции с помощью карты. Она предназначена для покрытия расходов эмитента на всех этапах осуществления транзакции. Обычно комиссия взимается в виде определенного процента от суммы сделки. Целью банковской комиссии за операцию является распределение издержек платежной системы между ее клиентами. Таким образом, комиссия за операцию является ключевым показателем, выравнивающим затраты, которые несут покупатель и продавец. В некоторых случаях, например в случае совершения операции по снятию наличности, комиссия выплачивается банком-эмитентом эквайеру.

Международные платежные системы обычно объясняют необходимость существования межбанковской комиссии за операцию тем, что в ее отсутствие эмитенты не могли бы получать достаточный доход и перекладывали бы свои издержки на держателей карт, что привело бы к снижению количества карт в рамках платежной системы.

Платежная система устанавливает комиссии за операции, действующие по умолчанию в том случае, если между эмитентом карты и эквайером не оговорены условия совершения расчетов. Кроме того, платежная система руководит процессом сбора и перевода комиссий за операцию на протяжении всего процесса рас-

четов. Комиссии за операцию могут быть существенной составляющей торгового дисконта (merchant discount), т.е. издержек, которые несут продавцы, с тем чтобы иметь возможность принимать платежные карты в качестве оплаты. В некоторых странах комиссии за операции подлежат регулированию, а также законодательному изменению.

Торговый дисконт устанавливается эквайером для покрытия своих издержек и получения прибыли от участия в платежной системе; он включает в себя комиссию за операцию, а также комиссии, установленные эквайером за определенные услуги, которые он предоставляет продавцу.

Помимо торгового дисконта эквайеры могут взимать с продавцов дополнительные комиссии, например, за обработку данных. В свою очередь эмитенты также могут взимать с держателей карт комиссии за транзакции, включая комиссии за увеличение автоматически возобновляемого (револьверного) кредита. К традиционным комиссиям, выплачиваемым держателем карты банку-эмитенту, можно отнести:

- плату за эмиссию карты;
- комиссию за обслуживание карты, обычно выплачиваемую ежегодно;
- комиссию за предоставление выписок и иной информации по счету.

Таким образом, отношения между участниками платежной системы при оплате покупки по карте выстраиваются в соответствии со следующей схемой (рис. 3.3).

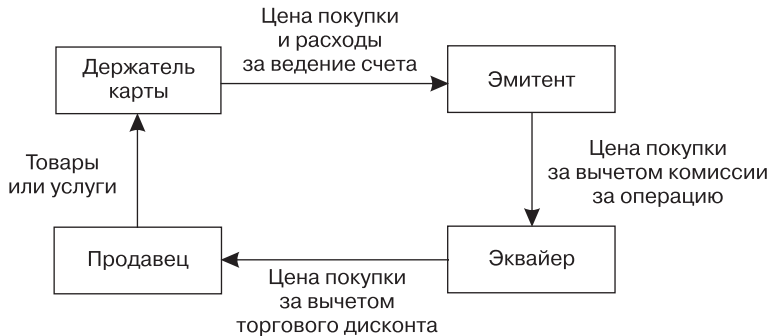


Рис. 3.3. Выплаты, осуществляемые между участниками платежной системы

ИННОВАЦИИ

Международные платежные компании направляют существенные средства на разработку новых продуктов и услуг для своих клиентов. В частности, стремительное развитие мобильных средств связи привело к расширению продуктовой линейки карточных платежных систем. В развивающихся странах степень проникновения мобильных телефонов гораздо выше, чем степень проникновения

банковских платежных карт. Это дает возможность для развития финансовых услуг и платежных продуктов на базе мобильных телефонов, которые позволяют потребителям совершать финансовые операции. В развитых странах мобильные платежи также имеют существенный потенциал роста. По мнению платежных компаний технологии мобильных платежей позволяют использовать мобильный телефон в качестве более удобного и безопасного платежного средства по сравнению с наличными деньгами¹. Такое платежное средство может быть использовано как имеющими, так и не имеющими банковский счет потребителями.

Компания Visa является основоположником следующих технологических инноваций, позволяющих расширять область применения электронных платежей:

- Visa Money Transfer представляет собой платформу для быстрого и безопасного перевода средств между счетами физических лиц внутри платежной сети Visa. На сегодняшний день держатели карт Visa могут не только совершать покупки, но и получать средства на свои счета практически из любой точки мира;
- Visa payWave — технология бесконтактных платежей на основании встроенного в карту микропроцессора, повышающего безопасность и скорость совершения транзакции. Такие технологии расширяют возможности и удобство использования потребителями платежных карт, поскольку ими можно, например, оперативно оплатить проезд или парковку, а также совершить покупку в торговом автомате;
- Visa также позволяет держателям карт совершать покупки через Интернет. Для этих целей потребители используют как дебетовые и кредитные карты, так и предоплаченные карты. Для обеспечения безопасности совершения транзакций компания разрабатывает различные инновационные способы идентификации держателя карты.

К инновационным разработкам компании MasterCard можно отнести следующие продукты и решения:

- MasterCard PayPass — бесконтактная платежная технология, позволяющая увеличить скорость совершения платежа. Используется для оплаты проезда, в ресторанах быстрого обслуживания, на заправочных станциях, в торговых автоматах, в кинотеатрах и др. Применение бесконтактной технологии возможно на базе платежных карт, выпускаемых отдельными банками (например, Citibank, J.P. Morgan Chase и MBNA), а также на базе мобильных телефонов (например, некоторых моделей Nokia);
- MasterCard MoneySend — услуга, позволяющая владельцам карт MasterCard совершать переводы денежных средств через банки, онлайн через Интернет, через банкоматы или посредством мобильного телефона;
- MasterCard inControl — технология, позволяющая держателям карт устанавливать параметры транзакций, т.е. определять, как, когда и где могут быть использованы их карты.

¹ <http://www.mastercard.com> (см. документ: MasterCard Annual Report 2010).

Visa и MasterCard также разработали так называемые 3D-решения, позволяющие идентифицировать держателя карты посредством персонального кода, проверяемого эмитентом карты, когда карта используется для оплаты покупок через Интернет. Другим способом повышения доверия держателей карт к онлайн-платежам является использование одноразовых («виртуальных») паролей. Они могут создаваться в момент подключения держателя карты к серверу банка через Интернет. Оба этих способа не раскрывают информацию об истинном номере платежной карты.

Стандарт EMV начал разрабатываться в 1994 г. компаниями Europay, MasterCard и Visa. Первая версия технических требований в рамках данного стандарта была создана в 1996 г. В 2002 году компания Europay окончательно объединилась с платежной сетью MasterCard. В 2004 году к стандарту присоединилась японская платежная сеть JCB, а в 2009 г. — American Express. Сегодня EMV представляет собой мировой стандарт кредитных и дебетовых платежных карт, основанных на технологии чипа. Основной целью создания нового стандарта была безопасность совершения карточных платежей. По состоянию на I квартал 2008 г. в мире было выпущено более 730 млн, а по состоянию на 2010 г. — уже около 1 млрд платежных карт, совместимых со стандартом EMV. Платежи, проводимые при помощи карт стандарта EMV, могут быть как контактными, так и бесконтактными. Можно выделить следующие преимущества платежных карт стандарта EMV:

- 1) чиповые карты являются более надежными с точки зрения предотвращения мошенничества по сравнению с кредитными картами, защищенными только информацией, закодированной на магнитной полосе карты;
- 2) уникальная цифровая подпись служит доказательством подлинности чипа в случае офлайн-операций и не дает возможности преступникам использовать поддельные платежные карты;
- 3) такая карта может быть использована для совершения безопасных онлайн-платежей, что позволяет защитить держателей карт, продавцов и эмитентов от мошеннических действий благодаря уникальному онлайн-шифру (криптограмме);
- 4) поддерживает усовершенствованные способы идентификации держателя карты;
- 5) позволяет хранить больше информации по сравнению с магнитными полосами на картах.

РЕГЛАМЕНТЫ И ПРАВИЛА ПЛАТЕЖНЫХ СИСТЕМ

Содержательно регламентирующие документы сетей Visa и MasterCard во многом похожи, поэтому далее будут рассмотрены регламенты международных карточных платежных систем на примере компании Visa.

Регламенты платежной сети Visa подразделяются на международные и региональные и регулируют взаимоотношения между системой Visa и ее участниками. Региональные регламенты описывают правила взаимодействия между участ-

никами платежной системы в каждом конкретном регионе или стране. Правила, регулирующие отношения между всеми участниками системы в Европе, описываются в отдельном документе, поскольку Visa Europe является самостоятельным юридическим лицом. К основным регулирующим документам Visa можно отнести:

- Visa International Operating Regulations;
- Visa International Certificate of Incorporation and Bylaws;
- Visa U.S.A. Inc. Certificate of Incorporation and Bylaws;
- Interlink Network, Inc. Bylaws and Operating Regulations;
- Visa Cash Program Operating Regulations;
- Plus System, Inc. Bylaws and Operating Regulations;
- Visa Product Brand Standards.

В документе Visa International Operating Regulations¹ описаны правила, регламентирующие взаимоотношения между участниками платежной системы, предъявляемые к ним требования, правила совершения транзакций и т.д. В основе документа лежит следование десяти базовым принципам деятельности компании.

Первый принцип — принцип управления — состоит в том, что компания Visa разрабатывает и устанавливает правила функционирования платежной системы с целью минимизации рисков, а также предоставления удобной, безопасной и повсеместной возможности совершения платежей. Регламенты (правила) платежной системы представляют собой контракт, имеющий обязательную силу и заключенный между компанией Visa и участниками системы. Регламенты регулярно пересматриваются с учетом рыночных тенденций, технологического развития и других факторов.

Второй базовый принцип отражает регламентирование участия в системе. Платежная система Visa включает в себя такие элементы, как технологии, продукты, услуги, а также маркетинговые планы, способствующие развитию мировой торговли путем электронного перемещения денежных средств и информации между экономическими агентами. Участниками платежной системы могут быть финансовые организации, операторы (*processors*), осуществляющие передачу данных о платежах, и другие организации, удовлетворяющие всем предъявляемым к ним формальным требованиям. Большую часть участников платежной системы составляют финансовые институты или иные аналогичные организации, выпускающие платежные продукты для потребителей или привлекающие новых продавцов, еще не принимающих карточные продукты в качестве средства платежа. Участники платежной системы могут работать со сторонними организациями, помогающими им с выпуском и приемом платежных продуктов, а также с операторами, имеющими непосредственную связь с платформой VisaNet. Участники системы несут ответственность за все ошибки и действия таких привлеченных сторонних организаций, кроме того, они несут полную ответственность за эмис-

¹ <http://corporate.visa.com>

сию платежных продуктов и их прием в торговых точках, что включает в себя ответственность не только за проведение транзакции, но и за соответствие деятельности участников всем регламентам и требованиям Visa, а также законодательству.

Третий принцип строится на том, что все участники платежной системы признают за компанией Visa право интеллектуальной собственности на сам бренд Visa, торговые марки и технологии, а также соглашаются защищать эти права собственности. Участники системы могут использовать бренд и технологии Visa для предоставления платежных и финансовых услуг своим клиентам с учетом региональных требований банковского регулирования. Участник системы может получить у компании Visa один или несколько банковских идентификационных номеров (БИН) и несет ответственность за всю деятельность, связанную с БИНами.

Четвертый принцип говорит о поддержании и защите бренда Visa всеми участниками платежной системы. Использование торговых марок Visa должно согласовываться с требованиями Visa Product Brand Standards, и такие торговые марки не могут быть каким-либо образом изменены, а также не могут появляться реже, чем другие платежные марки, выпускаемые эмитентом или используемые продавцом. Бренд Visa всегда должен быть размещен на передней части платежного продукта (например, карты). Никакие конкурирующие товарные марки не могут быть нанесены на платежный продукт. Участники платежной системы Visa или третьи стороны не могут использовать имя Visa или названия принадлежащих компании марок, а также производные от этих названий в качестве составной части названия своей компании. Для рекламы продуктов Visa, спонсорства, услуг, процедур передачи данных или принятия карт к оплате могут быть использованы только торговые марки Visa. Аналогично для обозначения того, что карта может быть принята к оплате за пределами страны выпуска, может быть использован только бренд Visa, который должен быть более заметным, чем специфические для каждой страны торговые марки. Для того чтобы обозначить принятие платежной карты к оплате на местах продаж, может быть использован только бренд Visa, но не обозначение карты или другого платежного продукта.

Пятый принцип связан с продуктами и услугами, предоставляемыми платежной системой. Речь идет о платформах для кредитных, дебетовых, предоплаченных и коммерческих платежей. Участники платежной системы принимают стандарты выпуска платежных карт и технологии платежной системы, что обеспечивает слаженную работу системы, непрерывность совершения транзакций и передачи данных. В частности, магнитные полосы и чипы, используемые на платежных картах Visa, должны быть изготовлены в соответствии со стандартами и техническими требованиями Visa с тем, чтобы обеспечить глобальную функциональную совместимость и проведение платежей. Кроме того, компания Visa определяет требования относительно оформления карты и стандарты использования торговых марок для того, чтобы обеспечить целостность и безопасность продуктов и бренда Visa. Эмитенты — участники платежной системы соглаша-

ются работать только с одобренными компанией Visa фирмами, производящими платежные карты.

Шестой принцип отражает проблему принятия платежей. Продавцы — участники платежной системы, указывающие на то, что они принимают к оплате платежные карты, соглашаются принимать в качестве средства платежа соответствующие платежные продукты Visa. Если покупатель хочет оплатить покупку при помощи карты, продавец обязан провести соответствующую транзакцию через платежную систему; он не может отказать покупателю в принятии к оплате его карты на том основании, что карта выпущена эмитентом другой страны или дополнительно помечена брендом организации, являющейся конкурентной для продавца. Продавцы могут предлагать покупателям альтернативный способ оплаты, например сделать скидку в случае оплаты наличностью (*cash discount*). Однако такое поведение не должно оказывать давление на покупателя или отвергать выбранное покупателем средство оплаты. Продавцы вправе определять, могут ли некоторые обстоятельства вызвать чрезмерный риск, связанный с оплатой при помощи карты. Примером такой ситуации может служить транзакция, подтверждаемая при помощи цифровой подписи на специальном оборудовании при условии, что на оборотной стороне платежной карты не стоит образец подписи держателя карты, а последний не имеет при себе удостоверения личности с образцом подписи (например, паспорта). Продавцы — участники платежной системы не имеют права требовать с покупателей дополнительные комиссии и сборы, не предусмотренные компанией Visa, за исключением случаев, предусмотренных местным законодательством. Терминалы, используемые для считывания информации с магнитных полос и чипов, должны отвечать определенным стандартам и техническим требованиям с тем, чтобы обеспечить повсеместную совместимость продуктов платежной системы и принятие платежей.

Седьмой принцип связан с непосредственным проведением транзакции. Компания Visa определяет требования, условия и исключения из правил с тем, чтобы обеспечить успешное совершение транзакций на всех ее этапах, т.е. в момент авторизации, а также в процессе клиринга и при расчете. Ключевой составляющей платежной системы Visa является платформа VisaNet, которая позволяет компании предлагать финансовым организациям широкий набор продуктов и сопутствующих услуг. Участники платежной системы обязаны предоставлять своим клиентам услуги по авторизации и расчетам, связанным с транзакциями. Компания Visa определяет финансовую ответственность эмитентов и эквайеров, распределение которой может различаться в зависимости от условий принятия карт продавцами. В частности, если транзакция незаконно была совершена продавцом без непосредственного применения платежной карты¹, то финансовую ответственность в этом случае несут эквайеры.

¹ Такая ситуация возможна, если недобросовестному продавцу становится известна информация, размещенная на платежной карте: номер карты, имя владельца, срок истечения, CVV/CVC-код.

Согласно правилам платежной системы, эмитенты несут финансовую ответственность за транзакции, совершенные продавцом и должным образом проведенные эквайером. Финансовая ответственность за транзакции, которые были проведены с нарушениями требований платежной системы, может быть перенесена с эмитента карты на эквайера. Участники платежной системы обязаны совершать все этапы трансграничной транзакции с использованием платформы VisaNet, а также передавать информацию обо всех внутренних транзакциях с использованием продуктов Visa, проведенных вне системы VisaNet. В некоторых юрисдикциях участники системы обязаны проводить все транзакции (как трансграничные, так и внутренние) через платформу VisaNet. Это позволяет Visa улучшать управление рисками и разрабатывать способы борьбы с мошенничеством.

Восьмой принцип показывает важность управления рисками. Все участники платежной системы должны следовать предъявляемым компанией Visa требованиям по контролю над рисками. Кроме того, участники системы обязаны незамедлительно сообщать Visa обо всех мошеннических транзакциях или иной криминальной деятельности, связанной с проведением транзакций. Участники, имеющие доступ к информации о персональных счетах или транзакциях, проведенных в платежной системе, ответственны за соблюдение строгих стандартов в отношении защиты данных. Стандарты Visa могут соответствовать местным стандартам отрасли или превосходить их по степени предъявляемых требований. Участники платежной системы должны принимать необходимые меры, чтобы предотвратить использование платежной системы в нелегальных целях, например в целях отмывания денег или финансирования терроризма.

Девятый принцип отражает вопрос разрешения спорных ситуаций. Абсолютное большинство транзакций проходят через платежную систему без каких-либо затруднений. Однако существуют ситуации, когда совершение транзакции может быть оспорено как держателем карты, так и ее эмитентом. По этой причине Visa разработала правила и процедуры для эмитентов и эквайеров, которые помогают эффективно разрешать спорные вопросы с учетом интересов всех затронутых сторон, включая конечных потребителей платежных услуг (покупателей и продавцов). Эмитенты — участники платежной системы ответственны за принятие и проведение всех транзакций, однако у эмитентов есть право сделать возврат по транзакции в случаях, предусмотренных Visa. К таким случаям относятся, в частности, ошибки, совершенные в процессе обработки данных по неосторожности, некоторые виды мошенничества и определенные претензии со стороны держателей карты. Предполагается, что участники платежной системы по возможности решают спорные вопросы самостоятельно и только в случае невозможности этого передают ситуацию на рассмотрение и разрешение в компанию Visa. Таким образом, в случае неразрешенных спорных ситуаций Visa выступает арбитром.

Заключительный принцип платежной системы связан с вопросами ценообразования и различными комиссиями, в том числе комиссии за совершение

операции. Компания Visa устанавливает цены и комиссии на свои продукты и услуги исходя из динамики рынка и конкуренции в отрасли. Участники платежной системы выплачивают комиссии компании Visa за доступ и использование продуктов и услуг. Visa устанавливает некоторые комиссии между эмитентами и эквайерами за определенные действия участников системы, в частности вознаграждения продавцам в магазинах за возврат утерянных покупателями карт или предоставление копий чеков. Эквайеры и эмитенты платят или получают комиссию за совершение операций каждый раз, когда используется продукт Visa. Например, эквайеры выплачивают комиссию эмитентам за транзакции по покупке, и, напротив, эмитенты выплачивают комиссию эквайерам за quasi-cash-транзакции (в рамках таких операций картой оплачиваются некоторые товары, являющиеся близкими заменителями наличных денег, например фишки в казино, дорожные чеки, денежные переводы) и за предоставление продавцом кредита покупателю для совершения покупки (*merchandise credit or credit voucher*).

Согласно документам Visa, на настоящий момент на территории США действуют следующие правила принятия платежных карт¹. Продавцы имеют право установить минимальную сумму покупки, совершаемой при помощи кредитной карты. Это требование не распространяется на платежи, совершаемые при помощи дебетовых карт. При этом минимальная сумма покупки не должна превышать 10 дол. или сумму, установленную законодательно, и является одинаковой для всех карт вне зависимости от их эмитентов и карточной платежной системы. Верхнее ограничение суммы платежа при помощи кредитной карты может быть установлено только федеральными органами власти, а также высшими учебными заведениями, принимающими карту к оплате, и не зависит от эмитента карты и платежной системы. Аналогичные правила действуют и в других странах.

Основной регламентирующий документ платежной сети MasterCard называется MasreCard Rules и, как и в случае регламентов Visa, содержит в себе разделы, посвященные правилам участия в системе, лицензированию деятельности участников, их обязанностям. В данном документе также рассматриваются вопросы, связанные с торговыми марками платежной сети, правилами осуществления транзакций и расчетов, а также описываются правила, действующие в отдельных регионах работы системы. К другим регламентирующим документам MasterCard относятся:

- Chargeback Guide, описывающий различные вопросы, связанные с комиссиями платежной системы;
- Security Rules and Procedures для продавцов, рассматривающий различные аспекты работы системы с точки зрения безопасности совершения платежей;
- регламентирующие документы Maestro Global Rules.

Аналогичные регламентирующие документы разрабатываются для любой платежной системы.

¹ <http://corporate.visa.com> (см. документ: Card Acceptance in U.S. and its Territories).

3.2. ИНТЕГРАЦИЯ МПС И НПС

В рамках международных платежных систем возможно совершение как трансграничных, так и внутренних платежей. В то же время внутренние платежи в большинстве стран могут также быть проведены при помощи национальных карточных систем. Интеграция международных карточных платежных систем и национальных платежных систем затрагивает такие вопросы, как стандартизация технических требований, экономия от масштаба, конкуренция, протекционистская политика национальных государств и т.д.

МПС И ОБЪЕДИНЕНИЕ ЕВРОПЫ

Международные карточные системы стремятся расширять сферу своего влияния и достаточно оперативно реагируют на изменения экономической конъюнктуры. Деятельность европейских государств по созданию единой зоны платежей в евро нашла отражение в окончательном выделении отдельных самостоятельных подразделений в МПС: Visa Europe и MasterCard Europe.

Карточная платежная отрасль обслуживает существенную часть розничных продаж в Европе, генерируя значительные доходы¹. В середине 2000-х гг. в Европе наблюдалась тенденция дробления отрасли. Разрозненность карточных сетей во многом является следствием исторического процесса формирования платежных систем в отдельных странах Евросоюза. Однако построение Единой зоны платежей в евро (Single Euro Payment Area, SEPA) требует интеграции отдельных платежных сетей.

В 2008 году в зоне евро функционировали 33 карточные платежные системы, включая 27 национальных систем из 13 стран и 6 международных карточных платежных систем: Visa Europe, MasterCard Europe, American Express, Diners Club International, JCB International, China Union Pay. При этом торговый дисконт, выплачиваемый продавцами в рамках международных карточных платежных систем (MasterCard/Maestro, Visa), в среднем на 30—40% выше, чем торговый дисконт в рамках национальных сетей. Международные платежные системы устроены таким образом, что мелкие фирмы выплачивают более высокие комиссии по сравнению с крупными фирмами (разница может составлять до 60—70%)². В то же время такая дискриминация практически отсутствует в национальных платежных системах: разница в комиссиях для мелких и крупных фирм составляет в среднем всего 7%³. Некоторые банки-эквайеры (например, в Венгрии, Ирландии)

¹ Например, в 2005 г. совокупный объем покупок, совершенных при помощи платежных карт, составил более 1350 млрд евро, в то время как европейские фирмы заплатили более 25 млрд евро в виде комиссий.

² <http://ec.europa.eu> (см. документ: EUROPEAN COMMISSION, Competition DG, INTERIM REPORT I PAYMENT CARDS).

³ Там же.

дии, Дании, Бельгии, Испании, Швеции и на Мальте) взимают с продавцов один и тот же размер торгового дисконта вне зависимости от того, в рамках какой сети была эмитирована платежная карта. Такая практика носит название *blending* (смешивание) и ослабляет ценовую конкуренцию между платежными системами в Европе, что приводит к повышению комиссий, выплачиваемых фирмами. Уровень межбанковских комиссий за совершение операции обычно выше в международных карточных платежных системах и также различается по странам. В некоторых странах эквайеры выплачивают международным платежным системам более высокие комиссии за совершение внутренних транзакций по сравнению с трансграничными операциями. Это объясняется тем, что в таких странах минимальный уровень комиссии по внутренним транзакциям устанавливается на уровне трансграничной комиссии.

В соответствии с данными Европейской комиссии¹ можно выделить следующие уровни интегрированности карточных платежных систем в зависимости от того, вовлечена компания, владеющая платежной структурой, в финансовую или техническую деятельность, связанную с осуществлением платежных транзакций:

- 1) компания устанавливает технические стандарты, а также требования для участников платежной сети;
- 2) компания самостоятельно перенаправляет запрос об авторизации;
- 3) компания авторизует и проводит транзакции;
- 4) компания осуществляет клиринг и (или) расчет по транзакциям;
- 5) компания является эквайером;
- 6) компания продает и (или) сдает в аренду оборудование, необходимое для принятия карт в качестве средства платежа в местах продаж.

Таким образом, минимальный уровень интеграции равен 1, а максимальный — 6. Если следовать приведенной классификации, то из наиболее важных национальных карточных платежных систем в Европе по состоянию на 2006 г. 11 сетей соответствовали 1-му уровню интеграции, шесть сетей — 2-му уровню, пять сетей — 3-му уровню, четыре сети — 4-му уровню и по одной сети — 5-му и 6-му уровням.

Устройство международных карточных платежных систем, функционирующих в Европе, в целом является более сложным. Интеграция в рамках международных систем существенно различается в зависимости от страны (уровень интеграции варьируется от 1 до 5). При этом чем выше уровень интеграции в рамках платежной системы, тем в среднем ниже уровень конкуренции на рынке карточных платежных продуктов в данной стране. В связи с этим можно привести пример частичной дезинтеграции платежной системы MasterCard на рынке Австрии. В 1980 году австрийские банки организовали компанию *Europa Austria* с целью создания национальной дебетовой карточной системы, которая перешла

¹ <http://ec.europa.eu> (см. документ: EUROPEAN COMMISSION, Competition DG, INTERIM REPORT I PAYMENT CARDS).

на использование операционной платформы Maestro в 1998 г. В рамках платежной сети было совершено разделение финансовых и операционных аспектов деятельности: компания Europay Austria занималась привлечением и обслуживанием клиентов, в то время как операционная деятельность платежной сети была полностью сосредоточена в руках дочерней компании австрийских банков под названием APSS. В 2005 году австрийские банки продали операционную составляющую платежной системы компании First Data независимому международному карточному оператору. Это событие явилось важным шагом на пути роста конкуренции на австрийском рынке платежных карт.

Международные платежные системы Visa и MasterCard обслуживают практически все трансграничные транзакции на территории Европы, а также некоторые внутренние транзакции с использованием платежных карт. В некоторых странах — членах ЕС международные платежные компании проводят транзакции от имени местных банков — участников платежной сети. По этой причине степень интеграции между международными и национальными карточными платежными системами может существенно различаться в зависимости от страны. При этом такие платежные сети, как Amex, Diners Club и JCB, обычно являются в большей степени вертикально интегрированными, так как самостоятельно осуществляют эмиссию карт и деятельность по эквайрингу.

Во многих европейских странах (Австрия, Бельгия, Дания, Германия, Финляндия, Италия, Нидерланды, Португалия) банки — участники открытых карточных платежных систем (MasterCard и Visa) концентрируют деятельность по эквайрингу в руках одного совместного предприятия — межбанковской ассоциации. В такой ситуации вход на рынок для иностранных банков практически закрыт, поскольку местные банки взимают с них повышенные комиссии за совершение операции. Таким образом, продавцы сталкиваются с единственным источником предложения услуг по эквайрингу и не имеют возможности выбирать из конкурирующих между собой банков.

Обычно карточные платежные сети разрешают совместное использование товарных знаков на карте в случае, если они не являются конкурентами. Так, национальные платежные системы обычно не выступают конкурентами международным карточным сетям. На территории каждой страны зоны евро действует как минимум одна национальная карточная платежная система. Для того чтобы держатели карт имели возможность использовать их за пределами своей страны, карты обычно также относятся к одной из международных платежных систем (Visa или MasterCard). При использовании карты в качестве средства платежа на территории страны, в которой карта была выпущена, обычно задействуется национальный бренд, а при использовании карты за пределами страны (как в зоне евро, так и в других странах) используется международный бренд. При этом национальные карточные платежные системы по сравнению с международными системами являются менее дорогостоящими как для держателей карт, так и для продавцов.

В последние годы активно идет процесс интеграции европейского платежного рынка в единый стандартизированный рынок. За это время снизилось количество операторов на рынке платежных карт. В связи с этим Visa¹ полагает, что национальные платежные продукты будут приводиться к международным стандартам. Поскольку платежи, соответствующие единым стандартам, могут быть выполнены любыми операторами, это приведет к росту конкуренции в отрасли и количества участников рынка. По мнению MasterCard² стандартизация несет в себе выгоды с точки зрения экономии от масштаба и, напротив, приведет к снижению количества операторов на рынке платежных карт через процессы консолидации.

Изначально концепция создания единой зоны платежей в евро с точки зрения карточных продуктов предполагала вытеснение национальных платежных схем международными³. Предполагалось также, что международные платежные системы определяют и введут новые универсальные карточные услуги на всей территории евро. Однако такое развитие событий может привести к росту различных комиссий (и в особенности комиссий, выплачиваемых продавцами), что противоречит целям создания единой платежной зоны евро.

Опыт показал, что национальные карточные платежные системы смогли приспособиться к требованиям единой зоны платежей в евро⁴. Это означает, что в Европе отпала необходимость заменять более дешевые и эффективные национальные системы международными. В Евросоюзе также не исключается возможность создания единой европейской национальной платежной системы, однако на настоящий момент этот вопрос не решен⁵.

Платежная сеть MasterCard проводит большинство внутренних транзакций, выполненных при помощи одноименных карточных продуктов, в таких странах, как США, Великобритания, Канада и Бразилия, а также в ряде других стран. Однако абсолютное большинство транзакций, совершаемых внутри одной страны с использованием международных платежных карт Visa и MasterCard, проходят процесс авторизации, клиринга и (или) расчета через клиентов системы или других операторов системы, но без непосредственного участия платежных сетей VisaNet и MasterCard Worldwide Network. По этой причине международные платежные компании продолжают инвестировать средства в развитие сети и расширяют свои возможности по проведению внутренних транзакций. Например, до создания единой зоны платежей в евро проведение внутренних транзакций, выполненных при помощи дебетовых карт, полностью контролировалось национальными операторами. Однако в настоящее время MasterCard непосредственно участвует в проведении определенной доли внутренних транзакций, выполненных с использованием дебетовых карт, практически во всех странах зоны евро.

¹ <http://www.equens.com> (см. документ: Times of change).

² Там же.

³ <http://www.bankofgreece.gr> (см. документ: The Eurosystem's view of a SEPA for cards).

⁴ <http://www.ecb.int> (см. документ: Retail payments — integration and innovation).

⁵ <http://www.bundesbank.de> (см. документ: Single euro payment area).

РЕГУЛИРОВАНИЕ ДЕЯТЕЛЬНОСТИ МПС

В качестве одного из основных рисков для международных платежных систем выступает регулирование со стороны государства, препятствующее расширению деятельности МПС. В последние годы во многих странах существенно выросло регулирование платежных отраслей. Основная деятельность национальных правительств и контролирующих органов направлена:

- на регулирование и законодательное ограничение деятельности, связанной с установлением межбанковской комиссии по операциям (комиссии за обмен данными) и других цен;
- регулирование рынка какого-либо продукта или платежной отрасли в целом;
- проблемы в области конкуренции, вызванные действиями правительства, т.е. протекционистская политика национальных правительств.

Существенный интерес национальных правительств привлекает межбанковская комиссия по операциям. Во многих странах, например в странах Европейского союза и США, этот показатель не устанавливается исключительно в рамках платежной системы, а пересматривается и регулируется законодательно. Несмотря на тот факт, что межбанковская комиссия за совершение операции не является источником доходов для платежных компаний, законодательное регулирование комиссии может существенным образом повлиять на доходы международных карточных платежных систем. Комиссия за совершение операции выплачивается эквайером банку — эмитенту карты, т.е. в конечном итоге перекладывается на продавца, принимающего карты определенной платежной сети к оплате. Таким образом, изменение комиссии за совершение платежа может повлиять на спрос со стороны конечных пользователей платежных продуктов, т.е. на объем и число транзакций в рамках платежной системы и, как следствие, на ее доходы. Можно выделить следующие недавние примеры законодательного регулирования межбанковской комиссии за совершение операции и торгового дисконта:

- в мае 2009 г. парламент Франции приступил к рассмотрению законопроекта, регулирующего торговый дисконт. В октябре 2010 г. существенно измененная версия закона была принята, однако уже в январе 2011 г. законопроект был опротестован в Конституционном суде Франции;
- в июне 2009 г. Сенат Канады опубликовал доклад, в котором в качестве обязательной рекомендации было указано установление нулевой комиссии за совершение транзакции по дебетовым картам сроком на три года. Кроме того, в докладе рекомендовалось разрешить повышение ставки дисконта для продавцов, а также внести поправки в некоторые правила работы с картами. В ответ на этот доклад министерство финансов ввело в действие добровольный Кодекс поведения для участников карточной платежной отрасли. На рассмотрение в Сенат Канады также поступали законопроекты, ставящие своей целью установление законодательного или регулятивного

контроля над комиссией за совершение операции и аналогичными сферами платежной системы;

- в декабре 2009 г. парламент Венгрии приступил к рассмотрению законопроекта, регулирующего комиссии за совершение операции и торговый дисконт. В феврале 2010 г. был принят закон, предусматривающий регулирование только торгового дисконта. Однако впоследствии в январе 2011 г. закон был отменен;
- в мае 2010 г. Центральный банк Бразилии совместно с ведомствами по защите конкуренции опубликовал отчет, содержащий выводы относительно розничной платежной системы Бразилии и в том числе вывод о том, что процесс установления внутренних комиссий за совершение транзакции должен быть более прозрачным;
- в июле 2010 г. в США был утвержден законопроект (Wall Street Reform and Consumer Protection Act¹), который, в частности, требует, чтобы комиссии за совершение операций по дебетовым и предоплаченным картам были обоснованными и пропорциональны издержкам, понесенным эмитентом при совершении транзакции.

Центральные банки и регулирующие органы некоторых стран также рассматривали данный вопрос и предпринимали различные действия в области установления комиссий за совершение платежа и в аналогичных сферах работы карточных платежных систем. В 2002 году Резервный банк Австралии ввел правила, контролирующие издержки, которые могут быть учтены в процессе установления комиссий за совершение транзакции в четырехсторонних карточных платежных системах. Эти правила впоследствии пересматривались, однако не были отменены.

Можно привести следующие недавние примеры регулятивных мер в разных странах, с которыми столкнулась платежная сеть MasterCard:

- в январе 2007 г. Управление по защите конкуренции и потребителей Польши выпустило постановление о том, что внутренние комиссии за совершение операций в рамках платежной системы противоречат польскому законодательству в области конкуренции, а также наложило штрафы на финансовые организации, имеющие разрешение на деятельность от MasterCard;
- в феврале 2007 г. Управление по добросовестной конкуренции Великобритании приступило к изучению текущих комиссий за совершение операций по кредитным и дебетовым картам с «немедленным списанием» средств с целью выяснить, противоречат ли данные комиссии законодательству Великобритании и Евросоюза в сфере конкуренции;
- в декабре 2007 г. Европейская комиссия решила, что трансграничные комиссии за совершение операций по кредитным и дебетовым картам в рамках платежной сети MasterCard не соответствуют правилам конкуренции Европейского союза;

¹ Public Law 111-203, 111th Congress (см.: <http://www.gpo.gov>).

- в декабре 2009 г. в Венгрии на компанию MasterCard был наложен штраф в размере около 3 млн дол. США, причиной которого стало несоответствие внутренних комиссий за совершение операций законам страны в сфере конкуренции. В настоящий момент платежная компания оспаривает решение Венгерского конкурентного ведомства;
- в сентябре 2010 г. компания MasterCard получила уведомление от Резервного банка Южно-Африканской Республики о том, что намеревается направить в компанию независимого консультанта для составления рекомендаций по упрощению структуры комиссий за совершение платежей в рамках всей платежной системы Южно-Африканской Республики;
- платежная сеть Mastercard оспаривает решение Комитета конкуренции Италии, принятое в ноябре 2010 г., согласно которому MasterCard должна уплатить штраф в размере 2,7 млн евро. Причиной штрафа вновь стало несоответствие комиссий за совершение операций национальным законам в сфере конкуренции;
- в декабре 2010 г. Бюро по конкуренции Канады совместно с Трибуналом по конкуренции подало заявление об отмене правил MasterCard, связанных с комиссиями по совершению операций;
- в июне 2011 г. депутаты Государственной Думы утвердили текст парламентского запроса главе ФАС России о проведении проверки тарифной политики МПС и условий участия в них банков. Кроме того, депутаты Госдумы не исключали возможность сговора крупнейших платежных систем на российском рынке (Visa и MasterCard). Штрафы за соответствующие нарушения в сфере конкуренции составляют до 2% от оборота компании за злоупотребление доминирующим положением и до 4% от оборота за сговор, ограничивающий конкуренцию¹.

Аналогичные проблемы возникали у компании MasterCard в таких странах, как Бельгия, Колумбия, Чехия, Эстония, Израиль, Латвия, Нидерланды, Норвегия, Словакия, Турция, Венесуэла.

Существенные усилия, направленные на снижение комиссий за совершение операций, исходят не только от регулирующих и законодательных органов власти, но и от продавцов. Например, в США продавцы возбудили десятки коллективных и индивидуальных исков, обвиняющих Visa, MasterCard и другие платежные компании в том, что комиссии платежных сетей и правила принятия в платежные системы противоречат антимонопольному законодательству. В частности, в исках говорится о том, что принцип установления комиссий основан на горизонтальном фиксировании цен² компаниями MasterCard, Visa, а также

¹ <http://www.fas.gov.ru>

² Horizontal price-fixing имеет место, когда несколько производителей схожих товаров или услуг договариваются о поддержании цен на определенном уровне, т.е. действуют как единая монополия.

банками — членами их платежных сетей. Мнение самих платежных компаний¹ по этому вопросу состоит в том, что занижение комиссий может привести к ситуации, когда эмитенты платежных карт не смогут покрывать издержки, связанные с обслуживанием транзакций. Это приведет к снижению числа финансовых организаций-эмитентов, участвующих в платежной системе, и снижению объема транзакций, проводимых в рамках системы. Эмитенты могли бы назначать более высокие комиссии для держателей карт, что, однако, снижало бы привлекательность карточных программ для конечных потребителей и, как следствие, уменьшало бы объем транзакций в платежной системе и прибыли эмитентов. В итоге деятельность, направленная на снижение комиссий за совершение операций, вынуждает эмитентов пытаться снизить комиссии, которые взимаются с них платежными компаниями.

Можно привести другие примеры вмешательства органов государственной власти в деятельность платежных сетей. В феврале 2011 г. Антимонопольный комитет Нидерландов направил компании MasterCard отчет о возражениях, касающихся правил и политики платежной сети в области совместной маркировки платежных карт. (Согласно требованиям платежных компаний, в некоторых случаях на платежную карту может быть нанесен только логотип платежной сети.) В июле 2010 г. Швейцарское антимонопольное ведомство (WEKO) начало изучение внутренних комиссий, взимаемых с эквайеров, основываясь на поступающих от них жалобах. Ведомство хотело определить, требуется ли обязать компанию MasterCard прекратить взимание этой комиссии. Однако после представления платежной компанией дополнительной информации по данному вопросу жалобы банков были отклонены.

В июне 2010 г. в ответ на жалобы Украинской банковской ассоциации Антимонопольный комитет Украины направил компании MasterCard комплексный запрос, касающийся информации о правилах компании и внутренних комиссиях.

ПРОТЕКЦИОНИСТСКАЯ ПОЛИТИКА

Правительства некоторых стран, например России, Украины и Индии, проводят протекционистскую политику по отношению к отдельным национальным карточным платежным системам и операторам. С целью поддержки национальных карточных платежных операторов правительства ограничивают участие международных карточных операторов на локальных рынках. Законодательство некоторых стран также требует, чтобы внутренние платежи обрабатывались в центрах, находящихся на территории страны, или же только национальными компаниями.

Так, лидирующие позиции в Японии занимает платежная компания JCB, а в Китае — China Union Pay. Согласно законодательным требованиям СUP является единственным внутренним оператором и проводит всю информацию о наци-

¹ <http://www.mastercard.com> (см. документ: MasterCard Annual Report 2010).

ональных межбанковских карточных платежах в рамках собственной платежной сети.

China UnionPay была создана в марте 2002 г. по решению Государственного совета и Народного банка Китая. Первая кредитная карта, принадлежащая платежной системе, была выпущена в августе 2003 г., а первая дебетовая карта — в мае 2004 г. В начале 2005 г. карты UnionPay начали принимать в Сингапуре, Таиланде и Корее, что означало выход национальной платежной сети на международный рынок платежных услуг. В сентябре 2005 г. было подписано соглашение, в соответствии с которым платежные карты UnionPay начали приниматься в сети банкоматов Citicorp. В конце 2005 г. карты UnionPay начали принимать к оплате в США, а также в банкоматах некоторых европейских стран, а именно в Германии, Франции, Испании, Бельгии и Люксембурге. В августе 2008 г. карты UnionPay впервые стали эмитироваться в России.

Менее чем за десять лет UnionPay превратилась в центральную составляющую карточного рынка Китая и отвечает за работу единой межбанковской клиринговой и расчетной системы. Одним из важных направлений деятельности платежной системы UnionPay является международная экспансия. По состоянию на 2011 г. совокупное количество платежных карт UnionPay, выпущенных по всему миру, превысило 2,1 млрд. В 2009 году число межбанковских карточных транзакций в системе достигло 7 млрд и составило 1,1 трлн дол. США. Число продавцов, количество терминалов в местах продаж, а также банкоматов в рамках платежной системы достигло 2,13 млн; 2,88 млн и 930 тыс. соответственно. UnionPay заключила партнерские отношения примерно с 400 финансовыми организациями по всему миру.

На текущий момент международная платежная сеть UnionPay охватывает всю территорию Китая. Кроме того, карты CUP также принимаются в 117 странах и регионах, расположенных на пяти континентах. При этом более десяти из этих стран, включая Японию, Корею, Сингапур, Россию и Монголию, выпускают платежные карты UnionPay. Таким образом, в рамках платежной системы UnionPay выполняются межбанковские, межрегиональные и трансграничные платежи.

Японская платежная сеть JCB была основана в 1961 г. и вышла на международный рынок платежей в 1981 г. Первая карта сети JCB, эмитированная за пределами Японии, была выпущена в 1983 г. в Гонконге. Уже в 1987 г. платежные карты JCB принимались к оплате более чем в 100 странах и на территориях по всему миру. В последующие годы компания проводила активную экспансию на рынке международных карточных продуктов: в настоящее время карты JCB принимаются к оплате более чем в 190 странах. В 2006 году JCB подписала долгосрочное соглашение о сотрудничестве с платежной сетью Discover, согласно которому карты каждой из сетей принимаются в банкоматах и к оплате в сети партнера.

В настоящее время в Индии идет процесс создания национальной карточной платежной сети под названием RuPay, которой руководит национальная платежная корпорация Индии. Одной из целей создания национальной карточной

системы является снижение издержек индийских банков, которое должно быть достигнуто благодаря конкуренции между национальной и международными карточными системами. Кроме того, создание национальной карточной сети позволит хранить информацию о совершенных транзакциях внутри страны, а не за ее пределами. Карты новой национальной системы будут эмитироваться в соответствии с международными стандартами, однако экспансия системы RuPay на рынок международных платежей не предполагается. Эмиссия первой дебетовой карты запланирована на март 2012 г.

В России 27 июня 2011 г. был подписан Федеральный закон № 161-ФЗ «О национальной платежной системе»¹ (далее — Закон о НПС), определяющий национальную платежную систему как «совокупность операторов по переводу денежных средств (включая операторов электронных денежных средств), банковских платежных агентов (субагентов), платежных агентов, организаций федеральной почтовой связи при оказании ими платежных услуг в соответствии с законодательством Российской Федерации, операторов платежных систем, операторов услуг платежной инфраструктуры (субъекты национальной платежной системы)». Отметим, что Законом не предусматривается создание национальной карточной платежной системы. Тем не менее обсуждается возможность выдачи социальных карт всем гражданам РФ на базе национальной платежной системы. Предполагается, что, во-первых, чип такой карты будет содержать всю необходимую информацию о владельце карты и, во-вторых, такую карту можно будет использовать как обычную банковскую карту (для совершения платежей и для получения зарплат, пособий, а также для выплаты налогов и т.д.)². Однако новый Закон предусматривает изменения, связанные с работой международных платежных систем на отечественном карточном рынке. Через три года после опубликования Закона в силу вступает положение (ч. 11 ст. 16), согласно которому операционный центр, осуществляющий денежные переводы внутри страны, должен находиться на территории России. Это фактически означает, что либо МПС должны построить операционные центры на территории России³, если сочтут такие вложения рентабельными, либо в России должен быть построен свой операционный центр для обработки данных. При обсуждении второго варианта немаловажным является вопрос о том, согласятся ли МПС передать проведение своих транзакций стороннему оператору, поскольку это противоречит базовому принципу их работы и функционирования — самостоятельному проведению своих платежей.

Специфика российского рынка платежных карт⁴ состоит в том, что порядка 85—90% операций, совершенных при помощи карт, приходится на снятие наличных денег через банкоматы. При этом абсолютное большинство (примерно 90%)

¹ <http://graph.document.kremlin.ru>

² <http://ria.ru>

³ Заметим, что компания Visa работает на базе четырех таких центров.

⁴ <http://www.cbr.ru> (см. документы: «Обзор российского рынка платежных карт. Тенденции и перспективы развития» и «Обзор российского рынка платежных карт за 2009 год»).

таких операций проводятся в рамках банкоматной сети банка — эмитента карты. Поскольку такие операции не проходят авторизацию через МПС, для непосредственного обслуживания международными процессинговыми центрами остается малая доля российского рынка карточных платежей. Это ставит под сомнение целесообразность строительства собственного операционного центра международными компаниями на территории России.

Возможным решением в данной ситуации может быть использование европейского опыта. Российская единая платежная карта может сочетать в себе два бренда — национальной и международной платежной системы. При совершении внутренней операции транзакция будет проходить через национальную систему, а при совершении трансграничной операции будет задействоваться МПС¹.

Мировой опыт показал, что за последние десятилетия по всему миру существенно снизилось количество национальных карточных платежных сетей, поскольку большинство стран предпочли использовать международные сети для совершения как международных, так и существенной доли внутренних платежей. Принятие международных систем в качестве полноправных участников национального рынка сопряжено в большинстве стран с регулированием деятельности МПС в сфере ценообразования и конкуренции.

Тем не менее в последние годы некоторые национальные платежные сети при поддержке государства стремятся стать активными участниками на рынке международных платежей. Кроме того, такие страны, как Индия и Россия, стремятся создать новые национальные платежные сети. Эти факторы оказывают влияние и на развитие международных платежных систем.

Приложение к главе 3

Список использованных материалов

1. Материалы сайта платежной сети Diners Club: <http://www.dinersclubinternational.com>
2. Материалы сайта платежной сети Visa: <http://visa.com>
3. Материалы сайта платежной сети MasterCard: <http://www.mastercard.com>
4. Материалы сайта платежной сети China UnionPay: <http://www.unionpay.com>
5. Материалы сайта платежной сети Japan Credit Bureau: <http://www.jbccorporat.com>
6. Материалы сайта компании EMVCo: <http://www.emvco.com/>
7. Материалы сайта компании Equens: <http://www.equens.com>
8. Материалы Европейской Комиссии: <http://ec.europa.eu>
9. Материалы ЕЦБ и ЦБ отдельных стран: <http://www.ecb.int>, <http://www.bundesbank.de>, <http://www.bankofgreece.gr>

¹ <http://bankir.ru>

10. Материалы U.S. GPO: <http://www.gpo.gov>
11. Материалы Банка России: <http://www.cbr.ru>
12. Материалы ФАС России: <http://www.fas.gov.ru>
13. Материалы РИА Новости: <http://ria.ru>
14. Материалы <http://bankir.ru>
15. Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе».

ГЛАВА 4

ПЛАТЕЖНЫЕ И РАСЧЕТНЫЕ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

4.1. БАНКОВСКАЯ СИСТЕМА РОССИЙСКОЙ ФЕДЕРАЦИИ

Банковская система — это регулируемые банковским правом структурные, институциональные и функциональные взаимосвязи между центральным банком и кредитными организациями, которые возникают, изменяются и прекращаются в связи с осуществлением банковского регулирования и банковского надзора. Банковская система России является двухуровневой.

Первый уровень банковской системы представлен Центральным банком Российской Федерации (Банком России). Банк России, являясь юридическим лицом, одновременно осуществляет функции органа государственного управления. Он выполняет возложенные на него функции и задачи на основании Федерального закона от 10 июля 2002 г. «О Центральном банке Российской Федерации (Банке России)» (далее — Закон о Банке России). В этом Законе в качестве целей деятельности Банка России установлено наряду с обеспечением устойчивости рубля и банковской системы Российской Федерации обеспечение стабильности и развитие национальной платежной системы.

Банк России по вопросам своей компетенции имеет право издавать нормативные акты, обязательные для федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, всех юридических и физических лиц, действующих в сфере финансовых отношений. Он является важным субъектом финансовых взаимоотношений и влияет на формирование банковского законодательства.

Банковское законодательство содержит нормативные акты, относящиеся к банковской деятельности, т.е. устанавливающие правовое положение самих банков и иных кредитных организаций, регулирующие публичные отношения банков, а также частноправовые отношения банков с клиентами.

Второй уровень банковской системы представлен кредитными организациями, которые в целях получения прибыли осуществляют свою деятельность, направленную на удовлетворение потребностей общества в банковских платежных услугах.

Кредитная организация — это юридическое лицо, которое для извлечения прибыли как основной цели своей деятельности на основании своего устава и специального разрешения (лицензии)¹ Банка России имеет право осуществлять банковские операции. В соответствии с Федеральным законом от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» (далее Закон о банках и банковской деятельности) в России кредитные организации разделяются на банки и небанковские кредитные организации.

Кредитная организация создается в виде хозяйственного общества² на основе любых форм собственности, предусмотренных законодательством.

Банк — это кредитная организация, которая имеет исключительное право осуществлять в совокупности следующие банковские операции:

- привлечение во вклады денежных средств физических и юридических лиц;
- размещение указанных средств от своего имени и за свой счет на условиях возвратности, платности, срочности;
- открытие и ведение банковских счетов физических и юридических лиц.

Небанковская кредитная организация имеет право осуществлять лишь отдельные банковские операции (на которые выдана лицензия). Обычно небанковские кредитные организации осуществляют расчетные, депозитно-кредитные операции и операции инкассации.

Кредитные организации могут создавать союзы и ассоциации, не преследующие цели извлечения прибыли, для защиты и представления интересов своих членов, координации их деятельности, развития межрегиональных и международных связей, удовлетворения научных, информационных и профессиональных интересов, выработки рекомендаций по осуществлению банковской деятельности и решению иных совместных задач. Союзам и ассоциациям кредитных организаций запрещается осуществление банковских операций.

Кроме союзов и ассоциаций кредитные организации могут входить в состав финансово-промышленных объединений, таких как банковская группа и банковский холдинг.

Банковской группой признается не являющееся юридическим лицом объединение кредитных организаций, в котором одна (головная) кредитная организация оказывает прямо или косвенно (через третье лицо) существенное влияние

¹ См. инструкцию Банка России от 2 апреля 2010 г. № 135-И «О порядке принятия Банком России решения о государственной регистрации кредитных организаций и выдаче лицензий на осуществление банковских операций» (далее — Инструкция № 135-И) // Вестник Банка России. 2010. № 23.

² Акционерное общество (открытое или закрытое), общество с ограниченной ответственностью, общество с дополнительной ответственностью.

на решения, принимаемые органами управления другой (других) кредитной организации (кредитных организаций). Банковская группа образуется для решения совместных задач (совместного осуществления банковских операций) путем заключения соответствующего договора между двумя или несколькими кредитными организациями.

Банковским холдингом признается не являющееся юридическим лицом объединение юридических лиц с участием кредитной организации (кредитных организаций), в котором юридическое лицо, не являющееся кредитной организацией (головная организация банковского холдинга), имеет возможность прямо или косвенно (через третье лицо) оказывать существенное влияние на решения, принимаемые органами управления кредитной организации (кредитных организаций).

В целях повышения конкурентоспособности экономики Российской Федерации, ее диверсификации, стимулирования инвестиционной деятельности и финансирования крупных инфраструктурных проектов был создан Банк развития и внешнеэкономической деятельности (Внешэкономбанк). Внешэкономбанк является государственной корпорацией, созданной Российской Федерацией, статус, цели деятельности, функции и полномочия которой определяются Федеральным законом от 17 мая 2007 г. № 82-ФЗ «О Банке развития». Банк развития осуществляет инвестиционную, внешнеэкономическую, страховую, консультационную и другие виды деятельности, направленные на реализацию проектов в Российской Федерации и за рубежом. На Внешэкономбанк не распространяются некоторые положения законодательства о банках и банковской деятельности. Внешэкономбанк является инструментом реализации государственной экономической политики, направленной на решение задач по преодолению инфраструктурных ограничений экономического роста, повышению эффективности использования природных ресурсов, развитию высокотехнологичных отраслей промышленности, раскрытию инновационного и производственного потенциала малого и среднего бизнеса, поддержке экспорта промышленной продукции и услуг.

В банковскую систему также включена организация, которая имеет финансовый характер, однако ее деятельность не связана с проведением банковских операций, но так или иначе затрагивает состояние банковской системы. Этой организацией является Агентство по страхованию вкладов. Оно было зарегистрировано в январе 2004 г. как юридическое лицо, целью деятельности которого является обеспечение функционирования системы страхования вкладов. Агентство ведет реестр банков, осуществляет сбор страховых взносов и выполняет контроль за их поступлением в Фонд обязательного страхования вкладов, размещает и (или) инвестирует временно свободные денежные средства Фонда в порядке, определенном Федеральным законом от 23 декабря 2003 г. № 177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации». Кроме этого Агентство выполняет функцию конкурсного управляющего при банкротстве кредитных организаций, имевших лицензию на привлечение денежных средств

физических лиц во вклады, а также наделено правами по финансовому оздоровлению банков.

К сфере функционирования банковской системы России следует также отнести учреждения банковской инфраструктуры, которая объединяет организации, профессионально обеспечивающие деятельность любых кредитных организаций всех уровней, проведение ими банковских операций и сделок. Задачами таких учреждений банковской инфраструктуры являются:

- обеспечение средствами связи и коммуникаций (специализированные, компьютерные, системы связи и др.);
- обеспечение безопасности деятельности, экономической информации и т.д. (агентства безопасности, специализирующиеся в кредитной сфере, фирмы технической защиты информации и др.);
- информационное обеспечение (специализированные информационно-аналитические центры банковской информации, рейтинговые агентства, кредит-бюро и т.п.);
- кадровое обеспечение (высшие и средние учебные заведения банковской специализации, учебные центры, фирмы и агентства по набору и обучению кадров);
- научное, правовое и методическое обеспечение (научные центры и лаборатории, учебные заведения).

4.2. ПЛАТЕЖИ И РАСЧЕТЫ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Платежная система Российской Федерации является основной инфраструктурной составляющей национальной финансовой системы, предназначенной для перевода денежных средств между различными субъектами экономики. Эта система связывает друг с другом различные сферы экономики, объединяет региональные сегменты в единую систему государственных финансов, обеспечивает финансовое взаимодействие хозяйствующих субъектов между собой, а также физических лиц, юридических лиц и государства.

Безналичные расчеты в Российской Федерации осуществляются:

- через платежную систему Банка России;
- частные платежные системы;
- платежные системы государственных банковских организаций (Внешэкономбанк, Сбербанк России, ВТБ, Россельхозбанк и т.п.);
- платежные системы государственных учреждений (Федеральное казначейство, Почта России и т.п.).

Платежная система Банка России, частные и государственные платежные системы действуют на основании Гражданского кодекса Российской Федерации (далее — ГК РФ), федеральных законов «О национальной платежной системе», «О Центральном банке Российской Федерации (Банке России)», «О банках и бан-

ковской деятельности», «О банке развития», от 7 августа 2001 г. «О деятельности по приему платежей физических лиц, осуществляемой платежными агентами», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее — Закон о противодействии легализации доходов), других федеральных законов, а также нормативных документов Банка России.

Основным документом, регулирующим платежно-расчетные взаимоотношения в России, является ГК РФ¹, который содержит основные нормы, регулирующие наличные и безналичные расчеты в России. Кодексом установлено, что расчеты между юридическими лицами и расчеты с участием граждан осуществляются наличными деньгами и в безналичном порядке; а также в нем определены условия договоров банковского вклада и банковского счета, включающие тайну банковского счета, очередность списания денежных средств со счета при недостаточности денежных средств на счете для удовлетворения всех предъявленных к нему требований (приоритетность исполнения в зависимости от типа платежа), сроки проведения операций по счету, формы расчетов и ответственность участников за проведение платежа.

Федеральные законы о НПС и о Банке России устанавливают полномочия Банка России в области платежей. Банк России наряду с другими выполняемыми им функциями устанавливает правила осуществления расчетов в Российской Федерации и осуществляет расчетное обслуживание счетов бюджетов бюджетной системы Российской Федерации, проводит межбанковские безналичные расчеты.

Закон о НПС устанавливает правовые и организационные основы национальной платежной системы, регулирует порядок оказания платежных услуг, в том числе порядок осуществления перевода денежных средств, использования электронных средств платежа, деятельность субъектов национальной платежной системы, а также определяет требования к организации и функционированию платежных систем, порядок осуществления надзора и наблюдения в национальной платежной системе².

В сфере надзора в национальной платежной системе включены как кредитные организации, являющиеся операторами платежных систем, операционными центрами, клиринговыми центрами, так и организации, не являющиеся кредитными. За первыми надзор будет осуществляться в рамках банковского надзора с его инструментами и мерами воздействия. За вторыми (не являющимися кредитными организациями) Банком России будет осуществляться надзор непосредственно на основании норм Закона о НПС.

В отличие от надзора в национальной платежной системе, который нацелен на обеспечение исполнения законодательных и нормативных требований, наблюде-

¹ Статьи 140, 861—885 ГК РФ предусматривают применение на территории Российской Федерации платежей в наличной и безналичной форме и раскрывают сущность и порядок осуществления основных форм безналичных расчетов.

² В соответствии с Законом о НПС надзор и наблюдение в национальной платежной системе осуществляется Банком России.

ние в НПС ориентировано на задачи развития, следования стандартам лучшей мировой и отечественной практики, рекомендациям Банка России в целях обеспечения оптимального решения кредитными организациями и платежными системами задач эффективности и бесперебойности, а также адекватности НПС потребностям экономики, банковского сектора и финансового рынка Российской Федерации.

Национальная платежная система России определяется как совокупность операторов по переводу денежных средств (включая операторов электронных денежных средств), банковских платежных агентов (субагентов), платежных агентов, организаций федеральной почтовой связи при оказании ими платежных услуг в соответствии с законодательством Российской Федерации, операторов платежных систем, операторов услуг платежной инфраструктуры (субъекты НПС).

Основными организациями (расчетными институтами), через которые совершаются платежи в Российской Федерации, являются Банк России, банки и расчетные небанковские кредитные организации (РНКО). Осуществление платежей и расчетов между банковскими организациями через корреспондентские счета, открытые в бухгалтерском учете кредитных организаций и их филиалов, а также в расчетных подразделениях Банка России, принято называть межбанковскими расчетами. Структурная схема осуществления межбанковских расчетов приводится на рис. 4.1¹.

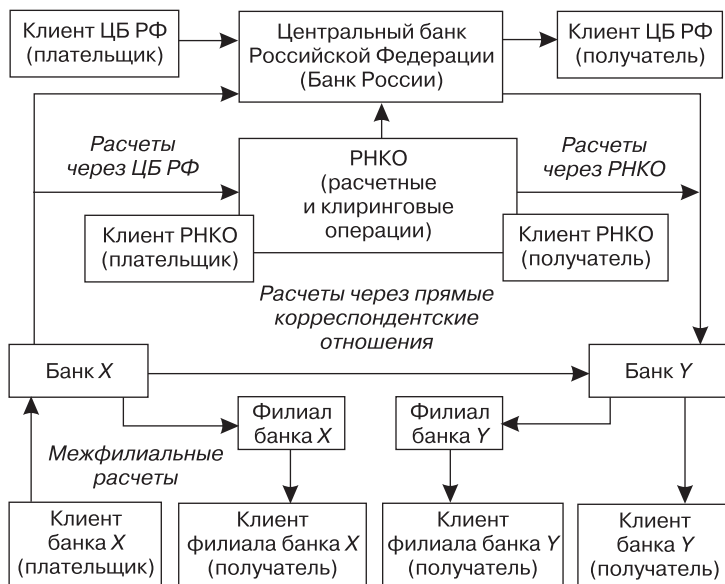


Рис. 4.1. Структурная схема осуществления межбанковских расчетов

¹ Подробнее о Законе о НПС см. главу 10.

4.3. ДЕНЕЖНЫЕ ПЕРЕВОДЫ И ПЛАТЕЖНЫЕ АГЕНТЫ

Денежный перевод — распространенная форма перевода денег по банковской или почтовой системе. В структуре денежного перевода всегда присутствует отправитель, получатель и посредник, взимающий за свои услуги определенную плату. Денежные переводы могут осуществляться в пределах одного государства и за рубеж, производиться в иностранной валюте или в рублях с возможностью взаимной конверсии.

Операции по переводу денежных средств в пользу юридических и физических лиц по поручению физических лиц могут осуществляться с открытием банковского (текущего) счета и без его открытия¹. При этом деятельность физических лиц при переводе денежных средств не должна быть связана с осуществлением ими предпринимательской деятельности.

При осуществлении безналичных расчетов по текущим счетам физическими лицами могут применяться установленные законодательством документарные формы безналичных расчетов (расчетные документы).

Банки осуществляют операции по переводу денежных средств по поручению физического лица без открытия банковского счета на основании представляемого физическим лицом документа. Форма документа, предназначенного для представления (заполнения) физическими лицами при перечислении денежных средств без открытия банковского счета, устанавливается банками либо соответствующими получателями средств, в адрес которых направляются платежи.

Порядок и условия осуществления операций по переводу денежных средств по поручению физических лиц без открытия банковского счета, включая порядок оплаты расчетных услуг, а также обязательства банка по переводу денежных средств, устанавливаются банком в соответствии с требованиями законодательства и нормативных актов Банка России. Информация, раскрывающая порядок и условия осуществления операций по переводу денежных средств, доводится до сведения физических лиц в доступной для ознакомления форме и считается принятой физическими лицами при подписании ими документов на перечисление денежных средств.

Законодательством Российской Федерации определяется функционирование платежных агентов двух основных видов:

- 1) платежный агент²;
- 2) банковский платежный агент³.

¹ См.: Положение Банка России от 1 апреля 2003 г. № 222-П «О порядке осуществления безналичных расчетов физическими лицами в Российской Федерации».

² Осуществляет свою деятельность на основании Закона о деятельности по приему платежей физических лиц, осуществляемой платежными агентами, который регулирует взаимоотношения платежного агента с другими участниками платежного процесса.

³ Осуществляет свою деятельность в соответствии с Законом о НПС.

Платежный агент — юридическое лицо или индивидуальный предприниматель, осуществляющие деятельность по приему платежей физических лиц.

Банковский платежный агент — юридическое лицо, за исключением кредитной организации, или индивидуальный предприниматель, которые привлекаются кредитной организацией в целях осуществления деятельности предоставления услуг по приему платежей, предусмотренной Законом о НПС.

Платежным агентом является оператор по приему платежей либо платежный субагент. Оператор по приему платежей — юридическое лицо, заключившее с поставщиком договор об осуществлении деятельности по приему платежей физических лиц. Платежный субагент — юридическое лицо или индивидуальный предприниматель, заключившие с оператором по приему платежей договор об осуществлении деятельности по приему платежей физических лиц. Плательщик — физическое лицо, осуществляющее внесение платежному агенту денежных средств в целях исполнения денежных обязательств физического лица перед поставщиком. Поставщик — юридическое лицо или индивидуальный предприниматель (за исключением кредитной организации), получающие денежные средства плательщика за реализуемые товары (выполняемые работы, оказываемые услуги и т.п.).

Под деятельностью по приему платежей физических лиц признается прием платежным агентом от плательщика денежных средств, направленных на исполнение денежных обязательств перед поставщиком по оплате товаров (работ, услуг). Прием платежей в основном осуществляется посредством программно-аппаратного комплекса, называемого платежным терминалом.

Платежный терминал — устройство для приема платежным агентом от плательщика денежных средств, функционирующее в автоматическом режиме без участия уполномоченного лица платежного агента.

Платежный агент осуществляет деятельность по приему от плательщика денежных средств, направленных:

- на исполнение денежных обязательств физического лица перед поставщиком по оплате товаров (работ, услуг);
- органам государственной власти, органам местного самоуправления и бюджетным учреждениям, находящимся в их ведении.

Кредитная организация вправе привлекать организацию, не являющуюся кредитной организацией, и индивидуального предпринимателя (банковский платежный агент) для принятия от физических лиц денежных средств.

При приеме платежей банковским платежным агентом кроме терминала может использоваться также и банкомат. Банкомат — устройство для осуществления в автоматическом режиме (без участия уполномоченного лица кредитной организации или банковского платежного агента) наличных денежных расчетов и (или) расчетов с использованием платежных карт.

Банковский платежный агент, являющийся юридическим лицом, в случаях, предусмотренных договором с оператором по переводу денежных средств, впра-

ве привлекать банковского платежного субагента на основании заключаемого с ним договора. Привлечение оператором по переводу денежных средств банковского платежного агента может осуществляться при соблюдении определенным законодательством требований.

На банковских и небанковских платежных агентов возлагается обязанность по составлению документов и предоставлению информации, подтверждающей платежные операции.

Процесс осуществления платежей включает следующие основные виды деятельности:

- прием платежей от физических лиц;
- сдача наличных денежных средств в кредитную организацию;
- перечисление денежных средств поставщику.

Процедуры расчета по платежам физических лиц и порядок взаимодействия с кредитными организациями и другими участниками расчетов должны выполняться в соответствии с нормативно-правовыми документами, регламентирующими соответствующие виды деятельности.

4.4. ПЛАТЕЖНАЯ СИСТЕМА БАНКА РОССИИ

Цели деятельности Банка России, его функции и полномочия в отношении платежной системы и расчетов определяют платежную систему Банка России в качестве одного из ключевых механизмов реализации денежно-кредитной и бюджетной политики в Российской Федерации, обеспечивают ее доминирующую роль в платежной системе Российской Федерации. Через платежную систему Банка России осуществляются значительные по количеству и преобладающие по объему доли платежей, проводимых в платежной системе Российской Федерации.

Вышеизложенные факторы определяют платежную систему Банка России как системно значимую платежную систему в Российской Федерации. Банк России осуществляет регулирование, оперативное управление и мониторинг собственной платежной системы, обеспечивает наблюдение за ней, а также исполняет свои обязательства перед другими участниками платежной системы Банка России.

В платежной системе Банка России функционируют системы расчетов, различающиеся по территориальному охвату и объему проводимых платежей, правилам и регламенту функционирования, составу участников и расчетным документам, скорости проведения платежей и используемой технологии, включающие в себя:

- систему банковских электронных срочных платежей (система БЭСП), предназначенную для осуществления расчетов в режиме реального времени в масштабах всей страны;

- более семидесяти отдельных систем внутрирегиональных электронных расчетов, работающих в непрерывном режиме;
- систему внутрирегиональных электронных расчетов Московского региона, функционирующую как в режиме рейсов, так и в непрерывном режиме;
- систему межрегиональных электронных расчетов, позволяющую осуществлять перевод денежных средств между регионами России в течение одного-двух операционных дней;
- системы расчетов с применением авизо (телеграфных и почтовых), основанные на использовании бумажных технологий, позволяющие осуществлять перевод денежных средств вне зависимости от территориальной привязки в течение одного — пяти операционных дней;
- ряд специализированных расчетных механизмов для отдельных регионов России и подразделений Банка России (расчеты между учреждениями Банка России, обслуживаемыми одним вычислительным центром, расчеты в пределах одного учреждения Банка России, межрегиональные расчеты по сделкам на рынке государственных ценных бумаг, межрегиональные расчеты по сделкам на единой торговой сессии межбанковских валютных бирж).

Участниками платежной системы Банка России являются Банк России в лице своих подразделений, кредитные организации (филиалы), Федеральное казначейство и его территориальные органы, а также другие клиенты Банка России, не являющиеся кредитными организациями (филиалами).

Каждая кредитная организация, расположенная на территории Российской Федерации, после получения лицензии Банка России в обязательном порядке открывает корреспондентский счет в учреждении Банка России по месту ее нахождения. Кредитная организация вправе также открыть в учреждении Банка России корреспондентский субсчет своему филиалу по месту его нахождения. Другие клиенты открывают в подразделениях расчетной сети Банка России банковские счета, которые могут быть использованы для осуществления платежей.

Идентификация участников платежной системы Банка России осуществляется с использованием нескольких справочников — справочника БИК России (для структурных подразделений Банка России, кредитных организаций и их филиалов), справочника участников системы БЭСП (для клиентов и структурных подразделений Банка России — участников системы БЭСП), а также локальных справочников, ведущихся в каждой региональной компоненте платежной системы Банка России (для всех клиентов, включая тех, которые не являются кредитными организациями и их филиалами). В справочниках применяются уникальные российские коды идентификации. Номера банковских счетов клиентов формируются по российской методике.

В платежной системе Банка России функции управления (в том числе оперативного) платежной системой Банка России и мониторинга ее функционирования распределены между тремя уровнями: федеральным (система БЭСП —

центральный аппарат Банка России), региональным (региональные компоненты — территориальные учреждения Банка России) и локальным (подразделения расчетной сети Банка России).

Функционирование платежной системы Банка России в настоящее время обеспечивается в основном системой коллективной обработки информации, включающей коллективные центры обработки информации высокой доступности, а также транспортной системой электронных расчетов и средой взаимодействия с клиентами Банка России. Обработка платежной информации ряда территориальных учреждений Банка России осуществляется вне системы коллективной обработки информации.

Расчеты в платежной системе Банка России осуществляются в основном валовыми методами, а используемые платежные инструменты и формы расчетов следующие:

- налично-денежные платежи;
- документарные платежи на базе платежных поручений, аккредитивов, платежных требований и инкассовых поручений.

Банком России и инфраструктурными организациями финансовых рынков установлен порядок функционирования расчетных механизмов по сделкам на рынке государственных ценных бумаг и единой торговой сессии межбанковских валютных бирж, позволяющий завершать расчеты в установленный срок, при этом часть расчетов по указанным сделкам завершается с использованием денежных средств на банковских счетах, открытых не в Банке России, а в кредитных организациях.

В платежной системе Банка России технологии обработки платежной информации и клиентские интерфейсы обмена электронными сообщениями различаются в зависимости от используемых систем расчетов набором используемых электронных сообщений, способом защиты платежной информации и транспортной средой. В платежной системе Банка России реализованы собственные унифицированные форматы электронных банковских сообщений, основанные на российских стандартах расчетных документов, отличающихся от международных стандартов в части состава реквизитов и размерности полей. В связи с этим взаимное преобразование электронных банковских сообщений, используемых в платежной системе Банка России, и финансовых сообщений, составленных в соответствии с международными стандартами, в ряде случаев осуществляется с применением операций, выполняемых ручным способом.

Платежи в платежной системе Банка России проводятся на платной основе и бесплатно в соответствии с законодательством Российской Федерации.

Для расширения возможности управления ликвидностью на корреспондентских счетах в Банке России предусматриваются процедуры рефинансирования (кредитования) кредитных организаций. В рамках рефинансирования кредитным организациям могут быть предоставлены внутрисдневные, овернайт и ломбардные кредиты. Внутрисдневной кредит — кредит Банка России, предостав-

ляемый кредитной организации путем осуществления платежа с ее счета сверх остатка денежных средств на данном счете в пределах установленного лимита кредитования, со сроком погашения в течение дня. Кредит овернайт — кредит Банка России, предоставляемый кредитной организации в конце дня в сумме непогашенного внутрисуточного кредита, сроком на один рабочий день. Ломбардный кредит — кредит Банка России, предоставляемый банку по его заявлению на получение ломбардного кредита по фиксированной процентной ставке или заявке на участие в ломбардном кредитном аукционе.

Развитие Банком России собственной платежной системы направлено на рост ее эффективности за счет сокращения издержек, улучшения качества предоставляемых услуг, повышения быстродействия как при проведении платежей, так и при выполнении запросов и управляющих воздействий, а также на снижение в ней кредитного риска, риска ликвидности, операционного, системного и правового рисков.

Основу перспективной платежной системы Банка России будет составлять единая, универсальная, централизованная на федеральном уровне многосервисная система расчетов, в которой реализуются функциональные возможности системы БЭСП и возможности действующих сервисов региональных компонент платежной системы Банка России. Через данную систему будут проводиться срочные и несрочные платежи в валюте Российской Федерации по правилам, установленным Банком России, в едином регламенте с использованием специализированных расчетных сервисов, предоставляемых участникам платежной системы Банка России.

Развитие платежной системы Банка России будет осуществляться в два этапа. На первом этапе развития платежной системы Банка России (2010—2013 гг.) формируется федеральная компонента, а также совершенствуется система БЭСП; на втором этапе (2014—2015 гг.) создается единая система валовых и нетто-расчетов, предоставляющая услуги по срочным и несрочным платежам всем участникам платежной системы Банка России¹.

4.5. ЧАСТНЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ

Частные платежные системы в России представлены системами, которые организованы банками или расчетными небанковскими кредитными организациями (НКО), которые находятся в собственности физических лиц и (или) юридических лиц без существенного государственного участия. Кроме этого операторами частных платежных систем могут являться международные и российские организации, специализирующиеся на предоставлении операционных услуг.

¹ Более подробно о функционировании и развитии платежной системы Банка России см.: Концепция развития платежной системы на период до 2015 года // Вестник Банка России. 2010. № 44.

В рамках функционирования частных платежных систем могут использоваться любые платежные инструменты, как в документарной, так и в бездокументарной форме.

По способу платежно-расчетных взаимоотношений в межбанковских платежных системах они разделяются на следующие виды:

- внутрибанковские платежные системы для расчетов между учреждениями одной кредитной организации;
- платежные системы кредитных организаций для расчетов по корреспондентским счетам, открытым в других кредитных организациях;
- платежные системы расчетных небанковских кредитных организаций.

Через внутрибанковские платежные системы осуществляются расчеты между головной кредитной организацией и ее филиалами и между филиалами по внутрибанковским платежным системам. Порядок проведения расчетных операций по этой платежной системе определяется кредитной организацией самостоятельно во внутрибанковских правилах с соблюдением требований, установленных Банком России. Наличие у кредитной организации внутрибанковской платежной системы позволяет ей не иметь корреспондентских субсчетов в учреждениях Банка России по месту нахождения каждого из филиалов, что способствует уменьшению потребности в ликвидных средствах.

Открытие взаимных корреспондентских счетов и проведение платежно-расчетных операций по этим счетам регулируются законодательством, правилами, установленными в нормативных документах Банка России, а также двусторонними договорами между кредитными организациями. Правилами разрешено проведение кредитной организацией транзитных платежей, т.е. платежей между кредитными организациями, с которыми у нее имеются корреспондентские отношения. Проведение кредитными организациями платежей через корреспондентские счета, открытые в других кредитных организациях, направлено на ускорение расчетов и экономию ликвидности. Правила, установленные Банком России, способствуют снижению рисков при проведении расчетных операций по корреспондентским счетам кредитных организаций, открытым в других кредитных организациях.

Расчетные небанковские кредитные организации (НКО) открывают счета участников расчетов кредитным организациям и другим юридическим лицам и осуществляют расчеты между ними по договору как на валовой, так и на нетто-основе. Окончательные расчеты совершаются в день проведения клиринга. Переводы денежных средств между расчетными НКО и в пользу кредитных организаций, не являющихся их участниками расчетов, осуществляются через платежную систему Банка России и счета, открываемые расчетными НКО друг у друга.

Нетто-расчеты осуществляются с предварительным депонированием средств на счетах участников в расчетных НКО для погашения дебетовой позиции. Обязательным условием при проведении неттинга является непревышение дебетовой нетто-позиции участника расчетов над суммой средств на его счете в расчетной

НКО и кредита, который может быть предоставлен этому участнику расчетной НКО на завершение расчетов. При отсутствии предварительно депонированных средств дебетовая нетто-позиция участника расчетов по результатам неттинга должна быть равна либо нулю, либо сумме предоставленного кредита.

Расчетные НКО, выполняющие функции расчетных центров организованного рынка ценных бумаг (ОРЦБ), осуществляют платежи по счетам участников ОРЦБ по поручению организатора торговли (биржи) в размере нетто-позиций, которые вычисляются биржей на основании денежных обязательств, возникающих по результатам заключения сделок.

Расчетные НКО, не являющиеся расчетными центрами ОРЦБ, для поддержания ликвидности участников расчетов при недостаточности денежных средств на их банковских счетах в расчетных НКО выдают краткосрочные кредиты на завершение расчетов как за счет собственных средств, так и за счет фондов, созданных участниками расчетов в этой расчетной НКО.

При невозврате срок кредитов, полученных за счет средств резервов (фондов), погашение осуществляется в соответствии с принципами солидарной ответственности участников расчетов, т.е. пропорционально всеми участниками, в соответствии с соглашением о создании и использовании фондов (резервов), что предотвращает кредитный риск расчетной НКО.

Международные платежи осуществляются кредитными организациями в соответствии со сводами правил и обычаев, кодифицированных Международной торговой палатой, чековой и вексельной конвенциями, межбанковскими соглашениями, межправительственными платежными соглашениями и торговыми договорами.

Кредитные организации, имеющие лицензию Банка России на осуществление банковских операций со средствами в рублях и иностранной валюте, проводят международные платежи через корреспондентские счета, открытые в зарубежных банках в иностранной валюте, либо через корреспондентские счета, открытые в российских кредитных организациях иностранными банками в иностранной валюте или рублях. Открытие счетов и проведение платежей осуществляются на основании двусторонних соглашений между российскими кредитными организациями и иностранными банками.

Кредитные организации, получившие лицензию Банка России на проведение банковских операций в рублях и иностранной валюте, также имеют право для осуществления платежей открывать рублевые счета нерезидентам: физическим лицам, юридическим лицам и официальным представительствам.

Кредитные организации, не имеющие такой лицензии, осуществляют международные платежи через кредитные организации, получившие необходимую лицензию.

В соответствии с правилами, установленными Банком России в рамках предоставленных ему законодательством Российской Федерации полномочий по валютному регулированию и контролю, кредитные организации открывают

физическим лицам — нерезидентам и юридическим лицам — нерезидентам две разновидности рублевых счетов: конвертируемые и неконвертируемые. На конвертируемые счета подлежат зачислению рубли от продажи товаров и оказания услуг российским резидентам, а также от финансовых и неторговых операций нерезидентов в России. Денежные средства на конвертируемых счетах могут использоваться для покупки иностранной валюты на внутреннем валютном рынке России (на использование денежных средств на неконвертируемых счетах на покупку иностранной валюты существуют ограничения).

Одной из основных областей бизнеса для частных платежных систем является обработка розничных платежных операций. Банки и расчетные НКО могут быть участниками и операторами розничных платежных систем, а также выполнять функции операционных, клиринговых и расчетных центров.

Большой объем розничных платежей осуществляется в России при помощи международных платежных систем Visa и MasterCard, являющихся технологическими учреждениями, которые объединяют банковские организации по всему миру и выполняют посредническую роль между банками, а также занимаются организацией расчетов и обеспечивают техническое взаимодействие между участниками систем.

В настоящее время информационно-коммуникационные технологии, такие как Интернет и мобильная связь, широко применяются в банковском бизнесе. Использование в платежных системах современных стандартов и сервисов обмена информацией привело к появлению разнообразных систем электронного обмена «банк — клиент», «телефонный банкинг», «интернет-банкинг» и «мобильный банкинг», которые объединены общим термином «дистанционное банковское обслуживание».

Развитие розничных платежных систем связывается с совершенствованием услуг, предоставляемых посредством дистанционного банкинга, который обычно определяется как оказание розничных платежных услуг вне традиционных отделений банков с использованием информационно-коммуникационных технологий и розничных агентов.

Основными платежными операциями для дистанционного банкинга в России являются расчетно-платежные услуги физическим лицам. Такие услуги до недавнего времени оказывали по преимуществу банки. Однако наряду с развитием платежной инфраструктуры кредитных организаций в России активно развивается платежная инфраструктура небанковских организаций, которая в основном представлена платежными терминалами для расчетно-кассового обслуживания клиентов.

Значительная доля платежных терминалов принадлежит небанковским компаниям, которые оказывают платежные услуги и отвечают за эксплуатацию систем дистанционного перевода денежных средств. Эти терминалы позволяют оплачивать коммунальные и другие услуги (например, телевидение, Интернет и т. п.), вносить квартплату, предоплату телекоммуникационных услуг, а также

погашать потребительский кредит и оплачивать другие виды товаров и услуг (например, покупки в Интернете, приобретение билетов). Большое количество пунктов приема платежей, которые принадлежат небанковским организациям, обусловлено динамичным развитием сети платежных терминалов, посредством которых физические лица могут осуществлять перевод денежных средств в пользу юридических лиц с целью оплаты различного вида услуг. Удобство расположения платежных терминалов, возможность осуществлять платежи в любое удобное для плательщика время, широкий перечень предоставляемых услуг — все это привлекает клиентов и способствует дальнейшему развитию сети платежных терминалов.

Перспективы развития платежно-расчетных технологий, осуществляемых банковскими и небанковскими организациями, связываются с внедрением единого стандарта электронного обмена UNIFI (ISO 20022 — UNiversal Financial Industry), который представляет собой набор средств моделирования, разработки и сопровождения стандартов сообщений для взаимодействия субъектов финансовой отрасли.

Предполагается, что реализация общей платформы для разработки финансовых сообщений на базе UNIFI стандартизует полный комплекс процедур электронного взаимодействия, используемых в финансовой отрасли. На основе бизнес-моделирования будут разработаны формализованные электронные сообщения, обеспечивающие взаимодействие плательщиков и получателя средств для осуществления электронной коммерции, т.е. весь процесс платежно-расчетного электронного документооборота, начиная от процедур заключения договора, выставления счета, осуществления оплаты и заканчивая подтверждением расчетных операций, будет формализован на основе сообщений стандарта ISO 20022. Областью стандартизации платежного взаимодействия являются различные платежные инструменты (документарные и бездокументарные), а также финансовые и торговые услуги (рынки ценных бумаг, обмена валют и товарные биржи). Такая стандартизация даст возможность сквозной автоматизированной обработки сообщений, циркулирующих между кредитными организациями, их клиентами, финансовыми рынками и платежными системами.

4.6. ПЛАТЕЖНАЯ СИСТЕМА СБЕРБАНКА РОССИИ

Сбербанк России (далее также Сбербанк) является крупнейшим банком Российской Федерации и СНГ. Его активы составляют более четверти банковской системы страны. По существующей информации, Сбербанк входит в 50 крупнейших банков мира по размеру основного капитала. На сегодняшний день Сбербанк является самым большим банком российской банковской системы. По объему активов и капитала, по финансовым результатам и масштабам инфраструктуры банк в несколько раз превосходит другие кредитные организации.

Учредителем и основным акционером Сбербанка является Банк России, в настоящее время ему принадлежит более 60% голосующих акций и более 57% в уставном капитале Банка. Остальными акционерами Сбербанка России являются более 263 тыс. юридических и физических лиц. Высокая доля иностранных инвесторов в структуре капитала Сбербанка России (более 32%) свидетельствует о его инвестиционной привлекательности. Государственной властью принято решение о постепенной приватизации пакета акций Сбербанка, принадлежащего Банку России.

Сбербанк России имеет собственную трехуровневую расчетную систему, расположенную во всех часовых поясах и экономических регионах страны и включающую более 20 тыс. отделений и филиалов. Расчетная сеть Сбербанка России сопоставима по размерам только с расчетной системой Банка России и является второй в Российской Федерации по количеству проводимых операций, объемам платежей и количеству филиалов. Эта расчетная система позволяет проводить существенные объемы и количество платежей внутри регионов и между ними в режиме реального времени. Все территориальные расчетные центры Сбербанка России работают в круглосуточном режиме.

По данным Банка России, доля Сбербанка России превышает 30% платежей, проводимых через расчетную сеть Банка России. Сбербанк осуществляет 3,1 млн расчетных операций ежедневно на общую сумму более 960 млрд руб.

Более 500 российских кредитных организаций (около 50% от общего числа) и более 150 банков-нерезидентов более чем из 25 стран мира имеют свыше 1500 счетов в Сбербанке России в 20 видах валют и драгоценных металлах.

Сбербанк России обладает уникальной филиальной сетью, в настоящее время в нее входят 18 территориальных банков и более 19 100 подразделений по всей стране. Дочерние банки Сбербанка России работают в Казахстане, на Украине и в Белоруссии. В соответствии с новой стратегией Сбербанк планирует расширить свое международное присутствие, выйдя на рынки Китая и Индии. Рассматривая международный вектор как важнейшую составляющую стратегии своего развития, Сбербанк России осуществляет казначейские операции на международном рынке и операции торгового финансирования, поддерживает корреспондентские отношения с более чем 220 ведущими банками мира и участвует в деятельности ряда авторитетных международных организаций, представляющих интересы мирового банковского сообщества.

Благодаря масштабам корреспондентской и филиальной сети Сбербанк России в настоящее время проводит по своей расчетной системе большое количество платежей своих клиентов и респондентов, занимает лидирующие позиции на российском денежном рынке и предлагает своим партнерам полный спектр операций с российским рублем.

При организации корреспондентских отношений Сбербанк оказывает следующие услуги:

- открытие и обслуживание корреспондентских счетов в рублях, свободно конвертируемых и ограниченно конвертируемых валютах;

- открытие и обслуживание корреспондентских счетов в российских рублях с предоставлением кредита в виде овердрафт;
- проведение платежей сверх установленного операционного времени;
- открытие и обслуживание обезличенных счетов драгоценных металлов;
- открытие и обслуживание накопительных счетов в валюте для оплаты уставного капитала;
- поддержание неснижаемого остатка средств на корреспондентских счетах кредитных организаций на условиях начисления процентов по ставкам межбанковского рынка;
- проведение расчетов по поручениям клиентов, в том числе по внешнеторговым операциям, проведение расчетов по межбанковским сделкам (конверсионным, депозитным, банкнотным);
- осуществление платежей с конверсией в 20 видах свободно конвертируемых и ограниченно конвертируемых валют, отличных от валюты счета;
- осуществление операций по приему и выдаче наличных денежных средств с корреспондентских счетов в иностранной валюте в пределах установленного максимального ежедневного объема операций с одним респондентом для банков-резидентов;
- осуществление переводов физических лиц, в том числе международных;
- организация электронного документооборота.

Сбербанк России открывает банковские счета, совершает платежи в рублях и иностранной валюте, а также осуществляет расчетно-кассовое обслуживание юридических лиц (резидентов и нерезидентов) и индивидуальных предпринимателей. Он осуществляет расчеты по поручению своих клиентов на территории России и за рубежом. При выполнении операций по счету в случае недостаточности собственных средств клиенты могут воспользоваться услугой овердрафтного кредитования. Всю необходимую информацию об операциях по счету клиенты Сбербанка могут получать с помощью автоматизированной системы «клиент — Сбербанк» в разнообразных форматах.

Данная система позволяет пользователю:

- получать информацию о состоянии счета и операциях по счету;
- передавать рублевые и валютные платежные поручения, получать отчеты об их исполнении;
- отправлять заявки на приобретение векселей, покупку и продажу иностранной валюты;
- давать поручения Сбербанку о перечислении денежных средств во вклады и на счета банковских карт физических лиц по проектам заработной платы;
- вести архив платежных документов;
- вести служебную переписку с банком;
- импортировать платежные документы из программы бухгалтерского учета компании и экспортировать в нее данные из выписок и платежных документов;

- назначать отдельным сотрудникам компании различные права по получению информации из банка и совершению банковских операций по счету.

Сбербанк России предоставляет своим клиентам возможность дистанционного управления счетом в банке через Интернет и телефон. Системы дистанционного обслуживания позволяют без необходимости посещения офиса банка в любое удобное время получать текущую информацию о состоянии счета, а также совершать банковские операции по счету. Использование Сбербанком современных технологий позволяет максимально защитить клиента от несанкционированного доступа к счету или потери информации. Автоматизированные системы дистанционного обслуживания обеспечивают конфиденциальность и надежную защиту информации, передаваемой в ходе электронных расчетов корпоративных клиентов.

Автоматизированная система интерактивного голосового обслуживания позволяет оперативно и в круглосуточном режиме получать по телефону или факсу информацию о состоянии счетов клиентов и сведения о наступлении срока платежа или срока погашения кредита.

Банковские карты Сбербанка России дают возможность безопасно оплачивать товары и услуги. Сбербанк предлагает выпуск и обслуживание карт международных платежных систем Visa, MasterCard и American Express, а также собственных микропроцессорных платежных карт. Имеется возможность оформления разнообразных банковских карт.

Для корпоративных клиентов, предприятий малого бизнеса и индивидуальных предпринимателей Сбербанком предоставляется широкий спектр услуг на основе платежных карт:

- зачисление заработной платы, пенсии и других видов доходов на счета по вкладам и счета банковских карт (зарплатные проекты);
- проведение расчетов уполномоченными представителями (держателями) организаций-клиентов с использованием банковских корпоративных карт;
- возможность приема в качестве средства платежа за предоставляемые клиентами товары и услуги карт ведущих международных платежных систем (торговый эквайринг).

Клиенты Сбербанка России — физические лица (держатели) могут использовать банковские платежные продукты на основе:

- дебетовых универсальных платежных карт;
- кредитных карт;
- дебетовых и кредитных карт с участием партнерских торгово-сервисных организаций (кобрендинг);
- многофункциональных социальных карт.

Совершение банковских операций без посещения подразделения банка может осуществляться через мобильный банк, Интернет или устройства самообслуживания.

Мобильный банк — это комплекс услуг, предоставляемых посредством мобильной связи держателям банковских карт Сбербанка России. Осуществлять

операции по банковской карте можно при помощи самостоятельных SMS-запросов в банк. Кроме этого имеется возможность установить на мобильный телефон небольшое специальное программное обеспечение, которое предоставляет интерфейс для использования услуги «Мобильный банк» и автоматически формирует запросы в банк.

Автоматизированная система дистанционного банковского обслуживания клиентов Сбербанка России позволяет ее пользователям управлять своими счетами, совершать платежные операции и получать необходимую информацию через Интернет.

Терминалы и банкоматы (устройства самообслуживания) Сбербанка России позволяют его клиентам самостоятельно совершать основные банковские операции. Устройства самообслуживания Сбербанка позволяют оперативно и без обращения в подразделение банка совершать основные банковские операции: получать наличные по банковской карте, пополнять счет банковской карты, оплачивать услуги операторов сотовой связи, ЖКХ, интернет-провайдеров и спутникового телевидения, погашать кредит, переводить деньги со счета на счет, получать информацию по своим счетам. Совершать платежи в устройствах самообслуживания можно не только с использованием банковской карты, но и наличными денежными средствами (в банкоматах с функцией приема наличных и информационно-платежных терминалах).

Сбербанк России совершает переводы в рублях и иностранной валюте между отделениями Сбербанка России, а также в другие кредитные организации на территории Российской Федерации и за ее пределами. Переводы — это способ перевести денежные средства физических лиц в пределах России и за рубеж посредством систем:

- внутренних переводов (денежные переводы между отделениями Сбербанка и в другие кредитные организации);
- внешних переводов (перевод денежных средств в страны дальнего и ближнего зарубежья);
- срочных переводов «Блиц» (денежные переводы между отделениями Сбербанка России со сроком исполнения не более одного часа и филиалами дочерних банков в Казахстане и Украине).

Переводы физических лиц осуществляются без открытия счета и со счета по вкладу.

Без открытия счета — перевод может осуществляться в рублях и иностранной валюте наличными деньгами и может быть направлен для выплаты физическому лицу наличными деньгами или путем зачисления на банковский счет.

Со счета по вкладу — перевод может осуществляться в рублях и иностранной валюте путем списания средств со счета по вкладу и может быть выплачен физическому лицу в любом регионе России или банке-нерезиденте наличными деньгами или путем зачисления на банковский счет.

Цели дальнейшего развития Сбербанка России фокусируются на четырех основных направлениях преобразований¹, которые предполагают значимые изменения во всех областях его деятельности.

1. Максимальная ориентация на клиента и в этом смысле превращение Сбербанка России в сервисную компанию. Это значит, что банк будет стремиться удовлетворить максимальный объем потребностей в финансовых услугах каждого своего клиента и тем самым максимизировать свои доходы от каждого набора клиентских отношений.

2. «Индустриализация» систем и процессов в Сбербанке России, которая должна повысить уровень управляемости и масштабируемости, снизить затраты, улучшить качество обслуживания клиентов и которая позволит банку более эффективно управлять кредитными и другими видами рисков.

3. Формализация производственной системы Сбербанка России как новой идеологии управления банком. Разработка процедур формализации производственной системы проводится на базе технологий Lean; этот подход предполагает интегрированную работу по оптимизации и рационализации деятельности по всем направлениям снизу вверх, создание в банке систематической способности к обновлению и самосовершенствованию, а также изменение менталитета и ценностных установок сотрудников.

4. Банк ставит перед собой задачу стать значимым участником мировой финансовой системы, поэтому выделяет развитие операций на международных рынках как одно из приоритетных направлений.

4.7. ПЛАТЕЖНАЯ СИСТЕМА ФЕДЕРАЛЬНОГО КАЗНАЧЕЙСТВА

Федеральное казначейство Министерства финансов Российской Федерации (Федеральное казначейство) создано в соответствии с Указом Президента РФ в 1992 г. с целью проведения государственной бюджетной политики, эффективного управления доходами и расходами в процессе исполнения бюджета Российской Федерации, повышения оперативности в финансировании государственных программ, усиления контроля за поступлением и использованием государственных средств. Это государственное учреждение является федеральным органом исполнительной власти (федеральной службой), осуществляющим в соответствии с законодательством Российской Федерации правоприменительные функции по обеспечению исполнения федерального бюджета, кассовому обслуживанию исполнения бюджетов бюджетной системы Российской Федерации, предварительному и текущему контролю за ведением операций со средствами федерального бюджета главными распорядителями, распорядителями и получателями средств федерального бюджета.

¹ См.: Стратегия развития Сбербанка России на период до 2014 года (www.sbrf.ru).

Федеральное казначейство состоит из Главного управления и территориальных органов в республиках, краях, областях, городах и районах, которым открываются банковские счета обычно в учреждениях Банка России по месту их нахождения. Оно осуществляет свою деятельность непосредственно и через свои территориальные органы во взаимодействии с другими федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, ЦБ РФ, общественными объединениями и иными организациями.

По совокупности операций, выполняемых Федеральным казначейством, оно представляет собой платежную, учетную, контрольную и информационную систему в области финансовой деятельности публично-правовых образований.

Публично-правовыми образованиями являются:

- Российская Федерация;
- субъекты Российской Федерации (83 единицы);
- муниципальные образования (24 296 единиц).

Федеральное казначейство, осуществляя кассовое исполнение бюджетов всех уровней бюджетной системы, обеспечивает единство техники, механизма существования бюджетной системы России, а также повышает уровень прозрачности бюджетных финансовых операций.

Традиционно под кассовыми операциями понимают действия, связанные с платежами, осуществляемыми с помощью наличных денег. Однако когда речь идет о кассовых операциях по исполнению бюджета, их трактуют более широко, рассматривая как наличную, так и безналичную форму денежных расчетов. Под кассовыми операциями по исполнению бюджета понимают операции с денежными средствами, которые обеспечивают их движение в наличной и безналичной форме. Эти операции включают в себя операции по зачислению денежных средств на счет бюджета (кассовые поступления), а также списание средств с бюджетного счета (кассовые выплаты). Осуществление кассовых (платежных) операций и их учет называется кассовым обслуживанием исполнения бюджета. В соответствии с Бюджетным кодексом Российской Федерации (далее — БК РФ) кассовое обслуживание исполнения бюджетов осуществляется Федеральным казначейством¹.

Федеральное казначейство и его территориальные управления входят в состав ассоциированных участников системы БЭСП Банка России, что сокращает время проведения операций со средствами федерального бюджета между счетом Федерального казначейства и счетами управлений по субъектам Российской Федерации.

Федеральное казначейство является оператором программно-аппаратного комплекса (сайт в Интернете) государственных закупок, который представляет собой единый на всю Россию ресурс, где размещается информация обо всех тендерах, кон-

¹ Порядок осуществления расчетов с бюджетной системой см.: приказ Федерального казначейства от 25 августа 2005 г. № 12н «Об утверждении Общего порядка кассового обслуживания исполнения бюджетов бюджетной системы Российской Федерации».

курсах и публикуются все контракты, все акты выполненных работ, кто бы ни был заказчиком — муниципальные образования, субъекты Федерации или федеральные структуры. Ведение общероссийского официального сайта государственных закупок выполняется совместно с Министерством экономического развития РФ.

В настоящее время законодательством Российской Федерации предусмотрена возможность уплаты платежей в бюджетную систему Российской Федерации только через кредитные организации, подразделения Федеральной почтовой связи и кассу местных администраций (для налоговых платежей и страховых взносов) на основе бумажной технологии. В то же время выполнен ряд проектов, направленных на минимизацию наличного денежного обращения и использование для расчетов с бюджетом современных платежных инструментов, что позволяет перейти к полномасштабному электронному документообороту при исполнении федерального бюджета. В рамках этих пилотных проектов денежные чеки и объявления на взнос наличными заменяются на более прогрессивные платежные инструменты — расчетные (дебетовые) банковские карты.

Федеральное казначейство проводит работы по модернизации своей платежной системы, на базе которой будут проводиться зачисления в бюджет и выплаты из бюджета с применением современных платежных технологий. На это направлены работы по созданию «электронного казначейства», совершенствованию системы бюджетных платежей, построению казначейской биллинговой системы и предоставлению государственных и муниципальных услуг в электронной форме.

4.8. ПЛАТЕЖНАЯ СИСТЕМА ПОЧТЫ РОССИИ

Федеральное государственное унитарное предприятие (ФГУП) «Почта России» создано распоряжением Правительства от 5 сентября 2002 г.; 13 февраля 2003 г. проведена государственная регистрация предприятия, принят его устав.

Сегодня Почта России включает в себя 86 филиалов, около 42 тыс. объектов почтовой связи, оказывающих услуги почтовой связи на всей территории Российской Федерации, включая все города и сельские населенные пункты. Ежегодно почтовые работники России принимают, обрабатывают и доставляют более 1,7 млрд писем, 54 млн посылок и почти 185 млн денежных переводов.

Всего Почта России предлагает своим клиентам свыше 80 почтовых, финансовых, информационно-коммуникационных и прочих услуг¹. Через почтовые отделения осуществляется доставка пенсий и пособий, а также подписных печатных изданий. В отделениях почтовой связи можно оплатить коммунальные услуги, получить и погасить банковский кредит, обналечить денежные средства с пластиковых карт, оформить страховку, приобрести лотерейные, театральные,

¹ Более подробно о структуре Почты России, платежных и финансовых услугах, а также о порядке функционирования систем денежных переводов см. официальный сайт предприятия в Интернете (www.russianpost.ru).

железнодорожные и авиационные билеты, а также товары народного потребления. Кроме того, в пунктах коллективного доступа желающие могут выйти в Интернет, отправить и получить электронную почту, распечатать документ и т.д.

В настоящее время Почта России самостоятельно не выполняет банковских операций, а специализируется на денежных переводах и выполняет функции платежного агента для совершения межбанковских расчетов. В рамках этой специализации Почта России предоставляет широкий диапазон платежных услуг.

Почтовый перевод денежных средств является одной из самых динамично развивающихся услуг почтовой связи, позволяющей осуществлять расчеты денежными средствами между физическими и юридическими лицами по всей стране посредством разветвленной филиальной сети почтовых отделений.

Сегодня почтовый перевод денежных средств широко применяется в различных сферах экономической деятельности и востребован при осуществлении следующих операций:

- погашение или выдача кредитов;
- операции по вкладам (пополнение, снятие денежных средств);
- расчет с поставщиком за поставленные товары, оказанные услуги;
- выплата заработной платы, пенсий, пособий, дивидендов, алиментов и т.п.;
- направление денежных средств на закупку продукции;
- расчеты по страховым взносам и премиям.

Заключение договора на осуществление переводов позволяет организациям существенно расширять границы их бизнеса, в том числе за счет клиентов в отдаленных населенных пунктах Российской Федерации, где почта иногда является единственным каналом приема и выдачи денежных средств.

Основным инфраструктурным элементом почтовых переводов является единая система перевода платежей (ЕСПП), оператором которой является Почта России. Техническая реализация ЕСПП основана на замене, где это возможно, пересылки бумажных переводных документов традиционной почтой на пересылку электронных переводных документов электронной почтой.

В системе действуют два типа терминалов:

- 1) защищенный почтово-кассовый терминал (ЗПКТ), обеспечивающий прием и выплату переводов;
- 2) защищенный пункт бумажной технологии (ЗПБТ), обеспечивающий преобразование бумажных документов в электронные и обратно.

ЗПКТ и ЗПБТ связаны между собой через главный пункт (ГП) системы по корпоративной электронной почте и обмениваются электронными документами. ЗПКТ устанавливаются в операционных окнах пунктов обслуживания клиентов, которые имеют выход в телекоммуникационные сети (ПОК-С).

ЗПБТ устанавливаются, как правило, в районных (городских) узлах почтовой связи, на почтамтах и образуют промежуточные пункты (ПП-С). ЗПБТ обмениваются с пунктами обслуживания, не имеющими выход в телекоммуникационные сети (ПОК-Б), бумажными документами по традиционной почте.

Основные функции ЗПКТ:

- обеспечение кассовых и учетных операций при приеме и выплате переводов в процессе обслуживания клиентов
- прием от ГП входящих электронных документов на оплату переводов и отправка на ГП исходящих электронных документов о принятых переводах.

Основные функции ЗПБТ:

- преобразование исходящих бумажных документов о принятых переводах, поступающих из подчиненных им пунктов обслуживания, в электронные и отправка их в ГП;
- преобразование входящих электронных документов, поступающих от ГП, в бумажные для их отправки в подчиненные пункты обслуживания на выплату переводов.

На участках бумажного документооборота сохранность, конфиденциальность и целостность информации о переводах достигается традиционными проверенными временем методами.

На участках электронного документооборота это достигается применением:

- электронной почты с гарантированной доставкой сообщений и криптографической защитой от несанкционированного доступа — шифрования;
- электронной цифровой подписи.

Система действует во всех регионах России. В объектах почтовой связи развернуто более 1540 ЗПКТ и более 1240 ЗПБТ. Практически все пункты обслуживания, производящие прием и выплату переводов, включены в ЕСПП.

При совершении денежных переводов Почта России оказывает следующие услуги:

- денежные переводы «КиберДеньги» (по России, в страны СНГ, Балтии и страны дальнего зарубежья);
- срочные денежные переводы «Форсаж» (срок доставки не превышает часа);
- денежные переводы Western Union (в страны дальнего зарубежья).

В почтовых отделениях также может быть доступна возможность оплаты платежей на терминалах самообслуживания и выдача наличных денежных средств держателям банковских карт. Предоставляя такие услуги, подразделения Почты России выступают в качестве банковских и небанковских платежных агентов.

В целях развития финансовых услуг, предоставляемых физическим и юридическим лицам, наблюдательный совет государственной корпорации «Внешэкономбанк» (ВЭБ) одобрил концепцию создания на базе Связь-банка и Почты России федерального почтового банка. По размеру розничной сети создаваемый «Почтовый банк» может стать крупнейшим в стране, вдвое обогнав по этому показателю Сбербанк. Предполагается, что у федерального почтового банка будет несколько типов банковских отделений. Более 30 тыс. отделений Почты России (из 42 тыс.) расположено в сельской местности. И там банк будет работать на особых условиях: сотрудники почты там одновременно будут сотрудниками банка. В городах функции сотрудников по банковским и почтовым операциям будут разделены.

ГЛАВА 5

ПЛАТЕЖНЫЕ ИНСТРУМЕНТЫ И ТЕХНОЛОГИИ

5.1. ДЕНЕЖНЫЕ СРЕДСТВА И ПЛАТЕЖНЫЕ ИНСТРУМЕНТЫ

Деньги по своей сути являются достаточно сложным мировоззренческим, философским и экономическим явлением. Существуют различные взгляды на задачи, решение которых может быть выполнено при помощи денег в национальной и международной экономике. Традиционным и широко распространенным мнением является то, что деньги — это мера стоимости, средство обращения, средство платежа и средство сбережения. Поскольку в данном параграфе деньги рассматриваются в контексте их использования в качестве платежных инструментов, будем исходить из того, что деньги являются инструментом для товарно-денежного обмена, а все их остальные свойства второстепенные.

В ранних экономических формациях роль денег выполняли различные товары (шкуры зверей, зерно, скот), постепенно физическим выражением денег стали драгоценные камни и благородные металлы (жемчуг, алмаз, золото, серебро и др.), наилучшим образом отвечающие требованиям денежного товара. Усложнение современных платежно-расчетных отношений обусловило замену металлических денег кредитными, имеющими форму бумажных денег и записей на счетах банковских организаций, а также обязательств банковских и небанковских организаций в виде электронных денег.

Исторически банки были местом хранения денег и других ценностей. О наличии денег на хранении выдавался сертификат (квитанция), который удостоверял, что деньги находятся в банке на хранении. Для оплаты крупной покупки достаточно было передать сертификат, а не денежные ценности. Со временем квитанции стали иметь такую же силу, как и реальные деньги, т.е. превратились в банкноты¹. В настоящее время в роли наличных денег выступают обязательства

¹ Слово «банкнота» происходит от английских слов *bank note*, что означает «банковская запись».

государства или центрального банка в форме банкнот. Безналичные денежные средства представляют собой записи об обязательствах на различных носителях информации или счетах, которые отражают количество денег, доступных для совершения расчетов. Самостоятельной стоимости такие деньги не имеют, а являются лишь номинальным обменным эквивалентом.

Безналичные расчеты на территории Российской Федерации осуществляются в формах, установленных ГК РФ, к которым относятся:

- расчеты платежными поручениями;
- расчеты по аккредитиву;
- расчеты по инкассо;
- расчеты чеками;
- иные формы, предусмотренные законом, установленные в соответствии с ним банковскими правилами и применяемые в банковской практике обычаями делового оборота.

Безналичные расчеты производятся через кредитные организации и учреждения Банка России.

Банк России в соответствии с Законом о Банке России является органом, координирующим, регулирующим и лицензирующим организацию платежных и расчетных, в том числе клиринговых, систем в Российской Федерации.

Банк России устанавливает правила и стандарты осуществления наличных и безналичных расчетов, проводит мониторинг деятельности платежных систем на основе статистической отчетности и осуществляет расчеты через свои учреждения.

Расчеты между участниками различных платежных систем могут совершаться посредством материальных (драгоценные металлы, монеты, наличные деньги, расчетные документы и т.п.) или электронных средств платежа.

Электронные средства платежа — средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

В настоящее время платежные инструменты и связанные с ними технологии можно условно классифицировать по следующим типам:

- налично-денежные платежи;
- документарные платежи на базе расчетных документов;
- платежи в системах банковских платежных карт;
- платежи в системах электронных денег;
- мобильные платежные технологии.

Вышеуказанное разграничение платежных операций является весьма условным. На практике платежные инструменты и средства осуществления платежно-расчетных операций являются естественным дополнением друг другу.

Денежные средства, используемые для расчетов документальными и бездокументальными платежными инструментами, могут перемещаться между платежными системами, использующими различные средства для расчетов. Например, для расчетов в платежной системе, использующей электронные деньги, денежные средства можно перевести платежным поручением, платежной картой или предоставить наличные денежные средства в пункте приема платежной системы. Таким образом, денежные средства юридического или физического лица (плательщика) могут быть распределены между различными системами розничных платежей в зависимости от его потребностей. Поток платежей, направленный от плательщика к получателю денежных средств, обычно сопровождается потоком с обратным направлением, который представляет собой товары, услуги и финансовые активы, предоставляемые в обмен на денежные средства.

Развитие платежных услуг, которые оказывают банковские и небанковские, расчетные и технологические организации, в рамках осуществления платежей тесно связано с развитием платежных инструментов и технологий. Возможно, что в скором времени не будет необходимости дифференцировать платежные операции между различными платежными инструментами и технологиями.

5.2. НАЛИЧНЫЕ ДЕНЬГИ

Наличные деньги — валюта одной из стран в каком-либо физическом представлении у конкретного физического или юридического лица. Примером физических представлений могут быть купюры и монеты.

Считается, что наличные деньги неудобны тем, что ими нельзя заплатить дистанционно, для этого обычно используется безналичная оплата посредством расчетных документов, платежных карт, электронных денег или мобильных платежей, но очень удобны, когда нужно оплатить что-либо конфиденциально или анонимно. В связи с этим доля оплаты товаров и услуг наличными деньгами все еще достаточно велика.

Эмиссия наличных денег представляет собой их выпуск в обращение, при котором увеличивается масса наличных денег, находящаяся в обращении.

Монополия на эмиссию наличных денег в России принадлежит ЦБ РФ. В условиях рыночной экономики директивного планирования не существует, однако центральные банки прогнозируют размер предполагаемой эмиссии, используя прогнозы кассовых оборотов коммерческих банков и собственные аналитические материалы.

Государство обязывает всех лиц¹ принимать банкноты и монеты в качестве законного средства платежа на данной территории. В Российской Федерации

¹ В соответствии с подразделом 2 Раздела I «Общие положения» ГК РФ в законодательстве России понятие «лица» охватывает физические лица, юридические лица и государство.

это требование формулируется в Законе о Банке России¹ и в ГК РФ². Российский рубль не относится к свободно конвертируемой валюте.

В целях организации на территории Российской Федерации наличного денежного обращения на Банк России возлагаются следующие функции:

- планирование объемов производства, перевозки и хранения банкнот и монеты, создание их резервных фондов;
- установление правил хранения, перевозки и инкассации наличных денег;
- установление признаков платежеспособности денежных знаков и порядка замены поврежденных банкнот и монет, а также их уничтожения;
- определение порядка ведения кассовых операций в Российской Федерации.

Организация наличного денежного обращения требует от Банка России серьезных материальных затрат. Они охватывают широкий спектр мероприятий, также затрагивающих процессы изготовления денежных знаков, выпуск их в обращение и изъятие из обращения. Этапы выпуска денег в обращение следующие:

- составление прогноза потребности в наличной денежной массе для бесперебойного проведения расчетов;
- изготовление денежных знаков и их защита от фальсификации;
- организация резервных фондов денежной наличности;
- транспортировка денежной наличности в регионы Российской Федерации;
- выпуск денег в обращение.

Эмиссия наличных денег, организация их обращения и изъятие из обращения на территории Российской Федерации осуществляются исключительно Банком России. Эмиссионная работа неразрывно связана с выполнением кассовых операций, так как все операции по изъятию денежных ценностей (банкнот и монет) из резервных фондов и их вложению в резервные фонды обязательно проходят через оборотную кассу соответствующего учреждения Банка России. Правила ведения кассовой работы определяются в соответствующих нормативных документах³.

Учреждениями Банка России, которые осуществляют расчетное и (или) кассовое обслуживание кредитных организаций (их филиалов) и других клиентов, являются подразделения расчетной сети Банка России — первое операционное управление Банка России, головные расчетно-кассовые центры, расчетно-кассовые центры, операционные управления, отделения, кассовые центры и полевые учреждения.

¹ Статья 29: банкноты (банковские билеты) и монеты Банка России являются единственным законным средством наличного платежа на территории Российской Федерации.

² Статья 140: рубль является законным платежным средством, обязательным к приему по нарицательной стоимости на всей территории Российской Федерации.

³ См.: Положение Банка России от 24 апреля 2008 г. № 318-П «О порядке ведения кассовых операций и правилах хранения, перевозки и инкассации банкнот и монеты Банка России в кредитных организациях на территории Российской Федерации».

На основе произведенных расчетов и полученных отчетных данных о выпуске в обращение и изъятии из обращения денежной наличности Банк России определяет заказ для государственного производственного объединения (ГПО) «Гознак» на изготовление денежных знаков по сумме и по купюрам различного достоинства.

Наличные деньги являются базисом всей денежной системы, наиболее ликвидным денежным средством и денежным резервом, что придает особое значение обеспечению прочности и устойчивости наличной составляющей денежной массы.

Банк России учитывает объективные факторы, определяющие потребность экономики в наличных деньгах:

- обычаи и привычки;
- организацию денежных расчетов;
- наличие значительного объема мелких операций в розничной торговле товарами и услугами;
- специфику ведения дел в мелком бизнесе;
- преобладание в стране населения с низкими доходами.

Сфера использования наличных денег в основном связана со следующими операциями:

- расчеты населения с предприятиями розничной торговли и общественного питания;
- оплата труда предприятиями и организациями, выплата других денежных доходов;
- внесение денег населением во вклады и получение по вкладам;
- выплата пенсий, пособий и стипендий, страховых возмещений по договорам страхования;
- выдача кредитными организациями потребительского кредита;
- оплата ценных бумаг и выплата по ним дохода;
- платежи населения за жилищные и коммунальные услуги, при подписке на периодическую печать;
- уплата населением налогов в бюджет и др.

Организации, предприятия, учреждения независимо от организационно-правовой формы хранят свободные денежные средства в учреждениях банков на соответствующих счетах на договорных условиях. Наличные денежные средства, поступающие в кассы организаций, подлежат сдаче в учреждения банков для последующего зачисления на счета этих предприятий. Денежная наличность сдается ими непосредственно в кассы учреждений банков через объединенные кассы при предприятиях. Наличные деньги могут сдаваться предприятиями на договорных условиях через инкассаторские службы учреждений банков или специализированные инкассаторские службы, имеющие лицензию Банка России на осуществление соответствующих операций по инкассации денежных средств и других ценностей.

Порядок и сроки сдачи наличных денег устанавливаются обслуживающими учреждениями банков каждому предприятию по согласованию с их руководителями исходя из необходимости ускорения оборачиваемости денег и своевременного поступления их в кассы в дни работы учреждений банков.

Организации могут иметь в своих кассах наличные деньги в пределах лимитов, установленных банками по согласованию с руководителями предприятий. Лимит устанавливается ежегодно всем предприятиям, имеющим кассу и осуществляющим налично-денежные расчеты независимо от организационно-правовой формы и сферы деятельности, исходя из объемов налично-денежного оборота предприятия с учетом особенностей режима его деятельности, порядка и сроков сдачи наличных денежных средств в учреждения банков, обеспечения сохранности и сокращения встречных перевозок ценностей.

Лимит может пересматриваться в течение года в установленном порядке по обоснованной просьбе предприятия (в случае изменения объемов кассовых оборотов, условий сдачи выручки и т.д.), а также в соответствии с договором с учреждениями банков.

Предприятия могут хранить в кассах наличные деньги сверх установленных лимитов только для выдачи заработной платы, выплат социального характера и стипендии не более трех рабочих дней.

По согласованию с обслуживающими учреждениями банков предприятия могут расходовать поступающую в кассу денежную выручку на цели, предусмотренные федеральными законами и иными правовыми актами, действующими на территории Российской Федерации, и принятыми в их исполнение нормативными актами Банка России.

Выдачи наличных денег предприятиям производятся, как правило, за счет текущих поступлений денежной наличности в кассы кредитных организаций. Для обеспечения своевременной выдачи кредитными организациями наличных денег со счетов предприятий, а также со счетов по вкладам граждан территориальные учреждения Банка России или по их поручению расчетно-кассовые центры устанавливают для каждой кредитной организации и их филиалов сумму минимально допустимого остатка наличных денег в операционной кассе на конец дня.

В целях максимального привлечения наличных денег в свои кассы за счет своевременного и полного сбора денежной выручки от предприятий учреждения банков не реже одного раза в два года проверяют соблюдение определенного Банком России порядка ведения кассовых операций и работы с денежной наличностью. Территориальные учреждения Банка России контролируют работу учреждений банков по организации наличного денежного оборота, соблюдению предприятиями порядка ведения кассовых операций и работы с денежной наличностью.

Территориальные учреждения Банка России периодически анализируют состояние наличного денежного оборота в регионе. Объектом анализа являются:

- складывающаяся тенденция в наличном денежном обороте и его структуре;

- источники поступлений наличных денег в кассы банков и направления их выдач;
- скорость возврата наличных денег в кассы банков;
- происходящие изменения в экономике;
- изменение индекса потребительских цен;
- уровень развития безналичных расчетов;
- уровень инкассации наличной денежной выручки (особенно торговой);
- причины роста эмиссии;
- результаты банковского контроля;
- происходящие изменения в направлениях использования денежных доходов населения и источниках их формирования.

При анализе состояния наличного денежного оборота используются:

- отчет о кассовых оборотах учреждений Банка России и кредитных организаций;
- информационно-аналитические материалы территориальных органов Госкомстата России;
- баланс денежных доходов и расходов населения;
- информация о проверках соблюдения порядка работы с денежной наличностью.

Схема, иллюстрирующая обращение наличных денежных средств, приводится на рис. 5.1, на котором пунктирной линией определено два контура (банковский и товарно-денежный), а стрелками с цифрами обозначены четыре вида деятельности, которые выполняются в процессе обращения наличных денежных средств:

- 1) выпуск наличных денежных средств в обращение;
- 2) распределение наличных денежных средств между держателями;
- 3) оплата товаров и услуг (использование наличных денег в качестве платежного инструмента);
- 4) возврат наличных денежных средств в банковские организации для зачисления их на депозит.

На рисунке стрелка 1 обозначает процедуру выпуска ЦБ РФ наличных денежных средств в обращение. В рамках процедур, которые идентифицированы стрелками 2, денежные средства распределяются между лицами, которые затем могут их использовать для оплаты товаров, работ или услуг. Это распределение предполагает, что на счетах кредитных организаций в ЦБ РФ и других клиентов Банка России, а также на счетах клиентов в кредитных организациях существуют безналичные денежные средства, в обмен на которые они получают наличные денежные средства. Денежные средства на указанных счетах являются разновидностью депозита, который представляет собой обязательства соответствующих банковских организаций перед клиентами. Клиенты ЦБ РФ представлены кредитными и государственными организациями, юридическими и физическими (при выплате денежных средств из кассы) лицами. Стрелки 3 обозначают дея-

тельность по использованию наличных денежных средств их держателями в качестве платежного инструмента. Те лица, которые получили наличные деньги за предоставленные товары или оказанные услуги, становятся держателями наличных денежных средств. На рисунке такое изменение статуса лиц обозначено широкой стрелкой с обратным направлением. Следующим шагом этих лиц может быть либо очередное использование для оплаты наличных денежных средств, либо направление средств для их зачисления на банковский депозит (стрелки 4).

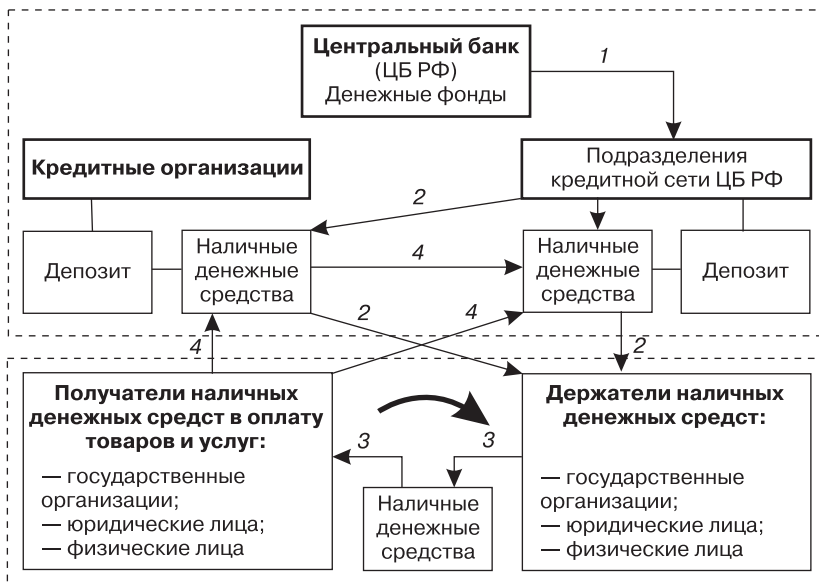


Рис. 5.1. Схема обращения наличных денежных средств

Процедуры инициирования платежа, обмена платежными инструкциями и расчета между участниками платежа осуществляются в следующем порядке. Процедура инициирования совершается после договоренности на поставку товаров или услуг, либо в момент передачи наличных денежных средств, либо в момент поставки товаров или предоставления услуг, в зависимости от того, какую роль играют наличные денежные средства при совершении платежа — дебетового или кредитового инструмента. Информация об оплате доводится до получателя посредством передачи ему плательщиком определенного количества денежных купюр. После двухсторонней проверки правильности выполнения достигнутой ранее договоренности процедура расчета считается завершенной.

В контексте рассмотренного процесса обращения наличных денежных средств они представлены в виде платежного инструмента, эмитентом которого является ЦБ РФ.

5.3. РАСЧЕТНЫЕ ДОКУМЕНТЫ

Описание форм расчетов и порядка взаимодействия юридических лиц с использованием расчетных документов приводится в Положении Банка России от 3 октября 2002 г. № 2-П «О безналичных расчетах в Российской Федерации», в котором определены основные реквизиты расчетных документов и правила их заполнения.

В рамках форм безналичных расчетов в качестве участников расчетов рассматриваются плательщики и получатели средств (взыскатели), а также обслуживающие их банки и банки-корреспонденты. Формы безналичных расчетов избираются клиентами кредитных организаций самостоятельно и предусматриваются в договорах, заключаемых ими со своими контрагентами.

Расчетный документ представляет собой оформленное в виде документа на бумажном носителе или в установленных случаях в виде электронного платежного документа:

- распоряжение плательщика (клиента или банка) о списании денежных средств со своего счета и их перечислении на счет получателя средств;
- распоряжение получателя средств (взыскателя) на списание денежных средств со счета плательщика и перечисление на счет, указанный взыскателем средств.

Банковская организация, которая принимает расчетный документ к проводке, выпускает платежный инструмент, на основании которого осуществляется безналичное зачисление денежных средств на счет получателя, поэтому эмитентами платежных инструментов в документарной форме считаются Банк России и другие кредитные организации.

К платежным инструментам в форме расчетных документов, используемым для осуществления перечислений денежных средств по инициативе плательщиков (кредитовые платежи), относятся платежные поручения и аккредитивы.

Платежным поручением является распоряжение владельца счета (плательщика) обслуживающему его банку, оформленное расчетным документом, перевести определенную денежную сумму на счет получателя средств, открытый в этом или другом банке. Схема проведения расчетов платежными поручениями приводится на рис. 5.2.

При совершении расчетов на основании платежного поручения процедура инициирования платежа начинается в момент представления расчетного документа плательщиком в свой банк. После проверки правильности заполнения реквизитов банк принимает платеж к переводу. Инициирование платежа (стрелка 1) проводится либо путем предоставления в банк бумажных экземпляров расчетных документов, либо посредством программно-аппаратного обеспечения, используемого при электронной передаче и обработке платежей.

Процедура обмена информацией по операциям, совершаемым на основании платежного поручения, включает в себя прием и передачу сообщений, которые

направляются соответствующим участникам расчетов (стрелки 3, 4, 6 и 7). Эти сообщения передаются бумажным или электронным способом и обычно включают:

- информацию о снятии денежных средств, отправляемую плательщику в виде выписки по его лицевому счету;
- отправляемую банком плательщика банку получателя денежных средств информацию о реквизитах принятого к проводу документа;
- информацию о зачислении средств, отправляемую получателю в виде выписки по его лицевому счету, с приложением копий расчетных документов;
- принимаемую банком получателя информацию о результатах выполнения зачисления средств на счет, указанный в расчетном документе, в виде выписки об операциях на корреспондентском счете.

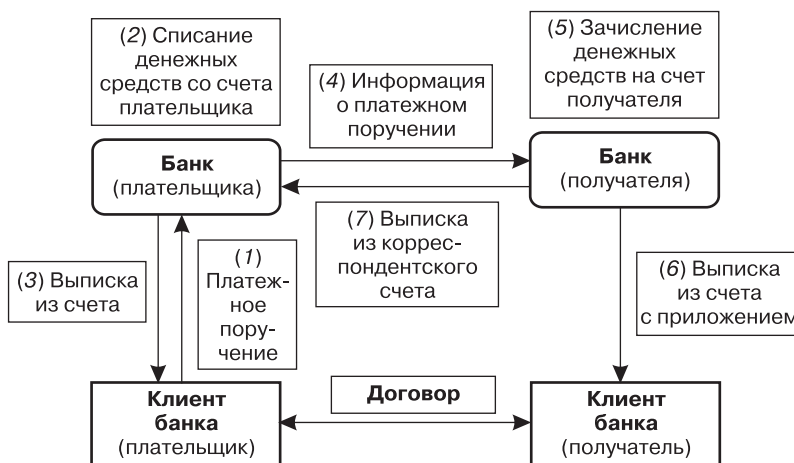


Рис. 5.2. Схема проведения расчетов платежными поручениями

В случае если банк плательщика и банк получателя физически являются одним и тем же учреждением, вместо обмена межбанковскими сообщениями (стрелки 4 и 7) осуществляется обмен информацией внутри одной организации. Следует иметь в виду, что подобный порядок замены межбанковской информации на внутрибанковский обмен информацией используется также при платежах на основании других расчетных документов, когда расчеты осуществляются внутри одного учреждения.

Процедура расчетов по платежному поручению состоит в выполнении операций по зачислению и списанию денежных средств на счетах банков и их клиентов, соответствующих платежному поручению (прямоугольники 2 и 5).

При расчетах по аккредитиву банк, действующий по поручению плательщика об открытии аккредитива (банк-эмитент), обязуется произвести платежи в пользу получателя средств по представлению последним документов, соответствующих всем условиям аккредитива, либо предоставить полномочие другому

банку (исполняющий банк) произвести такие платежи. В качестве исполняющего банка может выступать банк-эмитент, банк получателя средств или иной банк. Схема проведения расчетов аккредитивами приводится на рис. 5.3.

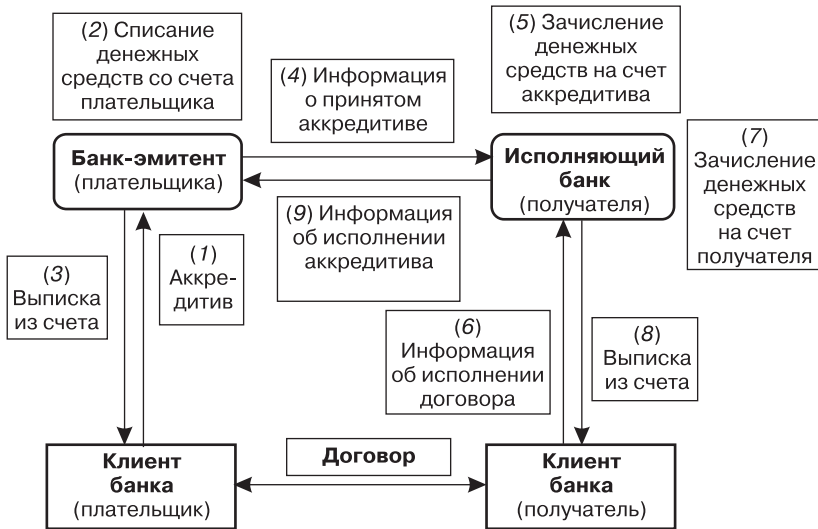


Рис. 5.3. Схема проведения расчетов аккредитивами

Основным отличием платежного поручения от аккредитива является то, что платежи на основании платежного поручения являются безусловными, а при аккредитивной форме оплаты для совершения платежей предусматривается выполнение получателем денежных средств определенных в договоре условий.

Договорные условия между плательщиком и получателем денежных средств являются источником различий в процедурах совершения платежей.

Процедура инициирования (стрелка 1) выполняется сходным с платежным поручением способом. Дальнейшие платежные операции на основании расчетного документа в форме аккредитива имеют отличия, определяемые порядком обмена информацией и расчетами между участниками платежных операций.

Информационный обмен сообщениями в банке-эмитенте включает операции, подобные операциям при расчетах платежных поручений (стрелки 3 и 4). В рамках осуществления аккредитивных платежей на исполняющий банк возлагаются обязанности по надзору за выполнением плательщиком договорных условий, поэтому плательщик представляет исполняющему банку документы, подтверждающие выполнение работ или предоставление услуг (стрелка 6). После проверки правильности исполнения договорных условий исполняющий банк отправляет сообщение банку-эмитенту об исполнении аккредитива (стрелка 9). Это сообщение может содержать информацию об использовании части денежных средств, указанных в аккредитиве, поскольку оплата осуществляется на сумму,

указанную получателем в подтверждающих его работу документах. Кроме этого о зачислении денежных средств информируется получатель в виде выписки по его лицевому счету (стрелка 8).

Процедура расчетов состоит в последовательном выполнении операций:

- по списанию денежных средств со счета плательщика и зачислению их на счет аккредитива (прямоугольники 2 и 5);
- списанию денежных средств со счета аккредитива и зачислению их на счет получателя (прямоугольник 7);
- выполнению окончательных расчетов, отраженных на корреспондентских счетах банков и счете плательщика на основании информации об исполнении аккредитива (стрелка 9).

К документарным формам платежных инструментов, используемым для получения платежа посредством дебетования счета плательщика по инициативе получателя, относятся платежные требования и инкассовые поручения (дебетовые платежи).

Платежное требование является расчетным документом, содержащим требование кредитора (получателя средств) по основному договору к должнику (плательщику) об уплате определенной денежной суммы через банк.

Инкассовое поручение является расчетным документом, на основании которого производится списание денежных средств со счетов плательщиков в бесспорном порядке.

Платежные требования, оплата которых может производиться или по распоряжению плательщика (с акцептом), или без его распоряжения (без акцепта), и инкассовые поручения, оплата которых производится без согласия плательщика, используются при расчетах по инкассо.

Расчеты по инкассо представляют собой банковскую операцию, посредством которой банк (банк-эмитент)¹ по поручению и за счет клиента на основании расчетных документов осуществляет действия по получению от плательщика платежа. Для осуществления расчетов по инкассо банк-эмитент вправе привлекать другой банк (исполняющий банк). Схема проведения расчетов платежными требованиями и инкассовыми поручениями приводится на рис. 5.4.

При совершении расчетов на основании платежных требований и инкассовых поручений процедура инициирования платежа начинается в момент представления расчетного документа получателем в его банк. После проверки правильности заполнения реквизитов расчетного документа банк принимает платеж к переводу. Процедура инициирования платежа (стрелка 1) проводится либо путем представления в банк бумажных экземпляров расчетных документов, либо посредством дистанционного обмена информацией, используемого при электронной передаче и обработке платежей.

¹ Банк называется эмитентом, поскольку он выпускает (эмитирует) дебетовый платежный инструмент.

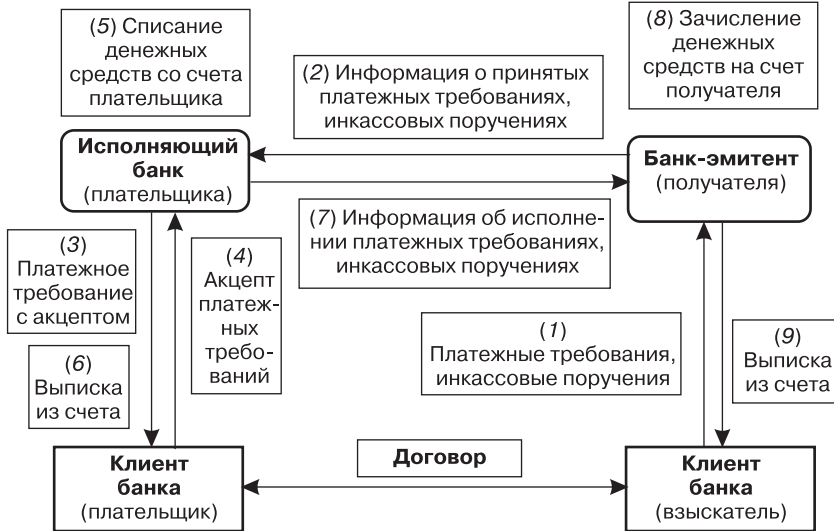


Рис. 5.4. Схема проведения расчетов платежными требованиями и инкассовыми поручениями

Процедура обмена платежной информацией для расчетов на основании инкассовых поручений и платежных требований без акцепта включает обмен следующей информацией:

- сообщение от банка-эмитента исполняющему банку, содержащее реквизиты расчетных документов (стрелка 2);
- сообщение о снятии денежных средств, отправляемое плательщику в виде выписки по его лицевому счету с приложением копий расчетных документов (направление стрелки с прямоугольником б);
- отправляемое банком плательщика банку получателя сообщение об исполненных расчетных документах с выпиской по корреспондентскому счету (стрелка 7);
- сообщение о зачислении средств, отправляемое получателю в виде выписки по его лицевому счету (стрелка 9).

Для информационного обмена по расчетам на основании платежных требований с акцептом добавляются сообщения о необходимости согласия на оплату расчетного документа от исполняющего банка (стрелка 3) и согласие (акцепт) плательщика на проведение платежа (стрелка 4).

Процедуры расчетов по платежным требованиям и инкассовым поручениям состоят в выполнении операций по зачислению и списанию денежных средств на счетах банков и их клиентов в соответствии с реквизитами, указанными в расчетных документах (прямоугольники 5 и 8).

Для осуществления безналичных расчетов могут применяться чеки, выпускаемые кредитными организациями, но не для платежей через платежную систему

Банка России. Порядок обращения чеков и их образцы Банком России не утверждаются.

Чек — это ценная бумага, содержащая ничем не обусловленное распоряжение чекодателя банку произвести платеж указанной в нем суммы чекодержателю. Чекодателем является лицо, имеющее денежные средства в банке, которыми он вправе распоряжаться путем выставления чеков, чекодержателем — юридическое лицо, в пользу которого выдан чек, плательщиком — банк, в котором находятся денежные средства чекодателя. Чеки используются на основании договоров о расчетах чеками, заключаемых между кредитными организациями и клиентами, межбанковских соглашений о расчетах чеками, а также правил проведения операций с чеками, разрабатываемых кредитными организациями.

Реквизиты чека, форма чека и порядок его заполнения определяются законом и установленными в соответствии с ним банковскими правилами. Схема проведения расчетов чеками приводится на рис. 5.5.

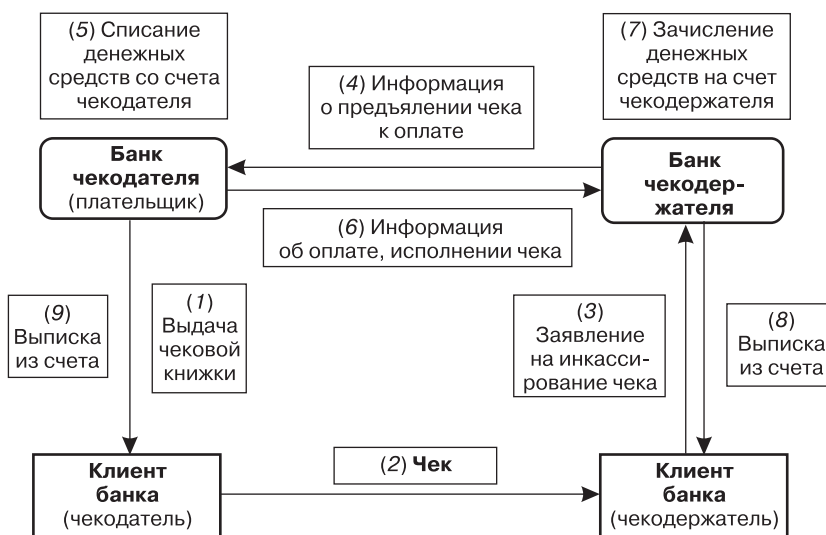


Рис. 5.5. Схема проведения расчетов чеками

Обычно для расчетов чеками банк выдает своему клиенту чековую книжку и зачисляет денежные средства со счета клиента на счет чековой книжки (чекодателя) определенную сумму. С этого момента чекодатель может совершать расчеты с использованием чеков. После того как чекодатель расплатился чеком с чекодержателем, последний может инициировать межбанковский платеж (стрелка 3), написав заявление о предъявлении чека к оплате (инкассировании). Заявление и сам чек являются основанием для проведения операций по получению денежных средств на счет получателя (чекодержателя).

Процедура обмена платежной информацией для расчетов на основании чека предусматривает обмен следующими сообщениями:

- сообщение об оплате от банка плательщика (чекодателя) банку получателя (чекодержателя), содержащее реквизиты инкассируемого чека (стрелка 4);
- отправляемое банком плательщика банку получателя сообщение об исполнении чека (стрелка 6);
- сообщение о зачислении денежных средств, отправляемое получателю в виде выписки по его лицевому счету (стрелка 8);
- сообщение о снятии денежных средств, отправляемое плательщику в виде выписки по его лицевому счету (стрелка 9).

Процедура расчетов по чеку состоит в выполнении операций по зачислению и списанию денежных средств на корреспондентских счетах банков, а также счетах чекодержателя и чекодателя в соответствии с реквизитами, указанными в расчетном документе (прямоугольники 5 и 7).

5.4. ПЛАТЕЖНЫЕ КАРТЫ

Платежная карта является видом инструмента¹ по безналичному перечислению денежных средств, предназначенному для совершения физическими и юридическими лицами платежно-расчетных операций.

Платежные карты — это инструмент, обеспечивающий платежно-расчетное взаимодействие. В настоящее время структура, характеристики и технологии использования платежных карт сложились как сфера посреднической деятельности, имеется достаточное нормативное обеспечение процедур реализации платежного оборота². Это позволяет использовать этот инструмент с минимальными рисками при проведении операций по переводу средств.

На территории Российской Федерации кредитные организации — эмитенты осуществляют эмиссию банковских карт, являющихся видом платежных карт как инструмента безналичных расчетов, предназначенного для совершения физическими лицами, в том числе уполномоченными юридическими лицами (держатели), операций с денежными средствами, находящимися у эмитента.

В состав структуры платежной системы на базе карт входят следующие субъекты, участвующие в платежных операциях.

Эмитент (*card issuer*)³ — кредитная организация, осуществляющая эмиссию карт, которая представляет собой деятельность по выпуску платежных карт, от-

¹ В данном случае платежный инструмент является средством порождения платежных инструкций.

² Нормативным документом, который регламентирует порядок расчетно-кассовых операций посредством банковских карт, является Положение Банка России № 266-П «Об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт».

³ Термины, используемые в области обращения банковских карт в России, как правило, заимствованы из терминологии, принятой в международных платежных системах на базе карт, поэтому основные понятия при необходимости сопровождаются английскими аналогами.

крытию счетов и расчетно-кассовому обслуживанию клиентов при совершении операций с использованием выданных им карт. Эмитент берет на себя финансовые обязательства перед своими клиентами по выданным им платежным картам.

Эквайер (*acquirer*) — кредитная организация, осуществляющая расчеты с организациями торговли или услуг по операциям, совершаемым с использованием платежных карт, и (или) выдающая наличные денежные средства держателям платежных карт, не являющимся его клиентами. Эквайер выполняет посредническую деятельность по осуществлению расчетов платежными картами между держателями карт и торгово-сервисными предприятиями, а также обеспечивает выдачу денег в пунктах выдачи наличных денежных средств по картам других эмитентов.

Расчетный агент (расчетно-клиринговый центр) — кредитная организация, осуществляющая расчетные операции между участниками платежной системы (эмитентами и эквайерами).

Процессинговый (операционный) центр — организация, обеспечивающая информационное, коммуникационное и технологическое взаимодействие между участниками расчетных взаимоотношений. Процессинг (*processing*) — деятельность, включающая в себя сбор, обработку и рассылку участникам расчетов информации по операциям с платежными картами и осуществляемая процессинговым центром.

Пунктами приема банковских карт могут быть:

- пункты выдачи (приема) наличных денежных средств — структурные подразделения эквайеров, такие как: кассы кредитной организации или ее подразделений, обменные пункты, банкоматы (ATM — *automated teller machine*) и т.д., выдающие или принимающие наличные денежные средства с использованием банковских карт;
- торгово-сервисные предприятия (*point of sale*) — организации, принимающие карты в качестве платежного инструмента для расчетов за реализуемые держателям карт товары и услуги.

Держатели платежных карт (*card holder*) — физические и юридические лица (клиенты), осуществляющие с использованием карт расчетные или кассовые операции. Владельцем карты обычно считается организация — эмитент платежной карты, а не ее держатель.

Взаимодействие держателя банковской карты с торгово-сервисным предприятием и банком-эмитентом может осуществляться путем дистанционного обслуживания с использованием различных информационно-коммуникационных технологий (мобильные средства связи, платежные терминалы, Интернет и т.п.).

Следует обратить внимание, что эмиссия карт, эквайринг платежных карт, выполнение функций расчетно-клирингового центра и процессинг — это виды деятельности, которые могут выполняться в рамках одной организации ее подразделениями, а могут быть распределены между несколькими различными организациями.

В Российской Федерации кредитная организация вправе осуществлять эмиссию банковских карт следующих видов:

- расчетных (дебетовых) карт;
- кредитных карт;
- предоплаченных карт.

Расчетная (дебетовая) карта предназначена для совершения операций ее держателем в пределах установленной кредитной организацией — эмитентом суммы денежных средств (расходного лимита), расчеты по которым осуществляются за счет денежных средств клиента, находящихся на его банковском счете, или кредита, предоставляемого кредитной организацией — эмитентом клиенту в соответствии с договором банковского счета при недостаточности или отсутствии на банковском счете денежных средств (овердрафт).

Кредитная карта предназначена для совершения ее держателем операций, расчеты по которым осуществляются за счет денежных средств, предоставленных кредитной организацией — эмитентом клиенту в пределах установленного лимита в соответствии с условиями кредитного договора.

Предоплаченная карта предназначена для совершения ее держателем операций, расчеты по которым осуществляются кредитной организацией — эмитентом от своего имени, и удостоверяет право требования держателя предоплаченной карты к кредитной организации — эмитенту по оплате товаров (работ, услуг, результатов интеллектуальной деятельности) или выдаче наличных денежных средств.

При осуществлении расчетов между держателем карты и торгово-сервисным предприятием различают онлайн операции, перед выполнением которых происходит соединение с центральным компьютером в процессинговом центре для авторизации, и офлайн транзакции¹, при выполнении которых между участниками и клиентами платежной системы нет непосредственной связи, поэтому авторизация и расчетная операция проводятся (оформляются) в кредитной организации — эквайере позднее.

Структурная схема платежной системы на базе банковских карт приводится на рис. 5.6. На схеме стрелками обозначаются процедуры инициирования расчетно-кассовых операций, пунктирные линии отражают процедуры информационно-технологического взаимодействия по переводу средств, а сплошными линиями выделяются операции, связанные с открытием и обслуживанием банковских счетов.

Процесс совершения платежей за предоставленные товары и услуги, а также получения наличных денежных средств предполагает следующий порядок выполнения платежных процедур.

¹ Транзакция (*transaction*) — единичная операция использования карты для приобретения товаров или услуг, получения или сдачи наличных денежных средств, следствием которой является списание или зачисление средств на счетах участников и клиентов платежной системы.

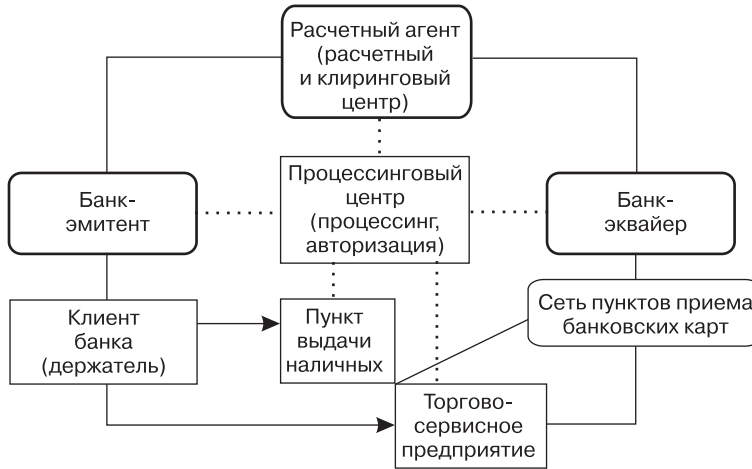


Рис. 5.6. Структурная схема платежной системы на базе карт

Процедура инициирования расчетной или кассовой операции начинается в момент использования банковской карты ее держателем в пункте выдачи наличных денежных средств или в торгово-сервисном предприятии. На основании информации, записанной в памяти карты, идентифицирующей клиента, формируется и отправляется запрос авторизации¹ в процессинговый центр. Процессинговый центр, получив авторизационный запрос, проверяет наличие карты в «стоп-листах»², по номеру карты определяет эмитента и пересылает ему запрос. Эмитент, получив авторизационный запрос, проверяет возможность клиента платить по карте, блокирует указанную в запросе сумму на карточном счете и дает подтверждение авторизации. В том случае, если проверки не дали положительного результата (например, требуемой суммы нет на счете и лимит кредитования исчерпан), в процессинговый центр возвращается отказ авторизации с указанием причины. Процессинговый центр, получив ответ авторизации, пересылает его в пункт приема банковской карты. В случае положительного ответа на авторизационный запрос клиент получает наличные деньги или оплаченные товары и услуги.

Процедура обмена платежной информацией между участниками расчетов в общем виде выглядит следующим образом. Каждый из пунктов приема банковских карт в конце дня формирует электронный журнал операций за день в виде файла

¹ Авторизация — разрешение, предоставляемое эмитентом для проведения операции с использованием банковской карты и порождающее его обязательство по исполнению представленных документов, составленных с использованием банковской карты.

² Стоп-лист — список номеров банковских карт, которые не принимаются к обслуживанию. В стоп-лист обычно заносится утерянные или украденные карты, что исключает возможность их несанкционированного или злоумышленного использования.

финансового подтверждения проведенных операций с помощью банковских карт, который отсылается в процессинговый центр и эквайеру. Процессинговый центр, получив журнал сообщений, сортирует его и формирует реестр платежей, после чего необходимая его часть отправляется эмитенту, эквайеру, расчетному агенту. Далее выполняется информационный обмен между расчетным агентом, эмитентом и эквайером, в рамках которого участники клиринговых и расчетных процедур обмениваются необходимыми для выполнения этих процедур сообщениями.

Основанием для дальнейших платежных операций являются информационные сообщения, направляемые расчетным агентом и другими участниками, для совершения расчетной процедуры, которая выполняется в следующем порядке.

Расчетный агент отправляет эмитенту, согласно реестру платежей, требование по оплате. Эмитент, получив файлы финансового подтверждения в виде реестра платежей из процессингового центра и требование по оплате от расчетного банка, снимает блокировку с карточных счетов клиентов по тем картам, номера которых присутствовали в файле. Затем списывает указанные суммы с этих карточных счетов и перечисляет их расчетному агенту для зачисления на свой счет. Расчетный агент на основании полученного реестра платежей списывает средства со счета эмитента и зачисляет их на счет эквайера. Затем расчетный агент отправляет эквайеру извещение о зачислении средств на его счет. Эквайер зачисляет денежные средства на счет предприятия, через пункт приема банковских карт которого была осуществлена операция оплаты по карте. Эквайер информирует торгово-сервисное предприятие об операциях по ее счету. Эмитент информирует клиента, держателя банковской карты, об операциях на карточном счете.

Ранее изложен процесс совершения платежей, предполагающий перед осуществлением расчетов выполнение клиринговых процедур, направленных на агрегацию платежных инструкций и возможное формирование чистых позиций требований и обязательств между участниками расчетов. Однако вышеуказанные платежные процедуры могут также выполняться в режиме реального времени, тогда процедуры обмена информацией и расчетов между участниками будут выполняться сразу после проведения авторизации.

5.5. ЭЛЕКТРОННЫЕ ДЕНЬГИ

Под электронными деньгами понимается хранимая стоимость или предоплаченный продукт, в котором данные о средствах или стоимости, доступных держателю для многоцелевого использования, хранятся на электронном устройстве, принадлежащем держателю¹. Это определение включает предоплаченные карты (иногда называемые электронными кошельками) и предоплаченные программ-

¹ См.: Обзор новаций в области электронных денег и платежей, совершаемых с использованием мобильных средств связи и Интернета // ЦБ РФ. Платежные и расчетные системы. Международный опыт. 2008. Вып. 6, 7.

ные продукты, которые используют компьютерные сети (иногда называемые цифровой наличностью). В случае с продуктами на основе карт предоплаченная стоимость обычно хранится на микропроцессорном чипе, встроенном в пластиковую карту — смарт-карту. Сетевые продукты используют для хранения стоимости специализированное программное обеспечение, установленное на стандартном персональном компьютере.

Международная терминология дает следующие определения в области обращения электронных денег.

Электронные деньги (*electronic money*) — стоимость, хранящаяся электронным способом в устройстве, таком как карта с микропроцессором или жесткий диск персонального компьютера.

Эмитент (*issuer*) в системе хранимой стоимости или аналогичной предоплаченной системе электронных денег — организация, которая получает платеж в обмен на стоимость, распространяемую в системе, и обязуется оплатить или предоставить возмещение по операциям или возратить остатки, предъявленные ей.

Эквайер (*acquirer*) — организация, признающая обязательства эмитента и осуществляющая расчеты с организациями торговли или услуг по операциям, совершаемым с использованием электронных денег, и (или) выдающая наличные денежные средства держателям, не являющимся его клиентами.

Продукты на основе карт (*card-based products*) — продукты электронных денег, предоставляющие клиенту портативное специализированное компьютерное устройство, как правило, карту с интегральной схемой, содержащую микропроцессорный чип. Продукты в области электронных денег на основе карт, известные также как многоцелевые предоплаченные карты или электронные кошельки, предназначены для совершения розничных платежей на небольшие суммы, являясь заменой банкнотам и монетам.

Продукты на основе программного обеспечения (*software based products*) — продукты электронных денег, использующие специализированное программное обеспечение персонального компьютера, которые, как правило, могут применяться для перевода электронной стоимости.

По сути электронные деньги (ЭД) являются денежными обязательствами эмитента в электронной форме, учет которых осуществляется на специальном устройстве.

Согласно определению, данному Европейской комиссией¹, «электронные деньги являются суррогатом наличности (монет и банкнот) и хранятся на элек-

¹ См.: Директива 2009/110/ЕС, выпущенная 16 сентября 2009 г.; в этой директиве также определены такие понятия, как «учреждение по выпуску электронных денег», «эмитент электронных денег» и «средство оплаты электронными деньгами». Ранее (2000 г.) в Евросоюзе действовало следующее определение электронных денег: «...денежная стоимость, представляющая собой особый вид права требования к организации-эмитенту, которое: 1) хранится на электронном носителе; 2) выпускается при получении денежных средств в стоимостном размере, не меньшем, чем эмитированная денежная стоимость; 3) принимается как средство платежа другими (помимо эмитента) организациями».

тронном устройстве. Они позволяют осуществлять безналичную оплату небольших сумм в разнообразных средах, в том числе через торговый терминал, мобильный телефон или Интернет». Данное определение поддается расширению в случае появления новых продуктов и технологий. Оно применимо к ситуациям, в которых провайдер платежных услуг эмитирует инструменты с предоплаченной стоимостью в обмен на средства, используемые третьей стороной для осуществления платежей.

В интерпретации российских финансовых властей электронные деньги — денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа. При этом не являются электронными денежными средствами денежные средства, полученные организациями, осуществляющими профессиональную деятельность на рынке ценных бумаг, клиринговую деятельность и (или) деятельность по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами и учет информации о размере предоставленных денежных средств без открытия банковского счета в соответствии с законодательством, регулирующим деятельность указанных организаций.

Платежные системы электронных денег — это такие системы, которые оперируют цифровой наличностью — эмитированными организатором (оператором) системы денежными единицами, которыми можно расплатиться или обменять на наличные денежные средства у соответствующих участников системы. В настоящее время это наиболее динамично развивающийся рынок платежных услуг. Клиенты вносят средства в платежную систему через банки, платежные терминалы и банкоматы, почтовую сеть, другие системы электронных денег на базе Интернета и с помощью предоплаченных карт. Далее клиент может использовать электронные деньги для покупок в Интернете, внутренних и международных денежных переводов, погашения потребительских кредитов, оплаты коммунальных услуг и т.п.

Существуют функциональные компоненты, которые являются общими для электронных платежных систем на основе карт и электронных денег. Такими общими составляющими являются:

- выпуск расчетного и (или) кассового инструмента (эмиссия);
- собственник безналичных денежных средств, депонированных, занятых или приобретенных у эмитента (держатель);
- операционная сеть программно-аппаратного обеспечения пунктов приема электронных платежных средств (эквайринговая сеть);

- программно-технические средства информационного обмена и обработки расчетно-кассовых операций (процессинг).

Различия в процедурах расчетно-кассового обслуживания между платежными системами на базе банковских карт и системами электронных денег связаны с различными средствами идентификации держателя, порядком исполнения операций, а также средствами взаимодействия потребителя и исполнителя расчетно-кассовых услуг. Процедура инициирования может осуществляться не только банковской картой, но и специальным программным обеспечением. Процедура обмена платежной информацией определяется порядком информационного обмена в конкретной электронной платежной системе. Процедура проведения расчета между эмитентом и эквайером устанавливается правилами платежной системы.

Платежно-расчетное взаимодействие электронными деньгами может происходить, минуя банковскую систему, т.е. перенос электронных денег (информации о денежных обязательствах эмитента) осуществляется непосредственно с устройства (компьютер или карта с микропроцессором) одного держателя (плательщика) на устройство другого (получателя). В этом аспекте электронные деньги очень похожи на наличные денежные средства. Организации, которые выполняют функции эквайера, эмитента и расчетного агента в рамках платежных систем на базе электронных денег, могут являться не только кредитные организации, но и другие юридические лица.

В Российской Федерации банки обычно осуществляют эмиссию электронных денег в форме prepaid финансового продукта (ПФП). ПФП представляет собой денежное обязательство банка в электронной форме, заменяющее в процессе его обращения требование физических или юридических лиц по оплате товаров, работ и услуг. Клиентом (держателем) является физическое лицо, принявшее условия договора эмиссии ПФП и получившее право совершать расчетно-кассовые операции с использованием ПФП в процессе его обращения. Обращение ПФП предполагает обмен финансового продукта путем уступки клиентом прав требования по данному виду продукта. Под эмиссией ПФП понимается деятельность по выпуску ПФП на основании привлеченных денежных средств в пределах размера, принимаемых банком обязательств, а также ведение учета совершенных операций с их использованием и расчетно-кассовое обслуживание участников расчетов. То есть банки выступают в роли эмитентов, эквайеров и расчетных агентов для участников платежей на базе ЭД, привлекая в качестве процессинговых центров организации, специализирующиеся в области информационно-коммуникационного и технологического обеспечения платежно-расчетных взаимоотношений.

Существует достаточно много разновидностей платежно-расчетного взаимодействия между их участниками, один из примеров совершения расчетов в платежной системе на базе электронных денег с использованием Интернета приводится на рис. 5.7.

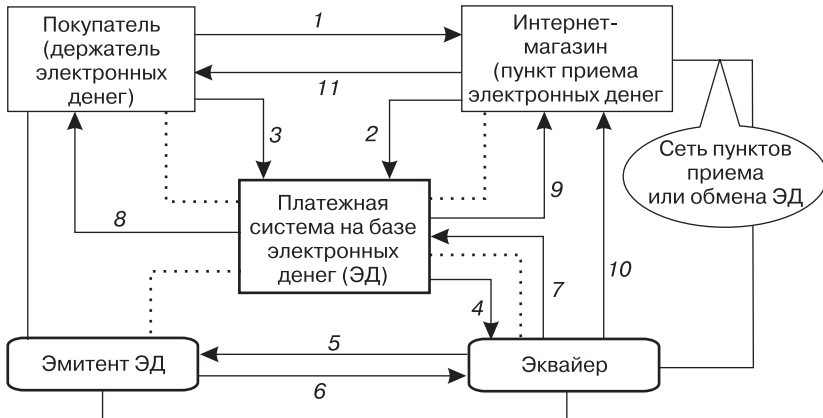


Рис. 5.7. Пример совершения расчетов в платежной системе на базе электронных денег с использованием Интернета

На рисунке стрелками и цифрами обозначается последовательность действий участников расчетов по осуществлению платежей в Интернете, пунктирными линиями выражается информационное взаимодействие (процессинговая деятельность), а сплошными линиями обозначаются отношения, связанные с учетом обязательств между участниками расчетно-кассовых операций в платежной системе на базе электронных денег. Оператор платежной системы может выполнять функции операционного, расчетного и клирингового центров.

При совершении покупки в интернет-магазине обычно выполняется следующая последовательность действий.

1. Запрос покупателя на оплату продавцу товара.
2. Перенаправление покупателя в автоматизированную платежную систему для введения параметров электронных денег.
3. Ввод данных, идентифицирующих средства оплаты (карточные данные, параметры электронной наличности и т.п.).
4. Санкционирование платежной операции эквайером для определения возможности использования данного вида электронных денег с целью оплаты в интернет-магазине.
5. Авторизация платежной операции эмитентом для определения платежеспособности покупателя.
6. Снятие электронных денежных средств с покупателя и зачисление их эквайеру.
7. Направление сообщения в платежную систему об успешности авторизации и регистрации платежной операции.
8. Направление информации о проведенной операции покупателю (плательщику)
9. Направление информации об оплате интернет-магазину (получателю).

10. Снятие электронных денежных средств с эквайера и зачисление их получателю.

11. Доставка товара покупателю.

На практике существует несколько разновидностей процедур реализации платежного процесса в системах электронных денег.

Во-первых, роли эмитента, эквайера, оператора платежной системы, расчетного центра, клирингового центра и продавца могут быть совмещены в рамках функционирования одного юридического лица, а могут быть распределены между различными организациями.

Во-вторых, платежно-расчетное взаимодействие выполняется как в режиме реального времени, так и возможно, что платежные инструкции будут обрабатываться периодически с формированием чистых клиринговых позиций.

В-третьих, после запроса покупателя об оплате выбранного им товара может не осуществляться перенаправление его в автоматизированную систему платежной системы, тогда все действия держателя электронных денег по оплате выбранного им товара будут выглядеть как единый процесс в рамках функционирования программного обеспечения интернет-магазина.

Кроме этого могут встречаться и другие нюансы программно-аппаратной реализации платежно-расчетных процедур.

5.6. МОБИЛЬНЫЕ ПЛАТЕЖНЫЕ ТЕХНОЛОГИИ

Быстрое развитие информационных технологий имеет главное воздействие на платежную индустрию. Новые информационно-коммуникативные технологии позволяют обеспечить достаточно низкую стоимость передачи платежных сообщений. Много факторов указывает на то, что в скором времени платежи с использованием мобильных телефонов станут главным платежным инструментом, но это потребует хорошо организованной системы защиты мобильных платежных технологий.

Развитие электронной торговли, использование Интернета и мобильных коммуникаций привели к появлению новых платежных технологий. Широкое использование мобильных телефонов для совершения платежно-расчетных операций способствовало появлению такого вида деятельности, как мобильная коммерция, который является общим названием, объединяющим различные коммерческие сервисы (кроме услуг связи), использующих мобильный телефон в качестве основного интерфейса пользователя с системами расчетов и платежей.

Для клиентов платежных систем услуги мобильного банкинга и мобильных платежей, которые являются различными направлениями мобильной коммерции, предоставляют уникальную возможность совершать платежно-расчетные операции в любое время и в любом месте.

Мобильный банкинг — управление банковским счетом с использованием мобильного телефона в качестве устройства идентификации владельца банков-

ского счета. При осуществлении платежей используются денежные средства, находящиеся на банковском счете. Как средство оперативного информирования мобильный банкинг позволяет клиентам уменьшить риск несанкционированного использования денежных средств на карточном счете, контролировать использование средств и получать отчеты относительно места и времени проведенных операций.

Для открытия банковского счета клиент направляется в офис банка или к платежному агенту, аккредитованному банком, где в надлежащем порядке устанавливается личность клиента в соответствии с требованиями закона. Он проходит процедуру идентификации, указывая свои имя, адрес и номер мобильного телефона, и представляет приемлемый документ, удостоверяющий личность. Если же у него уже есть банковский счет, он может зарегистрироваться для получения услуг мобильного банкинга с мобильного телефона, отправив текстовое сообщение на конкретный номер.

После открытия счета банк пересылает прикладную программу мобильного банкинга по беспроводной связи на телефон клиента. Клиент регистрирует номер своего телефона и выбирает свой персональный идентификационный номер (PIN). После того как клиент запустил программу мобильного банкинга, ему обычно предлагается выбрать и ввести PIN-код, затем он может совершать платежные операции, получать заработную плату, денежные переводы, другие поступления на банковский счет, а также производить платежи (например, оплачивать счета за коммунальные услуги и т.п.).

Мобильные платежи — совершение платежа при помощи мобильного телефона с использованием разновидностей электронных денег. Мобильные платежи осуществляются без использования банковских счетов клиентов и доступны пользователям, не имеющим собственного банковского счета. Выполняя операции через системы мобильных платежей, клиенты могут оплачивать различные товары и услуги, используя денежные средства в виде электронных денег или счет мобильного телефона у оператора сотовой связи.

Рассмотрим четыре основных устройства, которые мобильные телефоны могут заменить при совершении платежно-расчетных операций¹.

1. Мобильный телефон может использоваться как банковская карта. Банковская карта — это по сути принадлежащее клиенту запоминающее устройство, которое выполняет две функции: идентификацию пользователя и идентификацию счета (и учреждения), где находятся финансовые средства пользователя. Мобильный телефон используется для надежного хранения этой информации, позволяя избежать больших затрат на обеспечение картами всех клиентов банка. Факти-

¹ Более подробно о функционировании международных платежно-расчетных технологий с использованием мобильных средств см.: Mas, Ignacio, and Kabir Kumar. 2008. *Banking on Mobiles: Why, How, for Whom?* Focus Note 48. Washington, D.C.: CGAP, June. Mas, Ignacio, and Sarah Rotman. 2008. *Going Cashless at the Point of Sale: Hits and Misses in Developed Countries*. Focus Note 51. Washington, D.C.: CGAP, December (www.cgap.org).

чески модуль идентификации пользователя (сим-карта) в мобильных телефонах представляет собой смарт-карту (т.е. карту со встроенным чипом, аналогичную наиболее современным банковским картам), хотя и не в привычной пластиковой форме. PIN-код клиента банка и номер счета могут быть записаны на этой SIM-карте или в памяти телефона, действующих как виртуальная карта.

2. Мобильный телефон может играть роль терминала в торгово-сервисном предприятии (*point of sale* — POS), использоваться для направления запросов на осуществление операций и установления связи с соответствующим банком для получения разрешения на операцию. Такую функцию выполняет кассовый терминал POS в магазине: у него есть экран и клавиатура ввода данных для введения реквизитов операции, устройство для считывания с карты, фиксирующее хранящуюся на ней информацию о клиенте (для подтверждения его личности и нахождения его счета), а также безопасная линия связи с банком. Мобильный телефон может воспроизвести эти функции. Если клиент использует на своем телефоне виртуальную карту, мобильный телефон в качестве терминала POS сможет непосредственно ее считать; в иных случаях придется подсоединить к мобильному телефону устройство для считывания с карт.

3. Мобильный телефон может выполнять функции элементов банкомата. Если использовать денежные средства, доступ к которым обеспечивает мобильный телефон для оплаты в магазине, тогда он и кассовый аппарат магазина выполняют функцию банкомата по внесению и выдаче наличных денежных средств.

4. Мобильный телефон может использоваться как терминал для обслуживания клиентов через Интернет. Банковское обслуживание через Интернет (интернет-банкинг) удовлетворяет двум основным условиям, представляющим ценность для клиента: возможность контроля (моментальный доступ к любым понадобившимся реквизитам счета) и удобство (возможность дистанционного совершения платежей и денежных переводов). Однако применение этой системы обслуживания клиентов во многих случаях ограничено в связи с низким уровнем распространения самого Интернета. Мобильный телефон и беспроводная связь могут обеспечить клиентам интернет-терминал.

В основе мобильных платежных технологий лежит эталонная модель мобильной коммерции, разработанная Open Mobile Alliance (OMA)¹. Далее при объяснении порядка взаимодействия участников платежно-расчетных отношений будет использоваться модифицированная схема мобильной коммерции, которая в большей мере соответствует традиционной структуре платежных систем.

В модели мобильной коммерции определены четыре ключевые роли в любой транзакции: покупатель, продавец, эмитент (организация, которая обеспечивает покупателя средствами для оплаты товаров и услуг, осуществляет выпуск электронных средств оплаты) и эквайер (организация, с которой взаимодействует продавец, чтобы получить денежные средства за товары и услуги). Другими

¹ Информация об эталонной модели мобильной коммерции представлена на информационном портале Инфокоммуникационного союза в Интернете (www.mobilepaymentsrussia.ru).

участниками мобильных платежных систем являются платежные агенты, оператор мобильной связи и платежной системы, процессинговый (операционный) и расчетный центры. Все они участвуют в платежно-расчетных процедурах, выполняя конкретные функции. Расчетный и клиринговый центры обычно совмещаются в рамках одной кредитной организации. Однако функции расчетного и клирингового центра также могут выполняться одним из эмитентов или эквайеров. Участником платежной системы, отвечающим за идентификацию клиента в соответствии с требованиями законодательства РФ, является служба доверенной третьей стороны (ДТС). Схема взаимодействия участников мобильной коммерции приводится на рис. 5.8.

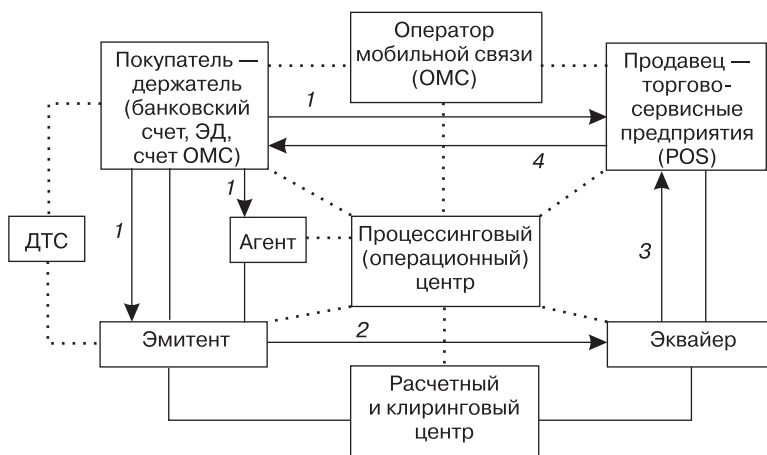


Рис. 5.8. Схема взаимодействия участников мобильной коммерции

На схеме пунктирными линиями обозначаются информационные взаимодействия между участниками, сплошными линиями определяются расчетно-кассовые отношения, а стрелки с цифрами показывают схему выполнения платежно-расчетных операций:

- 1 — инициирование покупателем перевода продавцу;
- 2 — перевод безналичных денежных средств от эмитента к эквайеру через расчетный и (или) клиринговый центр;
- 3 — зачисление денежных средств эквайером продавцу;
- 4 — поставка товаров, проведение работ или предоставление услуг.

Процедура инициирования платежа с использованием мобильного телефона может выполняться тремя альтернативными способами (стрелки 1):

- 1) через точку продажи торгово-сервисного предприятия;
- 2) через платежного агента;
- 3) путем мобильного взаимодействия с эмитентом платежного инструмента.

Процедура обмена платежной информацией для осуществления расчетов между покупателем (плательщиком) и продавцом (получателем) проводится с использованием электронных сообщений, которые передаются между участниками платежей посредством технических средств мобильного оператора и процессингового центра. Форматы сообщений и порядок взаимодействия участников определяются правилами и стандартами электронного обмена.

Процедура расчета может выполняться как в режиме реального времени, так и методами периодической (отложенной) валовой обработки, двухстороннего или многостороннего неттинга. В случае отложенного валового или нетто-расчета на расчетный центр возлагаются функции клирингового центра, который формирует чистые клиринговые позиции между эмитентами и эквайерами. При этом окончательный расчет между всеми участниками расчетов осуществляется по результатам клиринговой обработки платежных инструкций (стрелки 2 и 3), а поставка товаров, проведение работ или предоставление услуг (стрелка 4) может выполняться после получения информации от эмитента о платежеспособности покупателя и блокировки средств, необходимых для совершения платежа.

В рамках совершения мобильных платежных операций все функциональные обязанности по расчетному посредничеству между плательщиком и получателем средств могут выполняться в рамках одной платежной системы, организованной оператором мобильной связи. Однако, как правило, функции эмитента, эквайера и расчетного центра выполняют банковские организации, а функции процессингового центра возлагаются на организации, специализирующиеся в области платежного и информационно-телекоммуникационного взаимодействия.

В платежных системах на базе мобильных технологий расчетные активы могут быть представлены обязательствами кредитных организаций, небанковских эмитентов платежных инструментов и мобильных операторов.

Перспективы развития мобильных платежных технологий определяются совершенствованием институционального взаимодействия, мобильной платежной инфраструктуры и нормативно-правового обеспечения платежного процесса на основе современных телекоммуникационных стандартов и сервисов.

В рамках Технического комитета (ТК) 68 «Финансовые услуги» Международной организации по стандартизации проводятся работы по разработке международного стандарта мобильных финансовых услуг (ISO 12812). В настоящее время определены следующие части этого стандарта:

ISO 12812-1 — общие сведения;

ISO 12812-2 — безопасность и защита данных для мобильных финансовых услуг;

ISO 12812-3 — управление финансовыми приложениями;

ISO 12812-4 — мобильные платежи между физическими лицами;

ISO 12812-5 — мобильные платежи между бизнесом и физическим лицом;

ISO 12812-6 — основные мобильные банковские операции.

Разрабатываемые ТК 68 спецификации направлены на создание общих международных подходов к функционированию мобильных финансовых технологий

и обеспечение совместимости различных элементов мобильной платежной инфраструктуры.

Существенное влияние на развитие в области мобильных платежных систем оказывает процесс взаимовыгодной кооперации между банковским и телекоммуникационным сообществами, что позволяет оказывать клиентам современные мобильные платежные услуги. Для придания рынку платежных и финансовых услуг России, использующих мобильные технологии, нового импульса развития планируется создавать технические решения на основе сотрудничества между кредитными, телекоммуникационными и технологическими организациями. В рамках общих проектов организаций с различной специализацией разрабатываются новые платежные технологии, сочетающие характеристики мобильного банкинга и мобильных платежей.

ГЛАВА 6

РАСЧЕТНАЯ СИСТЕМА ОРГАНИЗОВАННОГО РЫНКА ЦЕННЫХ БУМАГ

Предметом настоящей главы является рассмотрение вопросов функционирования расчетной системы организованного рынка ценных бумаг (ОРЦБ) и взаимодействия инфраструктурных элементов ОРЦБ при проведении денежных расчетов по итогам биржевых торгов. Необходимо учитывать, что такая система расчетов, как и организованный рынок ценных бумаг в целом, находится в настоящее время в стадии существенных институциональных преобразований, которые характеризуются изменением принципов правового регулирования проведения организованных торгов, клиринга и расчетов, связанным со вступлением в силу Федеральных законов от 21 ноября 2011 г. № 325-ФЗ «Об организованных торгах»¹ (далее — Закон об организованных торгах), от 7 февраля 2011 г. № 7-ФЗ «О клиринге и клиринговой деятельности»² (далее — Закон о клиринге), Закона о НПС³, с одной стороны, и изменением инфраструктуры ОРЦБ, связанным с объединением биржевых структур Группы «Московская межбанковская валютная биржа» (ММВБ) и Группы «Российская торговая система» (РТС)⁴, — с другой стороны.

При этом следует отметить, что расчетная система ОРЦБ, созданная в середине 90-х гг. прошлого века и зарекомендовавшая себя за время функционирования как надежная и транспарентная система расчетов, в полной мере может стать, на наш взгляд, основой для построения платежной системы, предусматривающей переводы денежных средств по итогам организованных торгов.

¹ СЗ РФ. 2011. № 48. Ст. 6726.

² СЗ РФ. 2011. № 7. Ст. 904.

³ СЗ РФ. 2011. № 27. Ст. 3872.

⁴ Новое наименование объединенных биржевых структур ММВБ и РТС — «Группа ММВБ-РТС», новое наименование объединенной биржи — ОАО «ММВБ-РТС».

6.1. ПОНЯТИЕ И СТРУКТУРА ОРЦБ

Категория «организованный рынок ценных бумаг» была введена в оборот Банком России при разработке совместно с Министерством финансов РФ нормативной базы в 1993—1995 гг. для регулирования обращения государственных ценных бумаг. Затем правила ОРЦБ были распространены на обращение других финансовых инструментов и другие финансовые рынки.

Категория «организованный рынок ценных бумаг» достаточно активно используется в законодательных актах¹. Однако раскрывается эта категория не в законодательных актах, а в нормативном акте Банка России — Положении от 8 июля 1998 г. № 32-П «О порядке осуществления расчетов по операциям с финансовыми активами на ОРЦБ»² (далее — Положение № 32-П).

Согласно пункту 1.2 указанного Положения под **ОРЦБ** понимается совокупность отношений, связанных с обращением ценных бумаг, срочных контрактов и других финансовых активов, правила исполнения сделок и бухгалтерского учета с которыми соответствует требованиям, установленным Банком России.

Согласно иному определению, под ОРЦБ понимается система «отношений, связанных с заключением и исполнением сделок с государственными ценными бумагами по установленным и согласованным с Банком России процедурам»³.

Учитывая то обстоятельство, что правила ОРЦБ регулируют не только обращение ценных бумаг, но и обращение других финансовых активов, указанным выше отношениям более соответствовал бы, по нашему мнению, такой термин, как «организованный финансовый рынок», который применяется в документах концептуального характера.

Так, Стратегия развития финансового рынка Российской Федерации на период до 2020 года, утвержденная распоряжением Правительства РФ от 29 декабря 2008 г. № 2043-р⁴, содержит определение организованного финансового рынка. Под ним следует понимать общую торговую среду, в которой существуют различные по своей форме и степени институционализации системы заключения сделок с финансовыми инструментами в соответствии с выработанными участниками таких систем или установленными государством правилами.

В отдельных нормативных актах Банка России «организованный рынок ценных бумаг» и «биржевой рынок» (или «биржа») рассматриваются как тождественные понятия⁵.

Следует отметить, что законы о клиринге, НПС и организованных торгах не оперируют понятием «организованный рынок ценных бумаг», «предпочитая»

¹ См. НК РФ и др.

² Вестник Банка России. 1998. № 41.

³ Российский рынок государственных ценных бумаг / под ред. д.э.н. М.Ю. Алексева. Лондон : Ермани Пабликешенз ПиЭлСи, 1997. С. 58.

⁴ СЗ РФ. 2009. № 3. Ст. 423.

⁵ См. письма Банка России от 26 апреля 2011 г. № 61-Т и от 29 августа 2011 г. № 127-Т.

ему термин «организованные торги»¹, определения которого, изложенные в законодательных актах, не совпадают.

Согласно ст. 2 Закона о клиринге организованные торги — торги, которые проводятся фондовыми биржами или иными организаторами торговли на рынке ценных бумаг, товарными биржами, валютными биржами.

В соответствии со ст. 2 Закона об организованных торгах организованные торги — торги, проводимые на регулярной основе по установленным правилам, предусматривающим порядок допуска лиц к участию в торгах для заключения ими договоров купли-продажи товаров, ценных бумаг, иностранной валюты, договоров РЕПО и договоров, являющихся производными финансовыми инструментами.

По нашему мнению, определение ОРЦБ значительно шире определения организованных торгов, поскольку в содержательном плане оно охватывает не только отношения, связанные с организацией и проведением торгов, но также с организацией и осуществлением клиринга и расчетов по итогам таких торгов.

Основным нормативным правовым актом, регулирующим порядок размещения, обращения, обслуживания и погашения федеральных государственных ценных бумаг, является Положение Банка России от 25 марта 2003 г. № 219-П «Об обслуживании и обращении выпусков федеральных государственных ценных бумаг»² (далее — Положение № 219-П).

В соответствии с Положением № 219-П (в ред. Указания от 17 октября 2011 г. № 2716-У³, далее — Указание № 2716-У) участниками рынка федеральных государственных ценных бумаг (облигаций) являются: эмитент — Минфин России, генеральный агент эмитента — Банк России, первичный дилер, дилер, инвестор.

Инфраструктуру ОРЦБ составляют торговая и расчетная системы, а также Головной депозитарий (далее — депозитарий) (рис. 6.1).

Ключевым элементом ОРЦБ является торговая система.

Торговая система — юридическое лицо, имеющее лицензию профессионального участника рынка ценных бумаг на осуществление деятельности по организации торговли на рынке ценных бумаг и (или) лицензию фондовой биржи и уполномоченное на основании договора с Банком России организовывать в соответствии с нормативными актами Банка России заключение и исполнение сделок с облигациями.

Торговая система вправе осуществлять расчет позиций дилеров, составлять отчетные документы по совершенным сделкам и представлять их в расчетную систему и депозитарий.

¹ Федеральным законом от 21 ноября 2011 г. № 327-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона „Об организованных торгах“» в некоторые законодательные акты внесены изменения в части замены слов «на организованном рынке ценных бумаг» словами «на организованных торгах».

² Вестник Банка России. 2003. № 40.

³ Вестник Банка России. 2011. № 66. Указание вступило в силу с 1 января 2012 г.



Рис. 6.1. Инфраструктура ОРЦБ

Торговая система не может быть дилером, инвестором, депозитарием или расчетной системой.

В ранее действующей редакции Положения Банка России № 219-П содержалось иное определение торговой системы, согласно которому такая система определялась как юридическое лицо, имеющее лицензию профессионального участника рынка ценных бумаг на осуществление деятельности по организации торговли и уполномоченное на основании договора с Банком России обеспечивать процедуру заключения сделок с облигациями в соответствии с нормативными актами Банка России.

В связи с приведенными определениями обоснованно возникал вопрос о соотношении категорий «торговая система» и «организатор торговли на рынке ценных бумаг».

Н.Г. Семилютина¹ указывает на следующие различия упомянутых категорий:

- организатор торговли действует в соответствии с требованиями Федерального закона от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг»² (далее — Закон о рынке ценных бумаг), а также правовых актов ФСФР России на основании соответствующей лицензии. Торговая система (точнее, организация, выполняющая обязанности торговой системы) в отличие от организатора торговли действует на основании договора на выполнение функций торговой системы на рынке государственных ценных бумаг, и круг ее обязанностей определен в этом договоре;
- организатор торговли самостоятельно устанавливает требования, предъявляемые к участникам торгов, принимает в члены и допускает к участию

¹ См.: Семилютина Н.Г. Российский рынок финансовых услуг (формирование правовой модели). М. : Волтерс Клувер, 2005. С. 228.

² СЗ РФ. 1996. № 17. Ст. 1918.

в торгах участников торгов. Торговая система не вправе принимать самостоятельное решение о допуске или прекращении допуска к участию в торгах дилера; она лишь обязана обеспечить доступ к заключению сделок любой организацией, отвечающей признакам дилера согласно Положению № 219-П (т.е. заключившей договор с Банком России);

- организатор торговли самостоятельно разрабатывает и регистрирует в ФСФР России правила торгов (заключения сделок), определяет список ценных бумаг, допущенных к обращению, и иные документы. Торговая система не вправе определять критерии допуска ценных бумаг к обращению в торговой системе¹.

На основе проведенного анализа соотношения категорий «торговая система» и «организатор торговли на рынке ценных бумаг» Н.Г. Семилютина приходит к следующему выводу: «...несмотря на то, что Положение № 219-П устанавливает требование в отношении организации, выполняющей функции торговой системы, иметь лицензию профессионального участника рынка ценных бумаг на организацию торговли, торговая система при выполнении своих функций не отвечает признакам организатора торговли, перечисленным в Законе о рынке ценных бумаг»².

Следует отметить, что в законодательных актах понятие «торговая система» не использовалось до вступления в силу с 1 января 2012 г. Закона об организованных торгах, в котором торговая система рассматривается в качестве разновидности организатора торговли наряду с биржей.

Анализ норм Закона об организованных торгах позволяет выявить следующие отличия торговой системы от биржи.

Во-первых, из ч. 4 ст. 9 и ч. 4 ст. 12 Закона об организованных торгах следует, что оказание услуг по проведению организованных торгов, на которых заключаются договоры, являющиеся производными финансовыми инструментами, осуществляется только биржами. Нормативными правовыми актами федерального органа исполнительной власти в области финансовых рынков могут быть предусмотрены случаи, когда услуги по проведению организованных торгов, на которых заключаются отдельные виды договоров, являющихся производными финансовыми инструментами, могут оказываться торговой системой.

Во-вторых, согласно ч. 3 ст. 12 Закона об организованных торгах торговая система не вправе совершать действия и оказывать услуги, которые в соответствии с Законом об организованных торгах, иными федеральными законами и принятыми в соответствии с ними нормативными правовыми актами могут совершаться (оказываться) только биржей.

Так, в соответствии с п. 4 ст. 14 Закона о рынке ценных бумаг торговая система не вправе осуществлять листинг ценных бумаг путем их включения в котировальные списки.

¹ См.: Семилютина Н.Г. Российский рынок финансовых услуг (формирование правовой модели). С. 228.

² Там же.

В-третьих, организатором торговли может являться только хозяйственное общество, при этом биржей — только акционерное общество (ч. 1 ст. 5 и ч. 2 ст. 9 Закона об организованных торгах).

В-четвертых, биржа не вправе совмещать свою деятельность с брокерской, дилерской и депозитарной деятельностью, а также с деятельностью по управлению ценными бумагами. Что касается торговой системы, то она не вправе совмещать свою деятельность с указанными видами деятельности в случае ее совмещения с клиринговой деятельностью (ч. 5 ст. 9 и ч. 5 ст. 12 Закона об организованных торгах).

В-пятых, минимальный размер собственных средств лица, оказывающего услуги по проведению организованных торгов на товарном и (или) финансовом рынках на основании лицензии биржи, должен составлять не менее 100 млн руб. Для лица, оказывающего услуги по проведению организованных торгов на товарном и (или) финансовом рынках на основании лицензии торговой системы, данный показатель должен быть не менее 50 млн руб. (ст. 8 Закона об организованных торгах).

Следует отметить, что Указанием Банка России № 2716-У в Положение № 219-П внесены изменения, согласно которым размещение и обращение облигаций может осуществляться не только на торгах торговой системы, но также на торгах фондовой биржи, не являющейся торговой системой, в соответствии с правилами фондовой биржи, а обращение облигаций может осуществляться на внебиржевом рынке в соответствии с договором.

Следующий элемент инфраструктуры ОРЦБ — депозитарий, под которым понимается юридическое лицо, имеющее лицензию профессионального участника рынка ценных бумаг на право осуществления депозитарной деятельности и на основании договора с эмитентом осуществляющее централизованное хранение облигаций и учет прав на них в соответствии с законодательством Российской Федерации и условиями заключенных с депонентами договоров.

Депозитарий осуществляет деятельность на рынке облигаций в соответствии с Положением № 219-П (в ред., действующей согласно Указанию Банка России № 2716-У).

Депозитарий не может быть дилером или выполнять функции торговой системы.

В ранее действовавшей редакции Положения № 219-П депозитарий определялся как юридическое лицо, имеющее лицензию профессионального участника рынка ценных бумаг на осуществление депозитарной деятельности и заключившее соответствующий договор с эмитентом, а также уполномоченное на основании договора с Банком России обеспечивать учет прав на облигации по счетам ДЕПО дилеров и перевод облигаций по счетам ДЕПО. Также в ранее действовавшей редакции Положения № 219-П содержались пункты, раскрывающие понятия депозитарной системы и субдепозитариев, которые Указанием Банка России № 2716-У признаны утратившими силу, что связано с отменой двухуровневой си-

стемы депозитарного учета государственных ценных бумаг (требования об обязательном учете государственных ценных бумаг, принадлежащих владельцам, не являющимся дилерами, в субдепозитариях)¹.

Расчетная система представляет собой совокупность расчетных центров ОРЦБ, обеспечивающих расчеты по денежным средствам по сделкам с ценными бумагами и другими финансовыми активами.

Анализ определений расчетной системы ОРЦБ, изложенных в нормативных актах Банка России, регулирующих функционирование ОРЦБ на различных его этапах, позволяет выявить историю изменения подходов к содержанию этого определения.

Так, на этапе создания ОРЦБ расчетная система ОРЦБ рассматривалась как организация (банк, клиринговая палата, биржа, расчетная палата), имеющая право на ведение расчетных операций и уполномоченная на основании договора с Банком России обеспечивать денежные расчеты по сделкам с облигациями с соблюдением требований Положения об обслуживании и обращении выпусков государственных краткосрочных бескупонных облигаций, утвержденного приказом Банка России от 6 мая 1993 г. № 02-78².

Затем расчетная система ОРЦБ определялась как совокупность расчетных центров ОРЦБ и расчетных подразделений Банка России, обеспечивающих расчеты по денежным средствам по сделкам с облигациями (см.: Положение об обслуживании и обращении выпусков государственных краткосрочных бескупонных облигаций, утв. приказом Банка России от 15 июня 1995 г. № 02-125³).

И наконец, в действующих нормативных актах Банка России расчетная система ОРЦБ рассматривается как совокупность расчетных центров ОРЦБ, обеспечивающих расчеты по денежным средствам по сделкам с облигациями.

Первоначально инфраструктурные элементы объединялись в рамках ММВБ, отношения которой с Банком России регулировались договором от 17 мая 1993 г. на выполнение функций депозитария, расчетной и торговой систем на рынке государственных краткосрочных бескупонных облигаций.

Согласно действовавшему в то время нормативному акту — Временному порядку проведения Банком России операций на рынке государственных краткосрочных бескупонных облигаций в г. Москве, осуществления расчетов и учета по ним, утвержденному приказом Банка России от 6 мая 1993 г. № 02-78, заключение сделок по купле-продаже облигаций на первичном и вторичном рынке в г. Москве и расчеты по ним организовывались ММВБ на основании соглашения между Банком России и ММВБ. РКЦ открывал для ММВБ корреспондентский счет, через который осуществлялись все расчеты Банка России с участниками рынка облигаций. Денежные расчеты дилеров (за исключением Банка России) по сделкам

¹ См. п. 5 Информации Банка России «Об Указании Банка России» // Вестник Банка России. 2011. № 68.

² СПС «КонсультантПлюс».

³ Вестник Банка России. 1995. № 29—32.

купи-продажи облигаций осуществлялись расчетной системой ММВБ по их корреспондентским (текущим) счетам. Перечисление денежных средств со счетов дилеров в ММВБ на их основные корреспондентские (расчетные) счета в банковских учреждениях и зачисление средств на счета дилеров в ММВБ с их основных корреспондентских (расчетных) счетов в банковских учреждениях осуществлялись через корреспондентский счет ММВБ в РКЦ.

Однако совмещение разнородных по своей природе функций (в частности, функций торговой и расчетной систем) в одной организации могло привести к конфликту интересов и со временем стало противоречить динамично изменяющемуся законодательству, в том числе законодательству о банках и банковской деятельности.

Так, согласно Закону о банках и банковской деятельности осуществление расчетов по поручению физических и юридических лиц, в том числе банков-корреспондентов, по их банковским счетам является банковской операцией, а банковские операции может осуществлять только кредитная организация.

Учитывая требование законодательства, а также письмо от 7 марта 1996 г. № 248¹, которым Банк России разрешил создание кредитных организаций для выполнения функций расчетных центров ОРЦБ, функции расчетной системы были выделены из ММВБ и переданы специально созданным для этого расчетным небанковским кредитным организациям, в том числе созданной в 1996 г. Расчетной палате ММВБ. Функции депозитария были переданы ММВБ созданному в 1997 г. Национальному депозитарному центру (НДЦ). В настоящее время функции расчетного центра ОРЦБ и депозитария выполняет Национальный расчетный депозитарий (НРД), созданный путем объединения Расчетной палаты ММВБ и НДЦ в ноябре 2010 г. НРД является дочерней организацией ММВБ.

6.2. ПРАВОВОЕ ПОЛОЖЕНИЕ РАСЧЕТНОГО ЦЕНТРА ОРЦБ

Правовое положение кредитной организации, выполняющей функции расчетного центра ОРЦБ (РЦ ОРЦБ), определяется следующими нормативными актами Банка России: положениями № 32-П, № 219-П, а также договором на выполнение функций Расчетного центра ОРЦБ, заключаемым такой кредитной организацией с Банком России.

Следует отметить, что содержание определений РЦ ОРЦБ, приведенное в нормативных актах Банка России, не совпадает.

Так, согласно Положению № 32-П РЦ ОРЦБ — небанковская кредитная организация, которой на основании договора с Банком России на выполнение функций РЦ ОРЦБ открыт корреспондентский счет № 30105 в расчетном подразделе-

¹ Вестник Банка России. 1996. № 11.

нии Банка России для проведения расчетов в соответствии с Положением № 32-П и этим договором.

В соответствии с Положением № 219-П РЦ ОРЦБ — небанковская кредитная организация, уполномоченная на основании договора с Банком России обеспечивать расчеты дилеров по сделкам с облигациями путем открытия банковских счетов дилеров и осуществления операций по этим счетам.

Кредитную организацию, выполняющую функции РЦ ОРЦБ, следует рассматривать в двух аспектах: во-первых, как элемент банковской системы, во-вторых, как элемент инфраструктуры организованного рынка ценных бумаг.

Для определения места РЦ ОРЦБ в банковской системе следует рассмотреть классификацию кредитных организаций, основанную на совокупности банковских операций, право совершения которых предоставлено определенным видам кредитных организаций (ст. 1 и 5 Закона о банках).

Закон о банках охватывает общим понятием «кредитные организации» банки и небанковские кредитные организации, при этом к последним относит, во-первых, кредитные организации, имеющие право на осуществление переводов денежных средств без открытия банковских счетов и связанных с ними иных банковских операций, и, во-вторых, кредитные организации, имеющие право осуществлять отдельные банковские операции, допустимые сочетания которых для таких небанковских кредитных организаций устанавливаются Банком России.

Такие сочетания банковских операций установлены Банком России для двух видов НКО: расчетных НКО и НКО, осуществляющих депозитно-кредитные операции (НДКО).

Функции расчетных центров ОРЦБ выполняют только расчетные НКО.

Расчетные НКО, выполняющие функции расчетных центров ОРЦБ, в отличие от «обычных» расчетных НКО наделены Банком России полномочиями осуществлять расчеты по итогам биржевых торгов, в связи с чем режимы открываемых в Банке России счетов указанными расчетными НКО отличаются от режимов счетов, открываемых в Банке России другими расчетными НКО, на которые такие полномочия не возложены.

Таким образом, расчетные центры ОРЦБ следует рассматривать в качестве подвида расчетных НКО.

Место РЦ ОРЦБ в инфраструктуре организованного рынка ценных бумаг показано на рис. 6.2.

Расчетный центр организует расчеты на различных секторах ОРЦБ в соответствии с Положением № 32-П. Под сектором ОРЦБ понимается совокупность отношений, связанных с обращением на ОРЦБ финансовых активов, правила исполнения сделок с которыми одинаковы. Виды секторов ОРЦБ, как правило, соответствуют определенным видам биржевых рынков.

Перечень действующих секторов ОРЦБ и порядок их открытия в расчетных центрах ОРЦБ устанавливаются указаниями Банка России.



Рис. 6.2. Место РЦ ОРЦБ в банковской системе

Каждый РЦ ОРЦБ имеет право осуществлять денежные расчеты не более чем для пяти¹ секторов ОРЦБ:

- для расчетов по государственным федеральным ценным бумагам;
- расчетов по иным государственным и негосударственным ценным бумагам;
- расчетов на срочном рынке;
- расчетов на валютном рынке;
- расчетов на межбанковском кредитном рынке.

Каждый РЦ ОРЦБ имеет право самостоятельно устанавливать набор финансовых активов, расчеты по которым он обслуживает на любом из вышеуказанных секторов, кроме сектора ОРЦБ для государственных федеральных ценных бумаг. Расчеты по операциям с финансовыми активами в секторе ОРЦБ для государственных федеральных ценных бумаг производятся на основе специального предварительного разрешения Банка России для каждого вида таких финансовых активов.

О начале проведения расчетов по вновь открываемому сектору ОРЦБ расчетный центр ОРЦБ обязан уведомить Банк России не позднее чем за один месяц до начала проведения расчетов. В таком уведомлении должно содержаться указание на то, расчеты по какому сектору ОРЦБ предполагается обслуживать, какие торговые и (или) клиринговые системы финансового рынка будут задействованы, а также правила исполнения сделок и правила бухгалтерского учета. В случае воз-

¹ Такое требование по поводу количества секторов установлено Положением № 32-П. Один РЦ ОРЦБ может обслуживать указанные сектора для различных бирж, например валютный рынок ММВБ-РТС и валютный рынок Санкт-Петербургской валютной биржи. В этом случае это будут различные сектора и в сумме их должно быть не более пяти.

ражений Банк России в двухнедельный срок направляет РЦ ОРЦБ письменный ответ, запрещающий проведение соответствующих расчетов.

6.3. ОГРАНИЧЕНИЕ РИСКОВ В ДЕЯТЕЛЬНОСТИ РЦ ОРЦБ

Отсутствие в деятельности РЦ ОРЦБ основных видов рисков, прежде всего кредитного, обусловлено тем обстоятельством, что функции РЦ ОРЦБ в соответствии с нормативными актами Банка России могут выполнять только расчетные НКО, которые в отличие от банков не осуществляют активных операций, финансируемых пассивными операциями.

Банк России в целях регулирования (ограничения) принимаемых расчетными НКО рисков установил Инструкцией от 26 апреля 2006 г. № 129-И¹ (в ред. Указания Банка России от 12 декабря 2011 г. № 2747-У²) допустимые сочетания банковских операций, числовые значения методики расчета обязательных нормативов, а также особенности осуществления Банком России надзора за их соблюдением.

Согласно указанной Инструкции Банка России расчетные НКО вправе осуществлять в сочетании следующие банковские операции:

- открытие и ведение банковских счетов юридических лиц;
- осуществление переводов денежных средств по поручению юридических лиц, в том числе банков-корреспондентов, по их банковским счетам;
- инкассацию денежных средств, векселей, платежных и расчетных документов и кассовое обслуживание физических и юридических лиц;
- куплю-продажу иностранной валюты в наличной и безналичной форме;
- осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов).

РНКО не вправе осуществлять следующие банковские операции:

- привлечение денежных средств физических и юридических лиц во вклады;
- открытие и ведение банковских счетов физических лиц;
- осуществление переводов денежных средств по поручению физических лиц по их банковским счетам;
- привлечение во вклады и размещение драгоценных металлов;
- выдачу банковских гарантий.

Расчетным НКО в целях минимизации риска ликвидности и кредитного риска:

- запрещается деятельность по привлечению средств физических и юридических лиц (например, путем выпуска РНКО собственных векселей);

¹ Вестник Банка России. 2006. № 32.

² Вестник Банка России. 2011. № 72.

- разрешается размещать денежные средства от своего имени и за свой счет в пределах, установленных обязательными нормативами в соответствии с Инструкцией Банка России № 129-И, исключительно в долговые обязательства Российской Федерации; в депозиты в Банке России; в облигации Банка России; в кредиты и депозиты, размещенные в имеющих инвестиционный рейтинг не ниже ВВВ по классификации иностранного рейтингового агентства Standard & Poor's или не ниже аналогичного рейтинга по классификациям Fitch Ratings, Moody's, банках — нерезидентах стран, входящих в группу развитых стран, и в кредитных организациях — резидентах Российской Федерации; в государственные долговые обязательства стран из числа группы развитых стран, имеющих инвестиционный рейтинг не ниже ВВВ по классификации иностранного рейтингового агентства Standard & Poor's или не ниже аналогичного рейтинга по классификациям Fitch Ratings, Moody's;
- разрешается открывать корреспондентские счета помимо корреспондентского счета в Банке России только в имеющих инвестиционный рейтинг не ниже ВВВ по классификации иностранного рейтингового агентства Standard & Poor's или не ниже аналогичного рейтинга по классификациям Fitch Ratings, Moody's, банках — нерезидентах стран, входящих в группу развитых стран, и в кредитных организациях — резидентах Российской Федерации.

Исключением из приведенных выше требований является право расчетных НКО предоставлять кредиты от своего имени и за свой счет участникам расчетов на завершение расчетов по совершенным ими сделкам в пределах созданного участниками расчетов фонда поддержания ликвидности.

Другие ограничения связаны с тем, что расчетный центр ОРЦБ согласно Положению № 219-П не может быть дилером или выполнять функции торговой системы на рынке облигаций.

6.4. ПРАВОВОЕ ПОЛОЖЕНИЕ УЧАСТНИКА РЦ ОРЦБ

Согласно Положению № 32-П участник РЦ ОРЦБ — организация, которой открыт счет в Расчетном центре ОРЦБ для проведения денежных расчетов по сделкам на ОРЦБ на основании договора, заключенного с этим расчетным центром ОРЦБ, и в соответствии с указанным Положением.

Участниками РЦ ОРЦБ являются, как правило, организации — участники торгов (клиринга) на различных биржевых рынках, а также клиенты участников торгов (клиринга).

В зависимости от вида рынка к участникам торгов предъявляются специальные требования.

Так, участниками торгов на рынке федеральных государственных ценных бумаг могут быть только дилеры.

Из Положения № 219-П следует, что дилером признается юридическое лицо, являющееся профессиональным участником рынка ценных бумаг, совершающее в соответствии с действующим законодательством гражданско-правовые сделки (купли-продажи) с облигациями как от своего имени и за свой счет, так и в качестве поверенного или комиссионера, действующего на основании договора поручения или комиссии.

Дилер для выполнения указанных функций заключает в соответствии с Положением Банка России от 10 ноября 1998 г. № 59-П «О порядке рассмотрения документов и заключения Банком России договоров о выполнении функций дилера на рынке ГКО-ОФЗ»¹ договор с Банком России на выполнение функций дилера на рынке облигаций.

Участниками торгов и клиринга на валютном рынке могут быть только кредитные организации, имеющие лицензию Банка России на осуществление банковских операций со средствами в рублях и иностранной валюте. Требования к участникам торгов и клиринга на валютном рынке установлены правилами членства в секции валютного рынка ММВБ, утвержденного Советом директоров ММВБ, и правилами осуществления клиринговой деятельности Акционерным коммерческим банком «Национальный клиринговый центр» (НКЦ), который на валютном рынке осуществляет функции центрального контрагента.

Участниками торгов на срочном и фондовом рынках ММВБ могут быть юридические лица — профессиональные участники рынка ценных бумаг, имеющие лицензию на осуществление брокерской и (или) дилерской деятельности и (или) деятельности по управлению ценными бумагами, выданную уполномоченным федеральным органом исполнительной власти, отвечающие требованиям законодательства Российской Федерации и требованиям, предъявляемым к участникам торгов в соответствии с внутренними документами ММВБ и Фондовой биржи ММВБ, регламентирующими порядок совершения операций на соответствующем рынке.

Банк России является участником торгов на рынке федеральных государственных ценных бумаг, валютном и фондовом рынках.

Положение о деятельности по организации торговли на рынке ценных бумаг, утвержденное приказом ФСФР России от 28 декабря 2010 г. № 10-78/пз-н², устанавливает требование, согласно которому участниками торгов у организатора торговли могут быть только брокеры, дилеры, управляющие и Банк России. Организатор торговли осуществляет регистрацию (аккредитацию) участников торгов, клиентов участников торгов и клиентов брокеров (управляющих), являющихся клиентами участников торгов.

Таким образом, понятие «участник расчетного центра ОРЦБ» является производным от понятия «участник торгов (клиринга)», что не исключает возможность установления расчетным центром ОРЦБ как кредитной организацией к та-

¹ Вестник Банка России. 1998. № 79.

² Российская газета. 2011. 25 апреля.

ким участникам расчетов дополнительных требований, основанных на законодательстве о банках и банковской деятельности и нормативных актах Банка России.

Следует отметить, что Закон о НПС предусматривает, что участниками платежной системы (в том числе прямыми участниками) могут стать профессиональные участники рынка ценных бумаг, а также юридические лица, являющиеся участниками организованных торгов и (или) участниками клиринга в соответствии с Законом о клиринге.

Закон об организованных торгах (ст. 16) устанавливает новые требования к допуску к участию в организованных торгах и определяет категории лиц (в зависимости от предмета торгов), которые могут быть допущены к таким торгам.

Так, к участию в организованных торгах ценными бумагами могут быть допущены дилеры, управляющие и брокеры, которые имеют лицензию профессионального участника рынка ценных бумаг, управляющие компании инвестиционных фондов, паевых инвестиционных фондов, негосударственных пенсионных фондов, центральный контрагент, а также Банк России.

К участию в организованных торгах иностранной валютой могут быть допущены кредитные организации, имеющие право на основании лицензий Банка России осуществлять банковские операции со средствами в иностранной валюте, центральный контрагент, Банк России, а также иные юридические лица, которые вправе осуществлять куплю-продажу иностранной валюты в силу федерального закона. Если договоры купли-продажи иностранной валюты на организованных торгах заключаются с центральным контрагентом, являющимся уполномоченным банком, к участию в этих организованных торгах могут быть допущены иные юридические лица, созданные в соответствии с законодательством Российской Федерации.

К участию в организованных торгах, на которых заключаются договоры, являющиеся производными финансовыми инструментами, могут быть допущены Банк России, центральный контрагент, управляющие компании инвестиционных фондов, паевых инвестиционных фондов, негосударственных пенсионных фондов, а также дилеры, управляющие, брокеры, которые имеют лицензию профессионального участника рынка ценных бумаг, в том числе брокеры, имеющие лицензию на осуществление брокерской деятельности только по заключению договоров, являющихся производными финансовыми инструментами, базисным активом которых является товар. К участию в организованных торгах, на которых заключаются договоры, являющиеся производными финансовыми инструментами, базисным активом которых является товар, могут быть допущены также юридические лица, созданные в соответствии с законодательством Российской Федерации, если такие договоры заключаются за их счет¹.

¹ Части 1 и 4 ст. 16 Закона об организованных торгах, предусматривающие требования к участникам торгов ценными бумагами и участникам торгов, на которых заключаются договоры, являющиеся производными финансовыми инструментами, вступают в силу с 1 января 2013 г.

6.5. СТРУКТУРА ДОГОВОРНЫХ ОТНОШЕНИЙ НА ОРЦБ

Построение договорных отношений на ОРЦБ подчинено той же цели, что и создание организованного рынка ценных бумаг, а именно обеспечение размещения и обращения облигаций. Без организации договорных отношений между участниками рынка облигаций, в том числе между ее инфраструктурными элементами, заключение и исполнение сделок купли-продажи облигаций через торговую систему было бы невозможным.

В организации договорных отношений на ОРЦБ, на наш взгляд, следует выделить несколько уровней:

- 1) договор между эмитентом и генеральным агентом эмитента;
- 2) договоры, заключаемые инфраструктурными организациями с эмитентом и генеральным агентом эмитента;
- 3) договоры между инфраструктурными организациями;
- 4) договоры, заключаемые участниками торгов (клиринга) с Банком России и инфраструктурными организациями.

Рассмотрим структуру договорных отношений на ОРЦБ, обеспечивающих денежные расчеты по итогам биржевых торгов, через призму отношений НРД с другими участниками рынка государственных ценных бумаг (рис. 6.3).

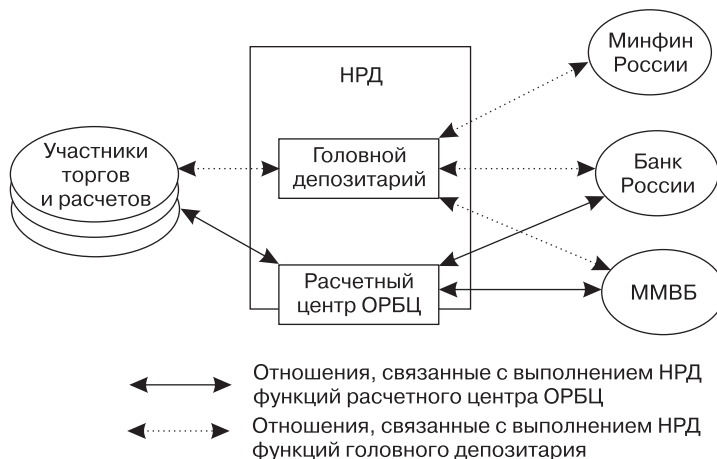


Рис. 6.3. Структура договорных отношений на ОРЦБ

Первый уровень договорных отношений представлен договором между Банком России и Минфином России, поскольку Банк России на рынке облигаций выполняет функции генерального агента эмитента — Минфина России.

Согласно п. 6.2 Положения № 219-П Банк России, выполняя функции генерального агента эмитента по обслуживанию выпусков облигаций:

- заключает договоры с организациями на выполнение функций торговой системы, расчетных центров ОРЦБ, а также договор о взаимодействии с депозитарием;
- заключает договоры с организациями на выполнение функций дилеров, первичных дилеров;
- устанавливает по согласованию с эмитентом условия проведения аукциона по размещению облигаций и по поручению эмитента проводит указанный аукцион;
- осуществляет по поручению эмитента дополнительную продажу на рынке облигаций, не проданных в период их размещения, а также выкуп облигаций размещенных ранее выпусков;
- выполняет иные действия в соответствии с договором между эмитентом и Банком России.

Второй уровень договорных отношений представлен договорами, заключенными Банком России с инфраструктурными организациями, в том числе с ММВБ и НРД, а также договором между Минфином России и НРД.

НРД выполняет функции РЦ ОРЦБ на основании договора «О выполнении функций Расчетного центра на организованном рынке ценных бумаг», заключенного с Банком России.

Из содержания этого договора следует, что функции РЦ ОРЦБ заключаются в обеспечении денежных расчетов по сделкам его участников с финансовыми активами на ОРЦБ.

На основании указанного договора РЦ ОРЦБ в расчетном подразделении Банка России открыт корреспондентский счет № 30106 «Корреспондентские счета расчетных центров ОРЦБ в Банке России», режим которого отличается от режимов таких корреспондентских счетов, как № 30102 «Корреспондентские счета кредитным организациям в Банке России» и № 30104 «Корреспондентские счета расчетных небанковских кредитных организаций».

Согласно ранее действовавшим Правилам ведения бухгалтерского учета в кредитных организациях¹ назначением корреспондентского счета РЦ ОРЦБ в Банке России являлся учет исключительно средств клиентов — участников РЦ для расчетов по операциям на ОРЦБ. Свои собственные средства РЦ ОРЦБ обязаны были учитывать на счете № 30110 «Корреспондентские счета в кредитных организациях-корреспондентах» (письмо Банка России от 10 октября 1996 г. № 339)².

Действующие в настоящее время Правила ведения бухгалтерского учета в кредитных организациях, расположенных на территории Российской Федерации, утвержденные Положением Банка России от 26 марта 2007 г. № 302-П³ (далее — Правила ведения бухгалтерского учета в кредитных организациях) значи-

¹ Вестник Банка России. 1997. № 49.

² Вестник Банка России. 1996. № 55.

³ Вестник Банка России. 2007. № 20—21.

тельно приблизили режим корреспондентского счета РЦ ОРЦБ в Банке России к режиму корреспондентского счета «обычной» НКО, предоставив РЦ ОРЦБ возможность учитывать на нем не только средства участников РЦ ОРЦБ, но и собственные средства.

НРД выполняет на ОРЦБ не только функции расчетного центра, но и как правопреемник НДЦ функции головного депозитария, которые заключаются в осуществлении централизованного хранения облигаций и учета прав на них в соответствии с законодательством Российской Федерации и условиями заключенных с депонентами договоров. Указанные функции НРД выполняет на основании соответствующих договоров с эмитентом и Банком России.

Третий уровень договорных отношений представлен договорами, заключаемыми НРД как при осуществлении функций РЦ ОРЦБ, так и функций головного депозитария с ММВБ, которая выполняет функции торговой системы на ОРЦБ.

Взаимодействие НРД при осуществлении функций РЦ ОРЦБ с ММВБ осуществляется на основе договоров, предметом которых является организация денежных расчетов на секторах ОРЦБ: «ГКО, ОФЗ-ПК» и «Срочный рынок ММВБ». Договор об организации денежных расчетов на секторе «Фондовый рынок ММВБ» заключен с НКЦ, осуществляющим клиринг обязательств по сделкам, заключенным на Фондовой бирже ММВБ.

Следует отметить, что ММВБ тесно взаимосвязана с НРД не только указанными выше договорными отношениями, а также технологически и технически, но и в правовом плане в силу своего преобладающего участия в его уставном капитале, в связи с чем имеет возможность определять решения, принимаемые органами управления НРД.

В соответствии со ст. 4 Закона о банках объединение юридических лиц с участием кредитной организации, в котором юридическое лицо, не являющееся кредитной организацией, имеет возможность прямо или косвенно (через третье лицо) оказывать существенное влияние на решения, принимаемые органами управления кредитной организации, признается банковским холдингом.

Таким образом, объединение ММВБ и НРД следует признать в силу указанного закона **банковским холдингом**, в который наряду с этими организациями входят также аффилированные с ними юридические лица.

О создании холдинга на базе биржи, являющейся ядром организованного рынка, вокруг которого могут быть объединены клиринг, расчеты и учетная система, указывается в Стратегии развития финансового рынка Российской Федерации на период до 2020 г. В частности, в этом документе отмечается, что «одной из приемлемых моделей консолидации биржевой инфраструктуры может стать вертикально интегрированная модель холдинга с широким представительством в его капитале банков, небанковских институтов и, возможно, государства и иностранных институтов». Далее в Стратегии указывается, что «в рамках такого холдинга возможны объединение локальных торговых площадок, в том числе специализирующихся по видам торгуемых инструментов и активов, расчетных

депозитариев, клиринговых организаций, а также унификация с учетом установленных государством единых требований электронных стандартов обмена данными, заключения сделок и расчетов». Предложенная модель, поясняется далее, «способна сконцентрировать и направить на дальнейшее повышение конкурентоспособности российского финансового рынка необходимые управленческие, технологические и финансовые ресурсы»¹.

И наконец, четвертый уровень договорных отношений на ОРЦБ представлен договорами, заключаемыми участниками торгов с Банком России и инфраструктурными организациями.

Из нормативных актов Банка России, регулирующих порядок обращения федеральных государственных ценных бумаг и расчетов на ОРЦБ, а также внутренних документов ММВБ, в том числе регламента проведения операций в системе электронных торгов по сделкам с государственными и иными ценными бумагами, утвержденного Правлением ММВБ, следует, что юридическое лицо для участия в торгах на рынке облигаций должно заключить следующие договоры:

- с Банком России — договор «О выполнении функций дилера на рынке ГКО-ОФЗ» ;
- с НРД как расчетным центром ОРЦБ — договор банковского счета для открытия счета участника расчетного центра ОРЦБ и соответствующее дополнительное соглашение к такому договору для открытия торгового счета, а с НРД как депозитарием — договор об обслуживании в депозитарии на рынке облигаций;
- с ММВБ — договор об участии в системе электронных торгов ММВБ по сделкам с государственными ценными бумагами и договор об обеспечении технического доступа к программно-техническому комплексу ММВБ.

6.6. ВИДЫ БАНКОВСКИХ И ВНУТРИБАНКОВСКИХ СЧЕТОВ, ИСПОЛЬЗУЕМЫХ В РАСЧЕТАХ НА ОРЦБ, И ИХ РЕЖИМЫ

Обязательства по сделкам, заключенным на организованном рынке ценных бумаг, могут считаться исполненными только после завершения соответствующих денежных расчетов, которые производятся с использованием банковских счетов, открываемых участниками расчетов в расчетных НКО, выполняющих функции расчетных центров ОРЦБ.

СЧЕТА УЧАСТНИКОВ РЦ ОРЦБ

Участникам расчетов НРД на основании заключенных с ними договоров банковского счета открывает счет № 30401 «Счета участников РЦ ОРЦБ», режим

¹ СЗ РФ. 2009. № 3. Ст. 423.

ведения которого установлен Правилами ведения бухгалтерского учета в кредитных организациях и Указанием Банка России от 15 июня 2001 г. № 977-У «О совершенствовании расчетов участников Расчетного центра ОРЦБ»¹ (далее — Указание № 977-У).

Режим счета участника РЦ ОРЦБ № 30401 предусматривает проведение следующих операций.

По кредиту счета проводятся средства:

- поступившие участникам РЦ для осуществления расчетов по операциям на ОРЦБ в корреспонденции с корреспондентским счетом РЦ ОРЦБ в Банке России, корреспондентскими счетами в кредитных организациях-корреспондентах и корреспондентскими счетами в банках-нерезидентах в СКВ;
- зачисленные РЦ ОРЦБ участникам РЦ после завершения расчетов по итогам операций на ОРЦБ в корреспонденции со счетом «Средства участников РЦ ОРЦБ для обеспечения расчетов по операциям на ОРЦБ» ;
- поступившие от других участников РЦ по их поручениям в корреспонденции со счетами участников РЦ.

По дебету счета списываются средства:

- перечисленные из РЦ ОРЦБ по поручению участников расчетного центра в корреспонденции с корсчетом Расчетного центра ОРЦБ в Банке России, корсчетами в кредитных организациях — корреспондентах и корсчетами в банках-нерезидентах в СКВ;
- переведенные участниками расчетного центра в РЦ ОРЦБ для обеспечения расчетов по операциям на ОРЦБ в корреспонденции со счетом «Средства участников РЦ ОРЦБ для обеспечения расчетов по операциям на ОРЦБ» ;
- перечисленные по поручению участника расчетного центра другим участникам расчетного центра в корреспонденции со счетами участников расчетного центра;
- депонируемые в РЦ ОРЦБ участниками расчетного центра в качестве гарантийного обеспечения расчетов по операциям на секторах ОРЦБ, для которых предусмотрено это обеспечение, в корреспонденции со счетом «Средства участников РЦ ОРЦБ, депонируемые в Расчетном центре для гарантийного обеспечения расчетов по операциям на секторах ОРЦБ» ;
- списанные РЦ ОРЦБ с участников расчетного центра в оплату комиссионного и других вознаграждений в корреспонденции с соответствующими счетами.

Указание Банка России № 977-У значительно расширяет возможности оперативного управления участниками РЦ ОРЦБ денежными средствами. В частности, согласно п. 2 участник РЦ ОРЦБ со счета участника РЦ ОРЦБ, открытого ему в РЦ ОРЦБ, может направлять денежные средства на счета, открытые ему

¹ Вестник Банка России. 2001. № 38.

в учреждении Банка России, в кредитных организациях, в том числе расчетных НКО, и другие счета этого участника РЦ ОРЦБ в РЦ ОРЦБ, а также осуществлять расчеты по своим обязательствам, включая расчеты с другими участниками РЦ ОРЦБ в одном РЦ ОРЦБ.

Счет участника РЦ ОРЦБ может быть открыт как в валюте Российской Федерации, так и в иностранной валюте (в последнем случае совершение операций по счету производится с соблюдением валютного законодательства).

СЧЕТА ДОВЕРИТЕЛЬНОГО УПРАВЛЕНИЯ

Для обеспечения расчетов по операциям доверительного управления кредитные организации — доверительные управляющие могут открывать в расчетных центрах ОРЦБ **счета доверительного управления** на балансовом счете № 40701 «Счета финансовых организаций».

Согласно Правилам ведения бухгалтерского учета в кредитных организациях, расчеты по операциям доверительного управления на ОРЦБ осуществляются с учетом следующих особенностей:

1) для расчетов по операциям доверительного управления доверительно-му управляющему открываются отдельные лицевые счета балансового счета № 30403 «Средства участников РЦ ОРЦБ для обеспечения расчетов по операциям на ОРЦБ» по видам валют;

2) для участия в торгах доверительный управляющий должен перечислить необходимую сумму денежных средств со счета № 40701 «Счета финансовых организаций», открытого в РЦ ОРЦБ, на отдельный лицевой счет балансового счета № 30403 «Средства участников РЦ ОРЦБ для обеспечения расчетов по операциям на ОРЦБ»;

3) по итогам торгов денежные средства доверительных управляющих перечисляются с отдельных лицевых счетов балансового счета № 30403 на открытые им в РЦ ОРЦБ лицевые счета балансового счета № 40701 «Счета финансовых организаций».

СПЕЦИАЛЬНЫЕ БРОКЕРСКИЕ И СПЕЦИАЛЬНЫЕ ДЕПОЗИТАРНЫЕ СЧЕТА

Участникам расчетов, не являющимся кредитными организациями, могут открываться на балансовом счете № 30401 **специальные брокерские и специальные депозитарные счета**.

Порядок открытия и режим специального брокерского счета регулируются ст. 3 Закона о рынке ценных бумаг, а также Требованиями к правилам осуществления брокерской деятельности при совершении операций с денежными средствами клиентов брокера, утвержденных приказом ФСФР России от 5 апреля 2011 г. № 11-7/пз-н¹.

Согласно ст. 3 Закона о рынке ценных бумаг денежные средства клиентов, переданные ими брокеру для совершения сделок с ценными бумагами и (или) за-

¹ Российская газета. 2011. № 122.

ключения договоров, являющихся производными финансовыми инструментами, а также денежные средства, полученные брокером по таким сделкам и (или) таким договорам, которые совершены (заключены) брокером на основании договоров с клиентами, должны находиться на отдельном банковском счете (счетах), открываемом (открываемых) брокером в кредитной организации (специальный брокерский счет).

Закон о рынке ценных бумаг устанавливает следующие требования к режиму специального брокерского счета, а также к порядку его открытия и ведения:

- брокер обязан вести учет денежных средств каждого клиента, находящихся на специальном брокерском счете (счетах), и отчитываться перед клиентом;
- на денежные средства клиентов, находящиеся на специальном брокерском счете (счетах), не может быть обращено взыскание по обязательствам брокера;
- брокер не вправе зачислять собственные денежные средства на специальный брокерский счет (счета), за исключением случаев их возврата клиенту и (или) предоставления займа клиенту в порядке, установленном ст. 3 Закона о рынке ценных бумаг;
- брокер вправе использовать в своих интересах денежные средства, находящиеся на специальном брокерском счете (счетах), если это предусмотрено договором о брокерском обслуживании, гарантируя клиенту исполнение его поручений за счет указанных денежных средств или их возврат по требованию клиента. Денежные средства клиентов, предоставивших право их использования брокеру в его интересах, должны находиться на специальном брокерском счете (счетах), отдельном от специального брокерского счета (счетов), на котором находятся денежные средства клиентов, не предоставивших брокеру такого права. Денежные средства клиентов, предоставивших брокеру право их использования, могут зачисляться брокером на его собственный банковский счет.

Расчетные центры ОРЦБ должны открывать специальные брокерские счета брокерам, не являющимся кредитными организациями, на балансовых счетах № 30401 «Счета участников РЦ ОРЦБ» и № 30403 «Средства участников РЦ ОРЦБ для обеспечения расчетов по операциям на ОРЦБ».

Требования об открытии и ведении **специального депозитарного счета** установлены ст. 7 Закона о рынке ценных бумаг.

Согласно указанной статье в случае оказания депоненту услуг, связанных с получением доходов по ценным бумагам и иных причитающихся владельцам ценных бумаг выплат, денежные средства депонентов должны находиться на отдельном банковском счете (счетах), открываемом (открываемых) депозитарием в кредитной организации (специальный депозитарный счет (счета)). Депозитарий обязан вести учет находящихся на специальном депозитарном счете (счетах) денежных средств каждого депонента и отчитываться перед ним. На денежные средства депонентов, находящиеся на специальном депозитарном счете (счетах), не может быть обраще-

но взыскание по обязательствам депозитария. Депозитарий не вправе зачислять собственные денежные средства на специальный депозитарный счет (счета), за исключением случаев их выплаты депоненту, а также использовать в своих интересах денежные средства, находящиеся на специальном депозитарном счете (счетах).

6.7. ВНУТРИБАНКОВСКИЕ СЧЕТА

Участнику расчетов, заключившему договор банковского счета с расчетным центром ОРЦБ, а также соглашение о проведении расчетных операций на секторах ОРЦБ к такому договору, РЦ ОРЦБ открываются лицевые счета к балансовым счетам № 30403 и 30405.

Неотъемлемой частью соглашения о проведении расчетных операций на секторах ОРЦБ являются правила проведения операций в секторах ОРЦБ, которые состоят из разделов, регулирующих порядок осуществления операций клиентом в следующих секторах ОРЦБ: ГКО, ОФЗ-ПК; срочный рынок ММВБ; фондовый рынок ММВБ; фондовый рынок СПВБ. Правила проведения операций в секторах ОРЦБ содержат регламенты работы НРД в каждом упомянутом секторе ОРЦБ. Соглашением о проведении расчетных операций на секторах ОРЦБ установлено, что правила проведения операций в секторах ОРЦБ могут изменяться и дополняться НРД в одностороннем порядке на основании изменений нормативных актов Банка России, документов клиринговой организации (организации, осуществляющей расчет денежных позиций участников по итогам торгов в секторах ОРЦБ), а также в связи с открытием по согласованию с Банком России новых секторов ОРЦБ.

Назначением счета № 30403 (**торговый счет**) является учет средств участников расчетного центра для обеспечения расчетов по операциям на ОРЦБ, которые блокируются до завершения расчетным центром расчетов по итогам операций, счета № 30405 (**счет депонирования**) — учет средств участников РЦ, депонируемых ими в качестве гарантийного обеспечения расчетов по операциям на тех секторах ОРЦБ, для которых предусмотрено создание обеспечения для завершения расчетов. Для расчетов на ОРЦБ также используется счет № 30407 (**клиринговый счет**), назначением которого является учет в РЦ ОРЦБ расчетов по зачету обязательств и требований по итогам операций их участников на ОРЦБ.

Режимы функционирования балансовых счетов № 30403 и 30407 предусматривают их обнуление на конец каждого операционного дня, в связи с чем остатки средств с указанных счетов зачисляются РЦ ОРЦБ на банковский счет № 30401 «Счета участников РЦ ОРЦБ».

Следует отметить, что лицевые счета к балансовым счетам № 30403, 30405, 30407 относятся к категории **внутрибанковских счетов** (внутренних счетов РЦ ОРЦБ), так как открываются Расчетным центром в соответствии с п. 2.4 Положения № 32-П без участия клиента и функционально предназначены для обеспечения расчетов по банковским счетам участников РЦ ОРЦБ (№ 30401) по операциям на различных секторах ОРЦБ.

По отношению к торговым счетам понятие «внутрибанковские счета» применяется в п. 3.4 Положения № 219-П.

Исходя из изложенного выше можно сделать вывод о том, что правовой режим банковского счета, установленный правилами главы 45 ГК РФ «Банковский счет», на указанные счета не распространяется и, следовательно, денежные средства, находящиеся на таких счетах, не могут быть объектами ареста и обращения взыскания.

Рассматриваемые счета не подпадают под определение счетов, изложенное в ст. 11 НК РФ¹, согласно которому счета (счет) — расчетные (текущие) и иные счета в банках, открытые на основании договора банковского счета, на которые зачисляются и с которых могут расходоваться денежные средства организаций и индивидуальных предпринимателей. Учитывая это обстоятельство, кредитные организации, выполняющие функции РЦ ОРЦБ и участники РЦ ОРЦБ, не обязаны сообщать об открытии лицевых счетов к балансовым счетам № 30403, 30405, 30407 в налоговые органы в соответствии со ст. 86 НК РФ, а операции по таким счетам не могут быть приостановлены налоговыми органами в соответствии со ст. 76 НК РФ.

Федеральная налоговая служба РФ (письмо от 16 января 2008 г. № 09-6-02/180) в ответ на запрос Расчетной палаты ММВБ касательно статуса счета № 30405 подтвердила, что этот счет относится к категории внутрибанковских счетов и не подлежит регистрации в налоговых органах.

Клиентам (в том числе нерезидентам), которые не являются участниками расчетов на ОРЦБ, открываются балансовые счета 30109 «Корреспондентские счета кредитных организаций — корреспондентов» и № 30111 «Корреспондентские счета банков-нерезидентов» — для кредитных организаций и на балансовых счетах Раздела 4 «Операции с клиентами» Плана счетов бухгалтерского учета в кредитных организациях — для организаций, не являющихся кредитными. Возможность открытия РЦ ОРЦБ указанных счетов для проведения расчетов, не связанным с операциями на организованном рынке ценных бумаг, подтверждена письмом Департамента бухгалтерского учета и отчетности Банка России от 5 августа 2008 г. № 18-1-2-5/1785.

6.8. ТОРГОВЫЕ И КЛИРИНГОВЫЕ БАНКОВСКИЕ СЧЕТА

Следует отметить, что Закон о клиринге, который вступил в силу с 1 января 2012 г., предусматривает использование при осуществлении клиринга и исполнении обязательств, допущенных к клирингу, в том числе по итогам организованных торгов, счетов двух видов: **торговых банковских счетов** (ст. 15) и **клиринговых банковских счетов** (ст. 16). Статус указанных счетов и их правовой режим принципиально отличаются от торговых и клиринговых внутрибанковских счетов, описанных выше.

¹ СЗ РФ. 1988. № 31. Ст. 3824.

Торговым банковским счетом, согласно Закону о клиринге, является отдельный банковский счет, открываемый участникам клиринга и соответствующий следующим требованиям:

1) на указанном счете учитываются соответственно денежные средства, которые могут быть использованы для исполнения и (или) обеспечения исполнения обязательств, допущенных к клирингу, а также обязательств по уплате вознаграждения клиринговой организации и организациям, указанным в п. 4—7 ч. 2 ст. 19 Закона о клиринге;

2) операции по указанному счету осуществляются либо на основании распоряжений клиринговой организации без распоряжения лица, которому открыт данный счет, либо на основании распоряжений лица, которому открыт такой счет, с согласия клиринговой организации.

Согласие клиринговой организации на совершение операций по торговому банковскому счету дается способом, предусмотренным договором банковского счета в соответствии с правилами клиринга, в том числе путем подписания клиринговой организацией платежного документа, в соответствии с которым лицо, которому открыт такой счет, дает распоряжение кредитной организации о совершении операций по этому счету.

Торговые банковские счета открываются с указанием клиринговой организации, которая вправе давать распоряжения по этим счетам.

Из статьи 16 Закона о клиринге следует, что клиринговым банковским счетом является отдельный банковский счет, который открывается клиринговой организацией и на котором учитываются денежные средства участников клиринга, лица, осуществляющего функции центрального контрагента, и (или) иных лиц, предусмотренных правилами клиринга. Денежные средства, учитываемые на таком счете, могут быть использованы для исполнения и (или) обеспечения исполнения обязательств, допущенных к клирингу, а также обязательств по уплате вознаграждения клиринговой организации и организациям, указанным в п. 4—7 ч. 2 ст. 19 Закона о клиринге.

Денежные средства участника клиринга и его клиентов должны учитываться во внутреннем учете клиринговой организации отдельно. Клиринговая организация по требованию участника клиринга должна вести отдельный внутренний учет денежных средств клиента данного участника клиринга, учитываемых на клиринговом банковском счете.

Клиринговая организация не вправе перечислять на клиринговый счет собственные денежные средства, за исключением случаев, когда в соответствии с правилами клиринга это необходимо для исполнения обязательств, допущенных к клирингу, а также для исполнения обязанности клиринговой организации по возврату денежных средств в случаях, предусмотренных ч. 12 ст. 23 и ч. 8 ст. 24 Закона о клиринге.

В случае признания клиринговой организации банкротом имущество, находящееся на клиринговом банковском счете, в конкурсную массу не включается. Де-

нежные средства подлежат возврату участнику клиринга, а иное имущество — передавшим его лицам в размере, оставшемся после исполнения всех обязательств по договору об оказании клиринговых услуг и обязательств, допущенных к клирингу.

Торговые и клиринговые банковские счета могут открываться как в рублях, так и в иностранной валюте.

Введение Законом о клиринге новых видов счетов, используемых для расчетов по итогам организованных торгов, является основанием для внесения соответствующих изменений в Правила бухгалтерского учета в кредитных организациях.

ОБЩИЕ ПРАВИЛА ПРОВЕДЕНИЯ РАСЧЕТОВ В СЕКТОРАХ ОРЦБ

В настоящее время НРД осуществляет денежные расчеты в трех секторах ОРЦБ:

- 1) рынок государственных ценных бумаг;
- 2) рынок негосударственных ценных бумаг (фондовый рынок);
- 3) рынок стандартных контрактов (срочный рынок).

Технология расчетов на всех перечисленных секторах установлена Положением № 32-П, Правилами бухгалтерского учета в кредитных организациях и внутренними документами клиринговой организации.

Следует отметить, что каждому банковскому счету, открываемому в НРД на балансовом счете № 30401, может соответствовать только один торговый счет, открытый для учета средств в соответствующем секторе ОРЦБ на балансовом счете № 30403.

В секторах ОРЦБ расчеты осуществляются в соответствии с правилами проведения операций в секторах ОРЦБ, состоящими из разделов, описывающих особенности проведения расчетов в отдельных секторах ОРЦБ. Указанные правила являются неотъемлемой частью соглашения о проведении расчетных операций в секторах ОРЦБ к договору банковского счета, регулирующего взаимоотношения НРД и клиента — участника расчетов при проведении денежных расчетов по операциям клиента на ОРЦБ.

Как уже отмечалось ранее, технология расчетов, установленная нормативными актами Банка России, является единой для всех секторов ОРЦБ, вместе с тем для каждого сектора ОРЦБ существуют особенности, которые будут рассмотрены далее.

Упрощенная схема проведения расчетов в секторах ОРЦБ представлена на рис. 6.4.

Схема включает в себя как операции по депонированию средств для участия в торгах, т.е. перечисление клиентами НРД средств с банковских счетов на торговые счета, так и возврат средств с торговых счетов на банковские счета клиентов, проведение расчетов по торгам с использованием клирингового счета, открываемого на балансовом счете № 30407, а также операции по удержанию в пользу клиринговой организации комиссионного вознаграждения, которые осуществляются путем списания средств с торговых счетов при проведении расчетов.

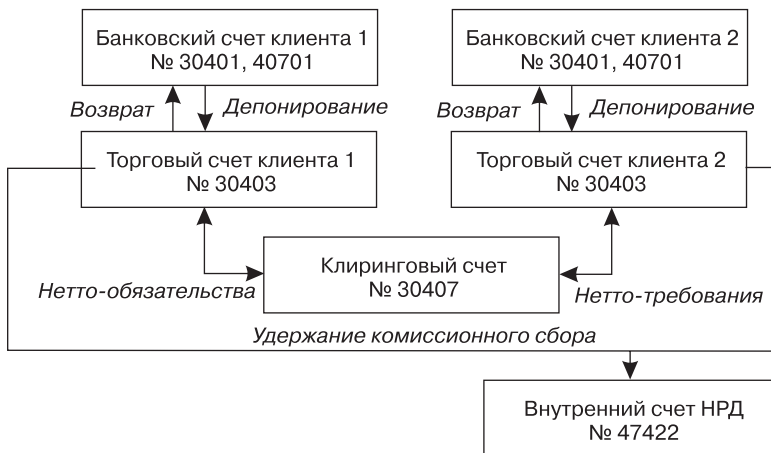


Рис. 6.4. Упрощенная схема организации расчетов в секторах ОРЦБ и используемые балансовые счета

6.9. ОСОБЕННОСТИ ПРОВЕДЕНИЯ РАСЧЕТОВ НА РЫНКЕ ГОСУДАРСТВЕННЫХ ЦЕННЫХ БУМАГ

Расчеты по операциям клиентов с государственными ценными бумагами осуществляются в секторе «ГКО, ОФЗ-ПК».

НРД в соответствии с нормативными актами Банка России, регулирующими порядок обслуживания и обращения государственных ценных бумаг на ОРЦБ, а также документами ММВБ для учета денежных средств клиентов по этим операциям открывает следующие виды торговых счетов.

Для клиента, не являющегося кредитной организацией, открываются:

- отдельный *торговый счет* для обеспечения расчетов по операциям с собственными средствами клиента;
- отдельный *торговый счет* для обеспечения расчетов по операциям со средствами инвесторов клиента как резидентов РФ, так и нерезидентов РФ. Указанный тип счета в соответствии с законодательством является специальным брокерским счетом;
- отдельный *торговый счет* для обеспечения расчетов по операциям с денежными средствами, переданными клиенту в доверительное управление.

Для клиента, являющегося кредитной организацией, открываются:

- *торговый счет* для обеспечения расчетов по операциям с собственными средствами и средствами инвесторов клиента, как резидентов РФ, так и нерезидентов РФ;
- отдельный *торговый счет* для обеспечения расчетов по операциям с денежными средствами, переданными клиенту в доверительное управление.

Расчетное обслуживание клиента в секторе «ГКО, ОФЗ-ПК» осуществляется в соответствии с регламентом работы НРД в секторе «ГКО, ОФЗ-ПК», положения которого коррелируют положениям регламента взаимодействия между НРД (как РЦ ОРЦБ) и ММВБ (являющейся клиринговой организацией на рынке государственных ценных бумаг), установленному договором, предметом которого является организация денежных расчетов на секторе ОРЦБ «ГКО, ОФЗ-ПК».

Указанными регламентами установлена следующая последовательность действий по информационному обмену между клиентом, РЦ ОРЦБ (НРД) и клиринговой организацией (ММВБ) в течение всего торгового дня и осуществлению операций по счетам в секторе «ГКО, ОФЗ-ПК».

1. Для участия в торгах клиент осуществляет перечисление денежных средств с банковского счета, открытого в НРД, на один из торговых счетов, что на рис. 6.4 обозначено как депонирование денежных средств.

2. Денежные средства клиента, перечисленные на торговые счета, блокируются НРД до момента получения от ММВБ отдельного документа под названием «Распоряжение на разблокировку денежных средств на торговых счетах».

3. После проведения блокировки денежных средств клиент тем не менее имеет возможность изменить свою денежную позицию на торгах в динамическом режиме. Для этих целей, т.е. для изменения суммы денежных средств, депонированных на торговых счетах, клиент должен предоставить в НРД платежное поручение на списание или зачисление денежных средств с банковского счета или на банковский счет, что будет означать намерение клиента увеличить или уменьшить сумму денежных средств, находящихся на торговом счете, соответственно.

4. Исполнение платежных поручений клиента для увеличения суммы денежных средств на торговых счетах осуществляется НРД в пределах остатка денежных средств на банковском счете клиента. При этом денежные средства, дополнительно перечисленные клиентом на торговые счета, также блокируются до получения от ММВБ упомянутого выше документа «Распоряжение на разблокировку денежных средств на торговых счетах».

Исполнение (отказ в исполнении) платежных поручений клиента для уменьшения суммы денежных средств, находящихся на торговых счетах, осуществляется НРД только на основании полученного от ММВБ документа «Распоряжение на разблокировку (неразблокировку) части денежных средств на счете № 30403» в пределах средств, переведенных на торговые счета.

При этом списание денежных средств с торговых счетов производится НРД на соответствующие им банковские счета клиента.

Проведение расчетов по итогам торгов, а также по уплате комиссионного вознаграждения осуществляется НРД на основании документа, получаемого от ММВБ и называемого «Сведения о нетто-обязательствах (нетто-требованиях) дилеров, обслуживающихся в Расчетном центре, и о комиссионном вознаграждении ММВБ по итогам вторичных торгов и (или) аукциона по облигациям». Указанный документ поступает в НРД после каждой клиринговой сессии на рынке

государственных ценных бумаг во время, установленное регламентом взаимодействия между ММВБ и НРД.

5. После проведения расчетов на основании получаемого от ММВБ «Распоряжения на разблокировку денежных средств на торговых счетах» со стороны НРД производится такая разблокировка.

6. После проведения расчетов по итогам окончательной клиринговой сессии после разблокировки денежных средств на торговых счетах НРД перечисляет денежные средства с торговых счетов на соответствующие им банковские счета клиента.

Схема организации и проведения расчетов по итогам торгов на рынке государственных ценных бумаг представлена на рис. 6.5.

Функции расчетных центров ОРЦБ выполняют в настоящее время две расчетных НКО: НРД и Петербургский расчетный центр (ЗАО ПРЦ). Для завершения расчетов необходимо осуществить урегулирование денежных позиций, сложившихся между указанными расчетными центрами ОРЦБ, результатом чего должно стать итоговое нулевое сальдо, что будет гарантировать правильность проведения расчетов. При этом урегулирование денежных позиций между указанными расчетными организациями осуществляется с помощью системы банковских электронных срочных платежей (БЭСП) Банка России. Расчеты производятся только после согласования с ММВБ как клиринговой организацией денежных нетто-позиций, сложившихся по итогам клиринга.

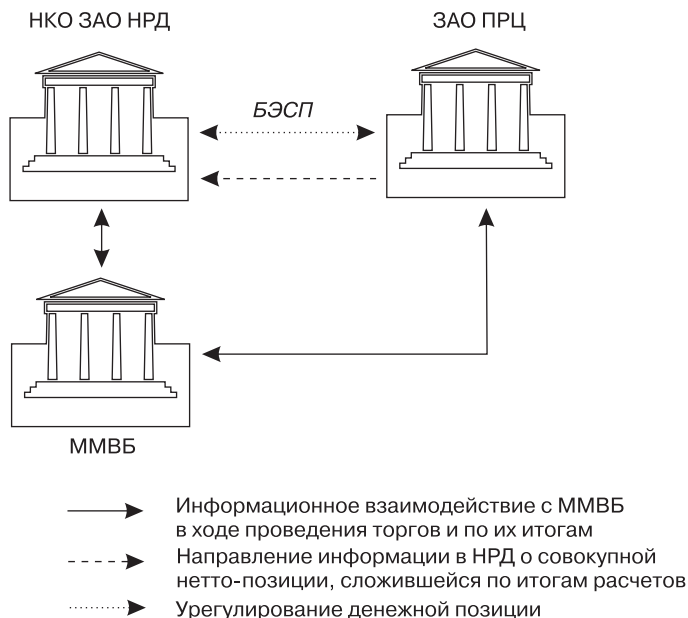


Рис. 6.5. Организация расчетов на рынке государственных ценных бумаг

6.10. ОРГАНИЗАЦИЯ РАСЧЕТОВ НА ФОНДОВОМ РЫНКЕ

Принципиальная схема проведения расчетов по итогам торгов на рынке негосударственных ценных бумаг (или фондовом рынке) представлена на рис. 6.6. Функции клиринговой организации на этом рынке выполняет НКЦ.

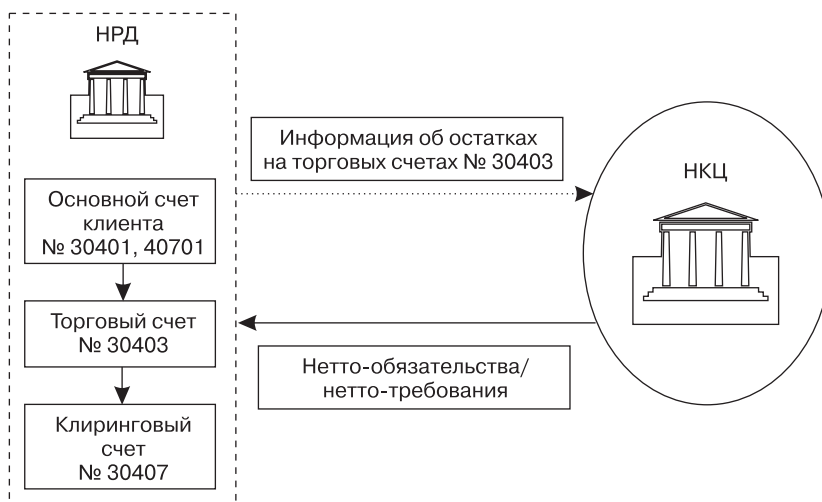


Рис. 6.6. Принципиальная схема проведения расчетов по итогам торгов на фондовом рынке

Для осуществления расчетов по операциям клиента в секторе «Фондовый рынок ММВБ», являющегося участником клиринга, НРД в случаях, предусмотренных Правилами осуществления клиринговой деятельности ЗАО «АКБ „Национальный клиринговый центр“» на рынке ценных бумаг, открывает следующие торговые счета.

Для клиента, не являющегося кредитной организацией, открываются:

- отдельный *торговый счет* для обеспечения расчетов по операциям с собственными средствами клиента;
- отдельный *торговый счет* для обеспечения расчетов по операциям со средствами инвесторов клиента как резидентов РФ, так и нерезидентов РФ (специальный брокерский счет);
- отдельный *торговый счет* для обеспечения расчетов по операциям с денежными средствами, переданными клиенту в доверительное управление.

Для клиента, являющегося кредитной организацией:

- *торговый счет* для обеспечения расчетов по операциям с собственными средствами и средствами инвесторов клиента, как резидентов РФ, так и нерезидентов РФ;

- отдельный *торговый счет* для обеспечения расчетов по операциям с денежными средствами, переданными клиенту в доверительное управление.

Для осуществления расчетов по операциям клиента в секторе «Фондовый рынок ММВБ», являющегося клиентом участника клиринга, НРД в случаях, предусмотренных Правилами осуществления клиринговой деятельности ЗАО «АКБ „Национальный клиринговый центр“» на рынке ценных бумаг, открывает торговый счет для обеспечения расчетов по операциям с собственными средствами клиента.

Термин «клиент участника клиринга» был введен для группы клиентов, не имеющих лицензии профессионального участника на рынке ценных бумаг, в целях предоставления им возможности участия в торгах на фондовом рынке через своего брокера, имеющего такую лицензию. Самостоятельно управляя своим денежным счетом в НРД, клиент участника клиринга получает возможность снизить свои риски потери ликвидности.

Расчетное обслуживание клиента в секторе «Фондовый рынок ММВБ» осуществляется в соответствии с регламентом работы НРД в секторе «Фондовый рынок ММВБ».

Расчеты в секторе «Фондовый рынок ММВБ» осуществляются в следующем порядке.

1. Для обеспечения расчетов по операциям в секторе «Фондовый рынок ММВБ» клиент осуществляет перечисление денежных средств с банковского счета на торговый счет.

2. Денежные средства клиента, перечисленные на торговые счета, блокируются НРД до получения от НКЦ отдельного документа — «Распоряжение на разблокировку денежных средств на счетах».

3. Для изменения суммы денежных средств, находящихся на торговых счетах (после блокировки таких денежных средств), клиент представляет в НРД платежное поручение на списание (зачисление) денежных средств с банковского счета (на банковский счет).

4. Исполнение платежных поручений клиента для увеличения суммы денежных средств на торговых счетах осуществляется НРД в пределах остатка денежных средств на банковском счете. На период торгов дополнительно перечисленные денежные средства клиента на торговых счетах также блокируются до получения от НКЦ документа «Распоряжение на разблокировку денежных средств на счетах».

Исполнение платежных поручений клиента (отказ в исполнении) для уменьшения суммы денежных средств, находящихся на торговых счетах, осуществляется НРД на основании полученного от НКЦ документа «Уведомление о возможности (невозможности) уменьшения суммы денежных средств» в пределах средств, переведенных на торговые счета.

При этом списание денежных средств с торговых счетов производится НРД на соответствующие им банковские счета клиента.

5. Проведение расчетов (отмена расчетов) по операциям клиента в секторе «Фондовый рынок ММВБ», в том числе по уплате комиссионного вознаграждения и возмещения, выполняется НРД на основании следующих документов, получаемых от НКЦ: «Сводной ведомости по обязательствам и требованиям по денежным средствам», «Ведомости по уплате комиссионного вознаграждения», «Ведомости по уплате возмещения», «Распоряжения на отмену сводной ведомости по обязательствам и требованиям по денежным средствам», «Распоряжения на отмену ведомости по уплате комиссионного вознаграждения», «Распоряжения на отмену ведомости по уплате возмещения».

6. Разблокировка денежных средств на торговых счетах осуществляется НРД на основании документа «Распоряжение на разблокировку денежных средств на счетах», получаемого от НКЦ.

7. После разблокировки денежных средств на торговых счетах НРД перечисляет денежные средства с торговых счетов на соответствующие им банковские счета клиента.

Следует отметить, что расчеты по итогам торгов в секторе «Фондовый рынок ММВБ» проходят как в рублях, так и в иностранной валюте. В последнем случае НКО ЗАО НРД обеспечивает расчеты по итогам торгов еврооблигациями РФ.

В отличие от расчетов на рынке государственных ценных бумаг, где существует несколько промежуточных клиринговых сессий, на фондовом рынке в настоящее время расчеты по итогам клиринга проводятся один раз в день, за исключением, конечно, расчетов по так называемому простому клирингу, проводимому между двумя участниками торгов. Такие расчеты могут осуществляться по мере их необходимости несколько раз за день.

ОСОБЕННОСТИ ПРОВЕДЕНИЯ РАСЧЕТОВ НА СРОЧНОМ РЫНКЕ

При проведении операций в секторе «Срочный рынок ММВБ» функции клиринговой организации выполняет ММВБ.

Для осуществления расчетов в секторе «Срочный рынок ММВБ» по операциям клиента, имеющего категорию клирингового обслуживания «клиринговый участник» на срочном рынке ЗАО «Фондовая биржа ММВБ» и (или) в секции срочного рынка (стандартные контракты) ММВБ в случаях, предусмотренных Правилами осуществления клиринговой деятельности ЗАО «Московская межбанковская валютная биржа» на срочном рынке, НРД открывает следующие торговые счета, отражаемые на балансовых счетах № 30403, и счета поставки, отражаемые на балансовом счете № 30405.

Для клиента, не являющегося кредитной организацией, открываются:

- отдельный торговый счет для обеспечения расчетов по операциям с собственными средствами клиента;
- отдельный торговый счет для обеспечения расчетов по операциям со средствами инвесторов клиента как резидентов РФ, так и нерезидентов РФ (специальный брокерский счет);

- отдельный торговый счет для обеспечения расчетов по операциям с денежными средствами, переданными клиенту в доверительное управление;
- счет поставки для обеспечения расчетов, в том числе по поставке базового актива.

Для клиента, являющегося кредитной организацией:

- отдельный торговый счет для обеспечения расчетов по операциям с собственными средствами и средствами инвесторов клиента, как резидентов РФ, так и нерезидентов РФ;
- отдельный торговый счет для обеспечения расчетов по операциям с денежными средствами, переданными клиенту в доверительное управление;
- счет поставки для обеспечения расчетов, в том числе по поставке базового актива.

Для осуществления расчетов в секторе «Срочный рынок ММВБ» по операциям клиента, имеющего категорию членства «клиринговый член» в секции стандартных контрактов на зерновые, зернобобовые и технические культуры ЗАО «Национальная товарная биржа» в случаях, предусмотренных Правилами осуществления клиринговой деятельности ЗАО ММВБ по сделкам, совершаемым в секции стандартных контрактов на зерновые, зернобобовые и технические культуры ЗАО «Национальная товарная биржа», НРД открывает следующие торговые счета, отражаемые на балансовых счетах № 30403, и счета поставки, отражаемые на балансовых счетах № 30405 сектора «Срочный рынок ММВБ» :

Для клиента, не являющегося кредитной организацией, открываются:

- отдельный торговый счет для обеспечения расчетов по операциям с собственными средствами клиента;
- отдельный торговый счет для обеспечения расчетов по операциям со средствами инвесторов клиента, как резидентов РФ, так и нерезидентов РФ (специальный брокерский счет);
- отдельный счет поставки для обеспечения расчетов по поставке базового актива, осуществляемых за счет собственных средств клиента;
- отдельный счет поставки для обеспечения расчетов по поставке базового актива, осуществляемых за счет средств инвесторов клиента.

Для клиента, являющегося кредитной организацией, открываются:

- торговый счет для обеспечения расчетов по операциям с собственными средствами и средствами инвесторов клиента, как резидентов РФ, так и нерезидентов РФ;
- счет поставки для обеспечения расчетов по поставке базового актива, осуществляемых как за счет собственных средств, так и за счет средств инвесторов клиента.

Расчетное обслуживание клиента в секторе «Срочный рынок ММВБ» осуществляется в соответствии с регламентом работы НРД в секторе «Срочный рынок ММВБ».

Операции по торговому счету и (или) счету поставки в секторе «Срочный рынок ММВБ» осуществляются в следующем порядке:

1. Для обеспечения расчетов по операциям в Секторе «Срочный рынок ММВБ» клиент осуществляет перечисление денежных средств с банковского счета на торговый счет и (или) счет поставки.

2. На период расчетов денежные средства клиента на торговом счете и (или) счете поставки блокируются НРД на основании следующих документов, получаемых от ММВБ: «Распоряжения на блокировку денежных средств, зарезервированных на Торговых счетах» и «Распоряжения на блокировку денежных средств, зарезервированных на счетах поставки и торговых счетах».

3. Проведение расчетов по операциям клиента в секторе «Срочный рынок ММВБ», в том числе по операциям связанным с поставкой базового актива, выполняется НРД на основании следующих документов, получаемых от ММВБ: «Распоряжение на проведение расчетов по результатам торгов и гарантийному обеспечению» и «Распоряжение на проведение расчетов по поставке».

4. Разблокировка денежных средств клиента на торговом счете и (или) счете поставки осуществляется НРД по окончании расчетов на основании получаемых от ММВБ документов: «Распоряжение на разблокировку денежных средств на торговых счетах» и «Распоряжение на разблокировку денежных средств на счетах поставки и торговых счетах».

5. После разблокировки денежных средств на торговом счете НРД перечисляет денежные средства с торгового счета на банковский счет клиента.

6. Для внесения дополнительных денежных средств в состав депозитной маржи (т.е. специального возвратного вноса, производимого каждым клиентом для обеспечения исполнения его обязательств в случаях и порядке, определяемых Правилами осуществления клиринговой деятельности на срочном рынке ММВБ) в ходе торговой сессии клиент предоставляет в НРД платежные поручения на перечисление денежных средств с банковского счета на торговый счет.

Исполнение платежных поручений клиента по внесению дополнительных денежных средств в состав депозитной маржи в ходе торговой сессии осуществляются НРД в пределах остатка денежных средств на банковском счете клиента.

7. Операции по торговому счету в случае внесения клиентом дополнительных денежных средств в состав депозитной маржи в ходе торговой сессии выполняются НРД на основании документа «Распоряжение на проведение расчетов по результатам торгов и гарантийному обеспечению», получаемого от ММВБ.

8. Для уменьшения суммы денежных средств на торговом счете клиент предоставляет в НРД платежное поручение на зачисление денежных средств на банковский счет.

Исполнение платежных поручений клиента для уменьшения суммы денежных средств на торговом счете осуществляется НРД в пределах остатка денежных средств на торговом счете.

9. Перед закрытием операционного дня остаток денежных средств клиента, находящийся на торговом счете, перечисляется НРД на банковский счет клиента.

10. Перечисление денежных средств клиента со счета поставки по операциям, не связанным с поставкой базового актива, осуществляется НРД на основании документа «Распоряжение на проведение расчетов по поставке», получаемого от ММВБ.

Следует отметить следующие основные принципиальные особенности проведения расчетов на срочном рынке (рис. 6.7).

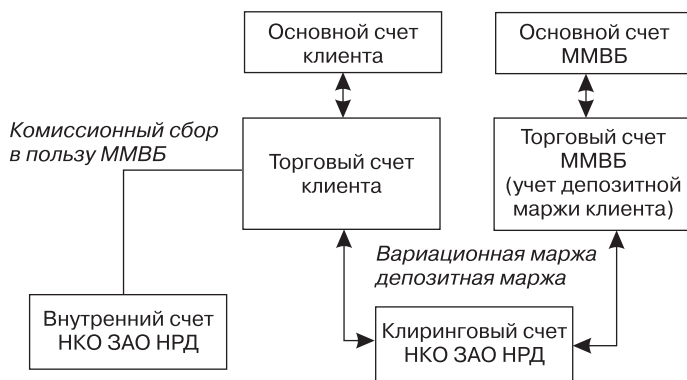


Рис. 6.7. Принципиальная схема проведения расчетов на срочном рынке

Денежные средства, перечисленные клиентом в составе вариационной маржи¹ и не использованные в расчетах за текущий день, перечисляются на торговый счет, открытый для ММВБ, и далее соответственно на банковский счет ММВБ, где эти средства хранятся до начала следующего операционного дня, а затем перечисляются НРД на торговый счет ММВБ, чтобы быть задействованными при проведении расчетов следующим операционным днем.

Кроме этого хотелось бы отметить, что денежные средства могут вноситься клиентами в состав депозитной маржи не только в рублях, но и в иностранной валюте. Отражение операций по счетам в этом случае будет также соответствовать схеме ОРЦБ, но технология расчетов будет отличаться тем, что окончательные расчеты в случае невыполнения участником торгов своих обязательств будут осуществляться в рублях после реализации депозитной маржи в иностранной валюте за рубли, что наглядно показано на рис. 6.8.

¹ Вариационная маржа — сумма, размер которой зависит от изменения цен на базовый актив или значений базового актива, уплачиваемая (получаемая) сторонами по сделкам в связи с изменением денежного обязательства по одной позиции в результате ее корректировки по рынку в соответствии с изменением расчетной (котировальной) цены, рассчитанная по единым правилам для срочных контрактов, заключенных на условиях одной спецификации, в соответствии с порядком, установленным спецификацией.

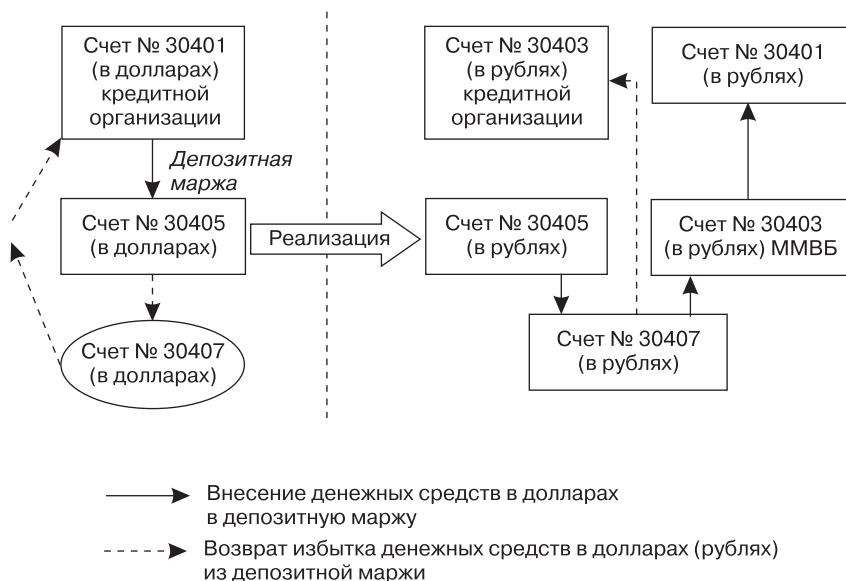


Рис. 6.8. Внесение средств в иностранной валюте в качестве депозитной маржи на срочном рынке и ее реализация в случае невыполнения участником своих обязательств в рублях

6.11. УЧАСТИЕ РЦ ОРЦБ В ПРОВЕДЕНИИ РАСЧЕТОВ НА ВАЛЮТНОМ РЫНКЕ

Следует отметить, что схема проведения расчетов на валютном рынке ММВБ принципиально отличается от ранее описанных схем проведения расчетов по торгам на других рынках ММВБ, на которых используется единая технология расчетов на ОРЦБ с учетом особенностей, характерных для расчетов по итогам торгов на отдельных рынках. Функции клиринговой и расчетной организации на валютном рынке ММВБ выполняет НКЦ, входящий в группу ММВБ и имеющий банковскую и клиринговую лицензии. При проведении расчетов на валютном рынке НРД отведена роль кредитной организации, выполняющей для НКЦ в соответствии с отдельным договором роль банка — корреспондента по расчетам в рублях (рис. 6.9).

Технология проведения расчетов при этом достаточно проста. Вначале участники торгов осуществляют предварительное депонирование денежных средств в рублях и иностранных валютах, направляя определенные суммы денежных средств в рублях на корреспондентский счет НКЦ, открытый в НРД, и в иностранных валютах на корреспондентские счета НКЦ, открытые в иностранных банках. Поскольку предварительное депонирование средств для участия в торгах

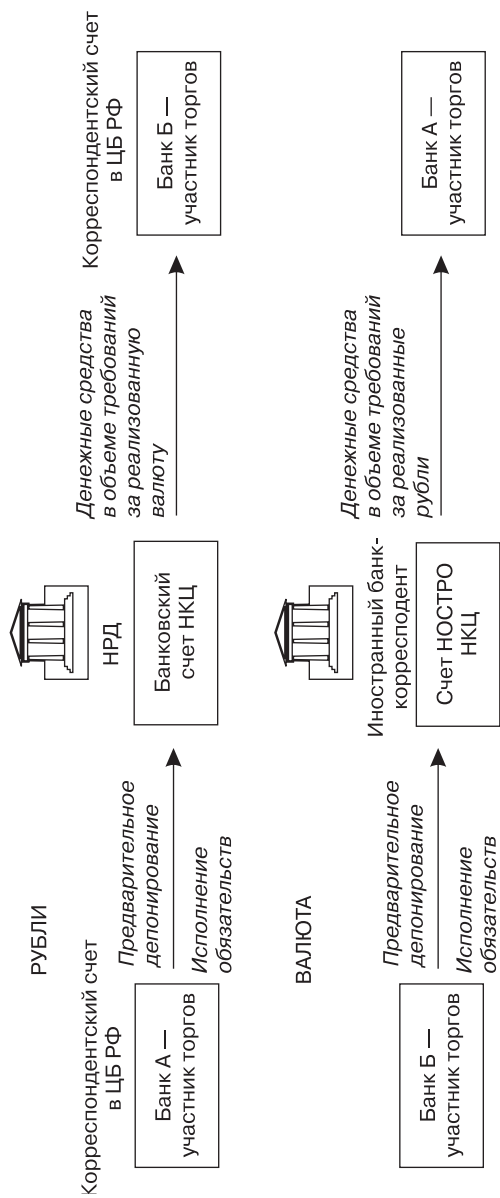


Рис. 6.9. Схема проведения расчетов на валютном рынке ММВБ

осуществляется не в полном объеме, по окончании торгов участники перечисляют на вышеуказанные корреспондентские счета денежные средства для полного исполнения своих обязательств по итогам торгов на валютном рынке. В завершение этого производятся клиринг, расчеты и перечисление денежных средств по итогам торгов и клиринга на счета участников торгов в соответствии с указанными ими банковскими реквизитами.

6.12. ПЕРСПЕКТИВЫ ПОСТРОЕНИЯ ПЛАТЕЖНОЙ СИСТЕМЫ, ПРЕДУСМАТРИВАЮЩЕЙ ПЕРЕВОДЫ ДЕНЕЖНЫХ СРЕДСТВ ПО СДЕЛКАМ, СОВЕРШЕННЫМ НА ОРГАНИЗОВАННЫХ ТОРГАХ

Следует отметить, что Закон о НПС предусматривает создание платежной системы, в рамках которой осуществляются переводы денежных средств по сделкам, совершенным на организованных торгах, что следует из следующих положений указанного Закона:

1) участниками платежной системы (в том числе прямыми участниками) могут стать профессиональные участники рынка ценных бумаг, а также юридические лица, являющиеся участниками организованных торгов и (или) участниками клиринга в соответствии с Законом о клиринге, о чем указывалось ранее;

2) платежные системы, в рамках которых осуществляются переводы денежных средств по сделкам, совершенным на организованных торгах, относятся к категории системно значимых платежных систем (п. 3 ч. 1 ст. 22);

3) при осуществлении надзора и наблюдения за платежными системами, в которых осуществляются переводы денежных средств в целях расчета по сделкам с ценными бумагами и (или) сделкам, совершенным на организованных торгах, Банк России взаимодействует с ФСФР России, в том числе по вопросам участия в платежных системах профессиональных участников рынка ценных бумаг, юридических лиц — участников организованных торгов и (или) участников клиринга, а также по вопросам взаимодействия операторов услуг платежной инфраструктуры с клиринговыми организациями, центральными контрагентами и (или) депозитариями (ч. 2 ст. 36);

4) особенности правил платежных систем, в рамках которых осуществляются переводы денежных средств по сделкам, совершенным на организованных торгах, устанавливаются Банком России по согласованию с уполномоченным федеральным органом исполнительной власти (ч. 10 ст. 20);

5) в платежных системах, в рамках которых осуществляются переводы денежных средств по сделкам, совершенным на организованных торгах, услуги платежного клиринга могут оказываться в рамках клиринговой услуги клиринговой организацией, осуществляющей свою деятельность в соответствии с Зако-

ном о клиринге (ч. 2 ст. 18 Закона о НПС). Расчетный центр платежной системы в этом случае может исполнять распоряжения участников платежной системы, поступившие от клиринговой организации, осуществляющей свою деятельность в соответствии с Законом о клиринге (ч. 5 ст. 19 Закона о НПС).

По нашему мнению, платежная система, предусматривающая осуществление переводов денежных средств по сделкам, совершенным на организованных торгах, может быть построена на существующей в настоящее время системе расчетов ОРЦБ, в которой НРД фактически выполняет функции оператора платежной системы, а также функции операторов платежной инфраструктуры (операционного центра и расчетного центра).

ГЛАВА 7

ЭЛЕКТРОННЫЕ ДЕНЬГИ И МОБИЛЬНЫЕ ПЛАТЕЖИ – МЕТОДОЛОГИЯ ИСПОЛЬЗОВАНИЯ ВНУТРИ КОММЕРЧЕСКОГО БАНКА

В соответствии с нормами Закона о НПС кредитные организации, работающие до момента его вступления в силу и (или) собирающиеся работать с электронными денежными средствами, обязаны уведомить об этом Банк России. Это уведомление о начале деятельности по осуществлению перевода электронных денежных средств подается в Банк России не позднее десяти рабочих дней со дня первого увеличения остатка электронных денежных средств¹, и в нем должны быть указаны (см. п. 4 ст. 12 Закона):

- 1) наименование и место нахождения оператора электронных денежных средств, а также номер его лицензии на осуществление банковских операций;
- 2) вид (виды) предоставляемых клиентам электронных средств платежа;
- 3) наименования организаций, привлеченных оператором электронных денежных средств для оказания операционных услуг и (или) услуг платежного клиринга (при их привлечении).

Также в соответствии с п. 5 ст. 12 Закона оператор электронных денежных средств (далее — оператор) обязан установить правила осуществления перевода электронных денежных средств (далее — Правила), включая:

- 1) порядок деятельности оператора электронных денежных средств, связанной с переводом электронных денежных средств;
- 2) порядок предоставления клиентам электронных средств платежа и осуществления перевода электронных денежных средств с их использованием;
- 3) порядок деятельности оператора электронных денежных средств при привлечении банковских платежных агентов, организаций, оказывающих операционные услуги и (или) услуги платежного клиринга;

¹ Остаток электронных денежных средств (остаток) — размер обязательств банка перед клиентом в сумме денежных средств, предоставленных клиентом, в том числе в результате возврата оператором связи (оператор) аванса за услуги связи.

- 4) порядок обеспечения бесперебойности осуществления перевода электронных денежных средств;
- 5) порядок рассмотрения претензий оператором электронных денежных средств, включая процедуры оперативного взаимодействия с клиентами;
- 6) порядок обмена информацией при осуществлении переводов электронных денежных средств.

Кроме того, оператор электронных денежных средств обязан обеспечить бесперебойность осуществления перевода электронных денежных средств в соответствии с требованиями, установленными нормативными актами Банка России (п. 6 ст. 12 Закона).

В данной главе будут даны рекомендации по методике создания правил осуществления перевода электронных денежных средств¹ (описанные методологические наработки в большей степени касаются перевода электронных денежных средств при увеличении остатков электронных денежных средств физических лиц — клиентов оператора связи).

7.1. ПОРЯДОК ДЕЯТЕЛЬНОСТИ ОПЕРАТОРА ЭЛЕКТРОННЫХ ДЕНЕЖНЫХ СРЕДСТВ

Оператор электронных денежных средств оказывает клиентам услуги по переводу электронных денежных средств в соответствии с Законом, нормативными актами Банка России и заключаемыми договорами. Предоставление клиентом денежных средств банку в целях осуществления перевода электронных денежных средств осуществляется после заключения с ним договора и сообщения реквизитов электронного средства платежа (далее — ЭСП ЭДС).

Оператор электронных денежных средств учитывает предоставленные клиентом денежные средства путем формирования записи в информационной системе, обеспечивающей учет остатков и изменение их размера при осуществлении переводов или возвратов остатков и отражающей размер остатка в сумме предоставленных клиентом денежных средств.

Оператор электронных денежных средств не предоставляет клиенту денежные средства для увеличения остатка, не осуществляет начисление процентов на остаток ЭДС или выплату любого вознаграждения клиенту.

Перевод электронных денежных средств осуществляется путем одновременного принятия оператором распоряжения с незамедлительным выполнением необходимых процедур контроля: уменьшения остатка клиента и увеличения остатка получателя средств на сумму перевода ЭДС. После исполнения распоряжения клиента об осуществлении перевода ЭДС оператор направляет клиенту

¹ Рекомендации составлены на основании опыта разработки подобных документов Центром исследования платежных систем и расчетов (ЦИПСИР — www.paysyscenter.ru) для нескольких банков — операторов электронных денежных средств.

подтверждение об исполнении его распоряжения. Указанные положения применяются также в случае возврата остатка оператором ЭДС.

До заключения договора с клиентом оператор электронных денежных средств предоставляет ему на интернет-сайте (банка, оператора) следующую информацию:

- 1) о наименовании и месте нахождения оператора ЭДС, а также о номере его лицензии на осуществление банковских операций;
- 2) об условиях использования ЭСП ЭДС;
- 3) о способах и местах осуществления перевода ЭДС;
- 4) о способах и местах предоставления денежных средств клиентом;
- 5) о размере и порядке взимания оператором ЭДС вознаграждения с физического лица в случае взимания вознаграждения;
- 6) о способах подачи претензий и порядке их рассмотрения, включая информацию для связи с оператором ЭДС.

7.2. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ КЛИЕНТАМ ЭСП И ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА

Предоставление клиентам ЭСП ЭДС и осуществление переводов электронных денежных средств с их использованием осуществляется на основании договора между клиентом и банком, который определяет взаимные обязательства клиента и банка, а также порядок взаимодействия и расчетов при осуществлении перевода электронных денежных средств клиента. Условия договора доводятся до клиента путем размещения на сайте банка.

Заключение договора осуществляется клиентами путем направления в банк SMS-сообщения или USSD-запроса¹ о заключении договора посредством услуг связи, предоставляемых оператором. Договор считается заключенным с момента подтверждения банком клиенту получения указанного выше SMS-сообщения или USSD-запроса. С этого момента клиент принимает все условия договора в целом.

Заключая договор, клиент дает согласие на обработку своих персональных данных, включая передачу сведений о нем третьим лицам с целью исполнения договора. Банк осуществляет обработку персональных данных клиента в течение всего срока действия договора, а также в течение трех лет с даты расторжения договора, по истечении которых персональные данные уничтожаются, за исключением случаев предусмотренных законодательством Российской Федерации.

Перечень видов SMS-сообщений и USSD-запросов устанавливается банком в договорах с клиентом и с оператором. Все SMS-сообщения и USSD-запросы фиксируются и хранятся в электронном виде в ИС оператора и могут использо-

¹ USSD-запрос — текстовое сообщение, формируемое клиентом и направляемое адресату (банку или оператору) в электронном виде посредством сервиса USSD в сетях GSM, предоставляемых оператором.

ваться в качестве доказательств при решении споров, в том числе в судебном порядке. Изменения в договор и тарифы вносятся банком в одностороннем порядке.

ПОРЯДОК УВЕЛИЧЕНИЯ ОСТАТКА И ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ЭДС

Увеличение остатка осуществляется в соответствии с условиями договора и тарифами банка. Увеличение остатка осуществляется на основании распоряжения, передаваемого клиентом банку через оператора посредством направления SMS-сообщений и USSD-запросов об увеличении остатка.

Для увеличения остатка клиент должен обеспечить наличие у оператора денежных средств в сумме, достаточной для уплаты комиссии за увеличение остатка в соответствии с тарифами банка. При недостаточности денежных средств у оператора увеличение остатка банком не осуществляется. Увеличение остатка за счет средств у оператора осуществляется клиентом в порядке, установленном договорами между оператором и клиентом, между банком и клиентом.

С момента увеличения остатка банк становится обязанным перед клиентом в размере суммы распоряжения.

В случае проведения оператором электронных денежных средств идентификации клиента — физического лица использование электронного средства платежа осуществляется клиентом — физическим лицом при условии, что остаток электронных денежных средств в любой момент не превышает 100 тыс. руб. либо сумму в иностранной валюте, эквивалентную 100 тыс. руб. по официальному курсу Банка России. Указанное электронное средство платежа является персонифицированным. Допускается превышение указанной суммы вследствие изменения официального курса иностранной валюты, устанавливаемого Банком России.

В случае непроведения оператором ЭДС идентификации клиента — физического лица использование электронного средства платежа осуществляется клиентом — физическим лицом при условии, что остаток электронных денежных средств в любой момент не превышает 15 тыс. руб. Указанное электронное средство платежа является неперсонифицированным. Общая сумма переводимых электронных денежных средств с использованием одного неперсонифицированного электронного средства платежа не может превышать 40 тыс. руб. в течение календарного месяца.

ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ЭДС

Для осуществления перевода клиент направляет в банк распоряжение посредством услуг связи, предоставляемых оператором, в виде SMS-сообщения или USSD-запроса о переводе. Все направляемые в банк SMS-сообщения или USSD-запросы о переводе должны осуществляться с номера клиента.

При приеме к исполнению распоряжения банк удостоверяется в праве клиента использовать ЭСП ЭДС, распоряжаться остатком, проверяет реквизиты

перевода, достаточность остатка для исполнения распоряжения. В случае если право клиента использовать ЭСП ЭДС, распоряжаться остатком не удостоверено, при несоответствии реквизитов перевода установленным требованиям, а также при недостаточности остатка банк не принимает распоряжение к исполнению и незамедлительно направляет клиенту об этом уведомление посредством услуг связи, предоставляемых оператором, в виде SMS-сообщения или USSD-запроса на номер клиента.

Прием распоряжения клиента к исполнению и его исполнение подтверждаются банком незамедлительно посредством услуг связи, предоставляемых оператором, в виде SMS-сообщения или USSD-запроса на номер клиента.

Порядок деятельности оператора ЭДС при привлечении банковских платежных агентов

Взаимоотношения между банком и банковским платежным агентом регулируются ст. 14 Закона о НПС, договором между банком и банковским платежным агентом и правилами.

В соответствии с договором, заключенным между банком и банковским платежным агентом, последний вправе оказывать банку следующие услуги:

- идентификация физического лица в целях осуществления перевода и возврата остатков;
- прием наличных денежных средств в валюте Российской Федерации в целях увеличения остатков через кассу или с применением платежных терминалов и банкоматов банковского платежного агента;
- выдача наличных денежных средств в валюте Российской Федерации в целях возврата остатков через кассу или с применением платежных терминалов и банкоматов банковского платежного агента.

Банк ведет реестр банковских платежных агентов с указанием адресов всех мест осуществления деятельности банковских платежных агентов.

Банк контролирует деятельность банковского платежного агента в соответствии с законодательством и договором и может осуществлять выборочные регулярные выезды на места присутствия банковского платежного агента с проверкой на соблюдение требований условий привлечения банковского платежного агента.

Порядок деятельности оператора ЭДС при привлечении оператора для оказания операционных услуг

Оператор оказывает услуги по обеспечению информационно-технологического взаимодействия в ИС оператора, включая оказание услуг по сбору, обработке и рассылке информации по операциям с использованием ЭСП ЭДС. При обращении клиента в банк с целью возможности осуществления операций по получению наличных денежных средств — получения наличных денежных средств

с использованием ЭСП ЭДС банк осуществляет прием соответствующего заявления клиента и иных документов (надлежащим образом заверенных копий документов) с целью идентификации клиента в соответствии с требованиями Закона о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (далее — Закон № 115-ФЗ). При принятии клиентом условий договора оператор осуществляет контроль за наличием и при необходимости сбор актуальных сведений (в том числе фамилии, имени, отчества, даты и места рождения, гражданства, реквизитов документа, удостоверяющего личность (серия и номер документа, дата выдачи документа, наименование органа, выдавшего документ и код подразделения (если имеется)); идентификационного номера налогоплательщика (если имеется), номеров контактных телефонов, адреса места жительства (регистрации) или места пребывания, адреса электронной почты), а для лиц, не являющихся гражданами Российской Федерации, дополнительно данных миграционной карты, дата начала срока пребывания и дата окончания срока пребывания в Российской Федерации) и данных документа, подтверждающего право на пребывание (проживание) в Российской Федерации (название, серия (если имеется), номер, дата начала срока действия права пребывания (проживания), дата окончания срока действия права пребывания (проживания)). Сведения о клиенте, указанные в настоящем пункте, должны быть документально подтверждены, и оператор должен располагать такими подтверждающими документами (копии документа, удостоверяющего личность клиента, миграционной карты и документа, подтверждающего право на пребывание (проживание) в Российской Федерации), необходимых банку для идентификации клиентов в соответствии с требованиями законодательства и нормативных актов Банка России.

Банк осуществляет выпуск и обслуживание ЭСП ЭДС. Пополнение остатка осуществляется оператором по распоряжению клиентов на возврат авансового платежа за услуги связи.

Подтверждение, данное оператором, порождает обязательство оператора перечислить банку денежные средства для пополнения остатка в сумме операции (включая сумму комиссии, установленной тарифами банка), указанной в таком подтверждении.

ОБЕСПЕЧЕНИЕ БЕСПЕРЕБОЙНОСТИ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ЭСП

При обеспечении бесперебойности осуществления переводов электронных денежных средств банк ориентируется на действующие рекомендации Банка России, стандарты ISO и успешные практики управления услугами и сервисами.

Меры, предпринимаемые банком, направлены на исключение и (или) снижение последствий, вызванных непредвиденными ситуациями при осуществлении переводов ЭДС, связанными с проявлением (по отдельности или в сочетаниях):

- выхода из строя технических средств;
- сбоя в работе автоматизированных информационных систем;

- нарушения коммунальной инфраструктуры;
- перебоев в энергоснабжении;
- непредвиденного дефицита ликвидности;
- отказа кредитных организаций-корреспондентов и (или) организаций-контрагентов, в том числе поставщиков услуг (провайдеров) кредитной организации, от исполнения своих обязательств.

Для обеспечения бесперебойности перевода электронных денежных средств оператор ЭДС банк осуществляет:

- мониторинг за переводом ЭДС, осуществляемым путем уменьшения остатка ЭДС плательщика и увеличения остатка ЭДС получателя средств на сумму перевода ЭДС; мониторинг распространяется на процессы, непосредственно находящиеся в зоне ответственности банка. При этом в случае выявления перебоев служба мониторинга своевременно информирует ответственные подразделения банка для оперативного устранения нарушений;
- меры, направленные на недопущение возникновения нарушений функционирования средств материально-технического обеспечения перевода ЭДС, а в случае возникновения указанных нарушений осуществляет меры по их устранению; предпринимаются ответственными подразделениями банка;
- анализ причин произошедших нарушений функционирования средств материально-технического обеспечения перевода ЭДС (например, сбой в работе программно-технического комплекса, обеспечивающего учет информации об остатках ЭДС и их перевод) и выработку мер по их дальнейшему устранению (минимизации);
- обеспечение отказоустойчивости средств материально-технического обеспечения перевода ЭДС, их тестирование в целях выявления недостатков функционирования, а в случае выявления указанных недостатков принимает меры по их устранению.

Для организации деятельности, связанной с обеспечением бесперебойности осуществления перевода ЭДС, оператором по переводу электронных денежных средств также применяются внутренние документы банка, отражающие следующие вопросы:

- способы мониторинга за переводом ЭДС;
- перечень возможных причин нарушения функционирования средств материально-технического обеспечения перевода ЭДС, влекущих прекращение осуществления перевода ЭДС или его ненадлежащее осуществление;
- план действий в случае произошедших нарушений функционирования средств материально-технического обеспечения перевода ЭДС;
- регламентные работы по обеспечению функционирования средств материально-технического обеспечения перевода ЭДС, резервному копированию информации об осуществленном переводе ЭДС, а также об остатках ЭДС.

7.3. ПРОТИВОДЕЙСТВИЕ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА

ОБЩИЕ УСЛОВИЯ ИДЕНТИФИКАЦИИ

В соответствии с подп. 1.1 п. 1 ст. 7 Закона № 115-ФЗ при приеме от клиента — физического лица денежных средств в сумме, не превышающей 15 тыс. руб., либо сумме в иностранной валюте, эквивалентной 15 тыс. руб., если у работников кредитной организации (банковского платежного агента) не возникает подозрений, что данная операция осуществляется в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, идентификация клиента — физического лица не проводится.

Сведения, требуемые в соответствии со ст. 7 Закона и Положением Банка России от 19 августа 2004 г. № 262-П «Об идентификации кредитными организациями клиентов и выгодоприобретателей в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», при проведении упрощенной идентификации фиксируются в автоматизированной банковской системе способами, определенными регламентными документами банка.

Признаки необычных операций и поведения клиентов, которые могут привести к подозрению, что операция осуществляется в целях легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма, описаны далее. В случае если у сотрудника кредитной организации (банковского платежного агента) возникает подозрение, производится идентификация клиента.

УПРОЩЕННЫЙ ПОРЯДОК ИДЕНТИФИКАЦИИ КЛИЕНТОВ ПРИ СОВЕРШЕНИИ ОТДЕЛЬНЫХ ВИДОВ БАНКОВСКИХ ОПЕРАЦИЙ И СДЕЛОК

Идентификация физического лица проводится на основании документа, удостоверяющего личность, который не содержит всех сведений, требуемых в соответствии с законодательством (упрощенная идентификация физического лица) при осуществлении:

- переводов денежных средств по поручению физических лиц без открытия банковских счетов;
- банковских операций и иных сделок с наличной иностранной валютой и валютой Российской Федерации, чеками (в том числе дорожными чеками), номинальная стоимость которых указана в иностранной валюте, предусмотренных нормативным документом Банка России, регламентирующим порядок осуществления уполномоченными банками отдельных видов банковских операций и иных сделок с наличной иностранной валютой и валю-

той Российской Федерации, чеками (в том числе дорожными), номинальная стоимость которых указана в иностранной валюте, с участием физических лиц.

Упрощенная идентификация физического лица предполагает установление фамилии, имени и (если иное не вытекает из закона или национального обычая) отчества, реквизитов документа, удостоверяющего личность клиента, и проводится только в случае, если наличествуют в совокупности (одновременно) следующие условия:

- операция не подлежит обязательному контролю и фамилия, имя и (если иное не вытекает из закона или национального обычая) отчество, а также другие имеющиеся у Банка сведения о физическом лице полностью не совпадают с информацией, содержащейся в перечне организаций и лиц, признанных в установленном порядке причастными к экстремистской или террористической деятельности;
- в отношении клиента, выгодоприобретателя или операции у банка не возникают подозрения в том, что они связаны с легализацией (отмыванием) доходов, полученных преступным путем, или финансированием терроризма;
- операция не имеет запутанного или необычного характера, свидетельствующего об отсутствии очевидного экономического смысла или очевидной законной цели, и совершение указанной операции не дает оснований полагать, что целью ее осуществления является уклонение от процедур обязательного контроля, предусмотренных Законом о НПС.

Упрощенная идентификация физического лица при осуществлении банковских операций и иных сделок может также проводиться на основании водительского удостоверения.

Проверка достоверности и действительности предъявленного документа

При проверке паспорта сотрудник кредитной организации (банковского платежного агента) обязан извлечь паспорт из обложки, если таковая имеется и осмотреть паспорт на предмет повреждения, наличия посторонних проколов (отверстий), деформации в виде валика сгиба обложки, прошивочных ниток на сгибе листов. Следует обращать внимание, не имеется ли в паспорте чернильных и жировых пятен, расплывов красочного изображения на страницах, помарок, порванных и склеенных страниц, обведенных слов или их фрагментов, так как они могут быть нанесены умышленно с целью маскировки подделки. Также необходимо сравнить совпадение серии и номера паспорта на страницах.

Особое внимание следует уделить осмотру фотографии и месту ее вклейки. При проверке паспорта необходимо убедиться в правильности его оформления, принадлежности его предъявителю, а также в подлинности документа, не истек ли срок действия паспорта либо своевременно ли произведена его замена. В случае

нарушения указанных правил паспорт считается недействительным (например, истек срок действия паспорта или пропущена дата его обязательной замены).

Сотрудник кредитной организации (банковского платежного агента) запрашивает у клиента, его представителя, а клиент, его представитель представляют всю информацию и документы, необходимые для идентификации клиента, его представителя. К сведениям, запрашиваемым у клиента, его представителя, относятся:

- фамилия, имя и отчество (если иное не вытекает из закона или национального обычая);
- дата и место рождения;
- гражданство;
- реквизиты документа, удостоверяющего личность: серия и номер документа, дата выдачи документа, наименование органа, выдавшего документ, и код подразделения (если имеется);
- данные миграционной карты: номер карты, дата начала срока пребывания и дата окончания срока пребывания; данные документа, подтверждающего право иностранного гражданина или лица без гражданства на пребывание (проживание) в Российской Федерации: серия (если имеется) и номер документа, дата начала срока действия права пребывания (проживания), дата окончания срока действия права пребывания (проживания);
- адрес места жительства (регистрации) или места пребывания.

Все документы, позволяющие идентифицировать клиента, его представителя, должны быть действительными на дату их предъявления.

Предъявляемые клиентами документы должны быть проверены на предмет их подлинности. Все документы должны представляться клиентом, его представителем в подлиннике или в копии, заверенной в надлежащем порядке. В случае представления клиентами копий документов работники банка вправе потребовать представления подлинников документов для ознакомления.

Сотрудник кредитной организации (банковский платежный агент) вправе не проводить повторную идентификацию клиента, его представителя, если такой клиент, его представитель уже были идентифицированы банком и к сведениям об этом клиенте, его представителе обеспечен оперативный доступ в постоянном режиме.

Банковский платежный агент обязан провести повторную идентификацию клиента, его представителя, если у банка возникают сомнения в достоверности сведений, полученных ранее в результате реализации данной процедуры.

Иностранные публичные должностные лица

Иностранные публичные должностные лица — это лица, на которых возложены или были возложены в прошлом важные государственные функции в конкретном государстве.

При принятии клиента на обслуживание банк и банковский платежный агент обязаны:

1) принимать обоснованные и доступные в сложившихся обстоятельствах меры по выявлению среди физических лиц, находящихся или принимаемых на обслуживание, иностранных публичных должностных лиц (ИПДЛ); при выявлении ИПДЛ банк может использовать любые из следующих источников информации:

- документы и сведения, полученные при идентификации клиента: в частности, информация о статусе клиента может быть получена из документа, удостоверяющего личность (например, дипломатический паспорт), из документа, подтверждающего право пребывания на территории Российской Федерации (например, въездная виза). Если информация о занимаемой должности указана самим клиентом, у него могут быть получены документы, подтверждающие его статус «иностранное публичное должностное лицо»,
- официальные списки (если подобные списки будут разработаны и доведены до кредитных организаций Росфинмониторингом, Министерством иностранных дел РФ, Банком России или иным государственным органом Российской Федерации, другой коммерческой или некоммерческой организацией, которой будет предоставлено право на создание таких списков),
- коммерческие списки, разрабатываемые третьими лицами,
- общедоступные источники информации (СМИ, Интернет и иные);

2) банковский платежный агент может заключить договор с физическим лицом, являющимся иностранным публичным должностным лицом или его супругой, супругом и близким родственником или действующим от имени указанных лиц, только на основании положительного решения председателя правления банка, принятого по результатам рассмотрения заявления соответствующих физических лиц (направленных в адрес банка в письменной форме);

3) в случае вынесения решения о принятии на обслуживание указанных лиц банк вправе запрашивать у таких лиц информацию, а также принимать меры по определению источников происхождения денежных средств указанных лиц в соответствии с Законом о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) на регулярной основе обновлять имеющуюся информацию о находящихся на обслуживании ИПДЛ;

5) выяснить при заключении договора, действительно ли физическое лицо является иностранным публичным должностным лицом. На основании полученных от клиента данных сотрудником банковского платежного агента делается отметка в информационной системе Банка об отнесении клиента в ИПДЛ.

Процедура проверки клиентов по перечню экстремистов

При принятии клиента на обслуживание сотрудник, ответственный за идентификацию клиента, проверяет данные потенциального клиента, полученные

в результате его идентификации, на совпадение с данными физических лиц, указанных в перечне экстремистов.

Помимо информации о потенциальном клиенте банк также проверяет по перечню лиц, связанных с клиентом, а именно:

- представителей клиента (лиц, имеющих полномочия совершать операции или сделки от имени клиента);
- лиц, в интересах которых клиент осуществляет операции с денежными средствами.

В случае выявления совпадения идентификационных данных клиента или связанного с ним лица с данными лиц, указанных в перечне экстремистов, данная операция подлежит приостановлению.

Порядок приостановления операций

После принятия от клиента распоряжения о проведении операции и установлении того обстоятельства, что хотя бы одной из сторон является физическое лицо, в отношении которого имеются полученные в установленном в соответствии с п. 2 ст. 6 Закона 115-ФЗ порядке сведения об их участии в террористической деятельности (перечень экстремистов), физическое, действующее от имени или по указанию таких организации или лица, банк принимает решение о приостановлении операции на два рабочих дня с даты, когда распоряжение клиента должно быть выполнено.

Если начало течения срока приостановления операции приходится на выходной или праздничный день, срок приостановления операции исчисляется с первого рабочего дня, следующего за соответствующим выходным или праздничным днем.

Если начало течения срока приостановления операции приходится на выходной или праздничный день и этот день является рабочим днем для банка, срок приостановления операции исчисляется с указанного выходного или праздничного дня.

При выявлении полного совпадения имеющихся сведений о клиенте или его контрагенте с информацией, содержащейся в перечне экстремистов, сотруднику банковского платежного агента, выявившему данное совпадение, необходимо проинформировать банк о факте обнаружения лица, причастного к экстремистской деятельности.

При получении информации от банковского сотрудника (платежного агента) банк обязан:

- сообщить в органы внутренних дел о факте обнаружения лица, причастного к экстремистской деятельности;
- незамедлительно (в день выявления) приостановить операции данного клиента.

Решение о приостановлении операции принимается руководителем банка или уполномоченным им лицом.

Приостановление операции по перечислению денежных средств физического лица с предоплаченной карты после приема от клиента наличных денежных средств и документа, предоставляемого клиентом для осуществления перевода, банк учитывает денежные средства по приостановленной операции на балансе банка, без перечисления денежных средств по назначению.

На следующий рабочий день после истечения срока приостановления операции банк осуществляет приостановленную операцию. В случае получения банком в течение срока приостановления операции постановления уполномоченного органа о приостановлении данной операции на дополнительный срок операция приостанавливается дополнительно на срок, указанный в постановлении уполномоченного органа.

По факту приостановления операции не позднее следующего рабочего дня банк направляет информацию о ней в уполномоченный орган.

Признаки необычных операций и поведения клиента

Признаки необычных операций:

- операции, не имеющие очевидного экономического смысла — когда клиенты намеренно пренебрегают экономической выгодой, преследуя иные неясные цели. Например, денежный перевод осуществляется в рамках одного города, или ситуация, когда клиент получает перевод и сразу же отправляет всю сумму другому человеку;
- частые операции отправления денежных переводов на крупные суммы. Такие переводы зачастую связаны с предпринимательскими целями, что запрещено законодательством;
- частые операции получения денежных переводов, особенно из разных стран от разных отправителей;
- операции, не соответствующие заявленным целям.

Признаки необычного поведения клиента:

- нервничает, суетится или агрессивен;
- настаивает на как можно более быстром проведении операции;
- неохотно предъявляет документ, удостоверяющий личность, или его документ кажется необычным, фальшивым или содержащим ложные сведения;
- предлагает деньги или подарки в обмен на то, чтобы сведения о его операциях не были документально зафиксированы или не направлялось сообщение в уполномоченный орган;
- хочет помешать тому, чтобы сведения о его операции (операциях) были документально зафиксированы, а также тому, чтобы сообщение о его операциях было направлено в уполномоченный орган;
- постоянный клиент, регулярно посылавший деньги домой один раз в месяц, вдруг начинает отправлять большие суммы каждую неделю другим лицам;
- (группа клиентов) регулярно совершает операции на сумму немного ниже ограничения, установленного законодательством или договором с банком;

- один или несколько клиентов часто отправляют переводы одному и тому же или связанным между собой получателям;
- представляет различные документы, удостоверяющие личность, каждый раз, когда он получает перевод;
- часто получает денежные переводы, в каждом из которых его имя указано по-разному или допущены несущественные ошибки;
- получает несколько небольших переводов в один день или в течение нескольких последовательных дней, а затем отправляет один или несколько переводов другому лицу;
- получает частые переводы или большие суммы от разных лиц, проживающих за рубежом, без разумного объяснения такого поведения;
- получает перевод и немедленно отправляет всю его сумму третьему лицу без разумного объяснения;
- несколько вошедших вместе в отделение клиентов пытаются сделать вид, что не знакомы друг с другом;
- постоянно совершает операции сразу после открытия, перед закрытием или во время пиковых часов нагрузки на отделение;
- совершает несколько операций в течение одного дня из одного отделения, но при этом старается обращаться каждый раз к разным сотрудникам;
- проявляет необычное любопытство в отношении внутренних систем контроля и действующих процедур по ПОД/ФТ;
- пытается установить неформальные взаимоотношения с сотрудниками.

Аутентификация клиента при его обращении

В отделении банка аутентификация клиента производится на основании документа, удостоверяющего личность. Клиент считается аутентифицированным в случае соответствия реквизитов документа, удостоверяющего личность, информации, содержащейся в базе данных банка.

В телефонном центре аутентификация клиента производится:

- по паролю. Клиент считается аутентифицированным в случае соответствия пароля, введенного при обращении в телефонный центр, паролю, присвоенному клиенту и содержащемуся в базе данных банка;
- фамилии, имени, отчеству клиента;
- дате рождения клиента;
- номеру и серии паспорта Российской Федерации клиента;
- номеру телефона сотовой связи клиента (при звонке с указанного номера и при наличии у банка технической возможности определить номер телефона сотовой связи клиента в системе банка).

Аутентификация клиента в телефонном центре может осуществляться одним или несколькими способами. Информация, полученная в результате аутентификации, должна соответствовать информации, содержащейся в базе данных банка.

В интернет-банке — аутентификация по логину. Клиент считается аутентифицированным в случае соответствия логина, введенного клиентом при подключении к интернет-банку, логину, присвоенному клиенту и содержащемуся в информационной базе банка.

ПОРЯДОК ПРЕДЪЯВЛЕНИЯ ПРЕТЕНЗИЙ

Порядок предъявления претензий клиентами

В случае несвоевременного или некачественного оказания банком услуг, в том числе при возникновении споров, связанных с расходными операциями, клиент вправе обратиться в банк с претензией.

Срок подачи клиентом претензии с момента совершения операции, вызвавшей такую претензию, указывается в соответствующем договоре, заключенном между банком и клиентом. Клиент вправе отозвать претензию.

Банк рассматривает претензию, а также обеспечивает клиенту возможность получать информацию о результатах ее рассмотрения, в том числе в письменной форме, по требованию клиента в срок, установленный договором, но не более 30 (тридцати) дней со дня получения претензии, а также не более 60 (шестидесяти) дней со дня получения претензии в случае использования ЭСП ЭДС для осуществления трансграничного перевода.

В случае непредъявления банку письменной претензии через отделение или претензии через телефонный центр по операциям в указанный в договоре срок, последние считаются подтвержденными и в дальнейшем обжалованию не подлежат.

Претензия может быть предъявлена в банк в письменном виде через отделение банка или зарегистрирована при устном обращении клиента в телефонный центр.

Порядок рассмотрения претензий банком

Решение по претензии принимаются только в случае аутентификации клиента.

При обращении с претензией клиента, использующего неперсонифицированное ЭСП ЭДС, сотрудник банка обязан с согласия клиента снять и заверить копию с документа, удостоверяющего личность физического лица. Копии документов, удостоверяющих личность, после регистрации претензии с указанием номера претензии хранятся в банке.

Полученная претензия клиента регистрируется в электронном виде с присвоением номера претензии, а также сведений о претензионной операции и ее реквизитах. Порядок регистрации претензии определяется внутренними документами банка. На любом этапе работы с претензией ей присваивается статус, отражающий этап рассмотрения.

Зарегистрированная претензия передается на обработку в ответственное подразделение банка для подготовки решения по претензии. Подразделение банка, ответственное за рассмотрение и исполнение претензий, вправе запрашивать любую информацию (сведения) и (или) документы, необходимые для подготовки ответов в установленные сроки, во всех подразделениях банка.

По факту принятия банком решения об удовлетворении претензии производится возмещение денежных средств (при необходимости).

Информирование клиентов о результатах рассмотрения претензий (писем) по претензиям происходит одним из следующих способов:

- путем исходящего обзвона сотрудниками телефонного центра;
- путем направления SMS-сообщения на мобильный телефон, указанный клиентом при оформлении претензии;
- путем направления письменного ответа с уведомлением о вручении по почте в случае, если претензия поступила в банк на юридический адрес банка через канцелярию (письменно через отделение);
- путем самостоятельного обращения клиента в телефонный центр или отделение.

Оперативное взаимодействие с клиентами осуществляет ответственный сотрудник банка по телефонам или электронным адресам, указанным клиентом при заключении соответствующего договора.

ГЛАВА 8

БЕЗОПАСНОСТЬ И НАДЕЖНОСТЬ ФУНКЦИОНИРОВАНИЯ ПЛАТЕЖНЫХ ТЕХНОЛОГИЙ

8.1. ПАРАДИГМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НПС. ОБЪЕКТЫ, ПРЕДМЕТЫ, ОТНОШЕНИЯ

Под национальной платежной системой в соответствии с определением, данным в Законе о НПС, понимается:

«совокупность операторов по переводу денежных средств (включая операторов электронных денежных средств), банковских платежных агентов (субагентов), платежных агентов, организаций Федеральной почтовой связи при оказании ими платежных услуг в соответствии с законодательством Российской Федерации, операторов платежных систем, операторов услуг платежной инфраструктуры (субъекты национальной платежной системы)».

Как объект защиты НПС представляет собой достаточно сложную и неоднородную структуру, объединенную положениями закона в некую виртуальную единую систему, которой по своей природе она не является. Целый ряд различных категорий субъектов этой виртуальной системы уже давно присутствует на отечественном финансовом рынке и рынке услуг, осуществляя свою деятельность, руководствуясь соответствующим федеральным законодательством: «О банках и банковской деятельности»; «О деятельности по приему платежей физических лиц, осуществляемой платежными агентами»; «О банке развития»; «О почтовой связи»; «О связи»¹ (прием платежей операторами мобильной связи).

¹ Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

В этой связи положения Закона о НПС призваны в какой-то мере установить основополагающие системные категории, подлежащие учету и единообразной реализации участниками этого рынка, а также подлежащие контролю единым государственным регулятором. В подобных условиях крайне затруднительно сформулировать работоспособные, имеющие практическое воплощение, основополагающие понятия для того или иного среза деятельности применительно к НПС, но потребность в этом есть.

Руководствуясь основными правилами терминологии и соответствующими нормами, можно дать следующее определение понятию «информационная безопасность национальной платежной системы» (произошло от определения «информационная безопасность» и содержания задач (целей деятельности) объекта защиты):

«Состояние защищенности целей деятельности НПС от угроз в информационной сфере, обеспечивающее реализацию задач эффективности и бесперебойности, а также адекватности национальной платежной системы потребностям экономики, банковского сектора и финансового рынка Российской Федерации».

Приведенное определение понятия «информационная безопасность национальной платежной системы» достаточно абстрактно, но на этом уровне иным оно быть и не может. Назначением его может быть определение общего контекста и направления работ всех субъектов системы, деятельность которых будет иметь уже более конкретное наполнение с учетом его роли в системе и более явное отражение в практике.

Для аналогичных целей в 2000 г. в документе «Доктрина информационной безопасности Российской Федерации» было приведено определение понятия «информационная безопасность Российской Федерации» :

«Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства».

Совершенно очевидно, что из данного понятия не проистекает система практических задач, но далее в контексте документа формулируется перечень специфических угроз и мер по противодействию.

Ровно для этих же целей было приведено определение понятия «информационная безопасность национальной платежной системы». На практике основу системы мер противодействия угрозам в информационной сфере целям НПС будут составлять решения как в узком — техническом, так и в более широком — технологическом и общеметодологическом плане. При этом основным «исполнительным механизмом» системы мер противодействия угрозам в информационной сфере целям ПНС будет организация-участник (пользователь услугами НПС), которая по этим же причинам будет являться и основным объектом контроля и надзора регулятора НПС. Физические лица — пользователи услугами системы будут

прямо или косвенно охвачены решениями и технологиями организаций-участников (пользователей услугами НПС).

В этой связи далее будет сделан акцент на деятельности и решении на уровне организации — основной категории участников НПС.

ОСНОВНЫЕ ПОНЯТИЯ И ИСТОЧНИКИ ПАРАДИГМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ НПС В СОВРЕМЕННЫХ УСЛОВИЯХ

Проблема информационной безопасности (ИБ) вообще, а для рассматриваемой предметной области в частности может трактоваться как в узком, так и широком смысле.

В узком смысле она известна с момента зарождения социума и процессов целенаправленной деятельности. Именно тогда возникают фундаментальные сущности, не имеющие прямого материального выражения, — системы отношений «субъект — объект», «субъект — субъект»; представление цели деятельности как состояния будущего в виде абстрактных информационных моделей; планов по реализации этих целей в виде тех же моделей.

В широком, современном смысле проблема ИБ в России насчитывает не более двадцати лет, так как для ее возникновения необходимо было наличие ряда основных условий, актуализировавшихся в этот период.

1. Должно было сформироваться сообщество независимых субъектов, действующих (реализующих свой бизнес, свои цели) самостоятельно, на свой риск.

2. Это сообщество должно было быть достаточно многочисленным для того, чтобы между субъектами сложились условия возникновения конфликта интересов, связанных с различными аспектами реализации целей их деятельности¹.

3. Должен был сформироваться и войти в практику новый тип объектов — информационный объект, а также система отношений «субъект — информационный объект», «множество субъектов — информационный объект».

4. Должна была сложиться развитая «операционная среда», обеспечивающая накопление, хранение, обработку, обмен информации между заинтересованными и (или) причастными сторонами.

В силу того, что все эти условия должны выполняться одновременно для развитых стран мирового сообщества, проблема ИБ также является новой, пик глобальной информатизации в мировом обществе начался в 1980-е гг.

В жизни проблема ИБ проявляется в виде противоборства вовлеченных сторон (субъектов), в котором каждый стремится поставить каждого под свой контроль, неявно управлять его деятельностью в своих интересах на основе манипуляций с потребляемой ими информацией (информационной сферой) либо как минимум нанести ущерб целям его деятельности, воздействуя на информационную

¹ Должно выполняться условие $|C| \gg |Ц|$, т.е. мощность множества субъектов $|C|$ существенно больше мощности множества всех возможных целей $|Ц|$.

сферу противника. Практически всегда конечной целью противников является получение материального (ресурсного) выигрыша, хотя все основные действия противоборства и осуществляются на «информационном поле». Указанный тезис иллюстрирует рис. 8.1.

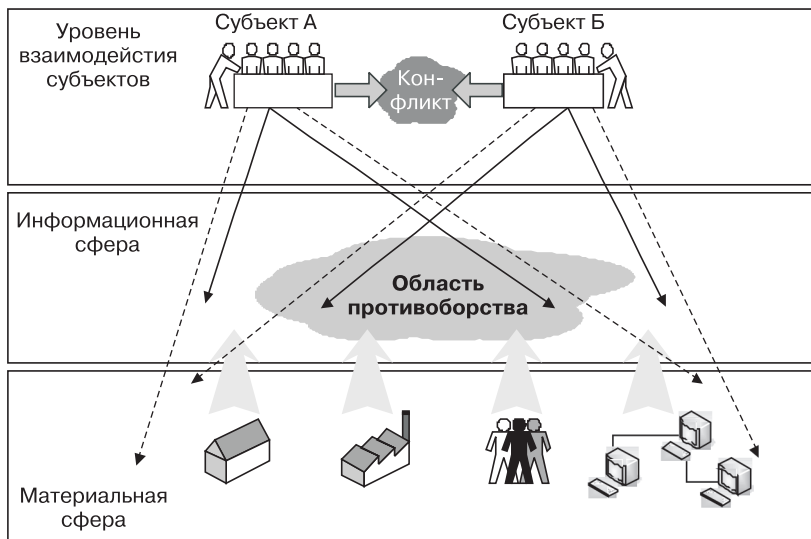


Рис. 8.1. Противоборство субъектов в информационной сфере

Как видно из рис. 8.1, материальная сфера включает совокупность различных объектов, представляющих для субъектов определенную ценность и рассматриваемых ими в качестве ресурсов. Между субъектами возникает конфликт, который выражается в стремлении каждого из них завладеть ресурсами, необходимыми для реализации собственной цели, а также в стремлении воздействовать на реализацию целей противников путем дезорганизации их деятельности и получения контроля над необходимыми им ресурсами. Проблема информационной безопасности в данном конфликте возникает тогда, когда материальные объекты имеют отражение в информационной сфере и большинство субъектов взаимодействует не с реальными ресурсами, а с их информационным отображением. Итогом противоборства в информационной сфере будет либо материальное преимущество одного из субъектов перед другим, либо создание ситуации, при которой один из субъектов не сможет достичь целей своей деятельности совсем или достичь целей с наименьшими возможными издержками.

В качестве примера подобного противоборства можно привести следующую ситуацию. Организация использует критически важный для ее деятельности ресурс, к примеру, оборудование, необходимое для осуществления деятельности. Данное оборудование отражено на балансе организации в виде соответствующих

записей бухгалтерского учета, которые представляют собой информационное отображение материального объекта. Противник (конкурирующая организация) организует некоторые манипуляции с указанными записями, в результате которых информационное отображение ресурса будет уничтожено или существенно искажено, что создаст неопределенность относительно наличия прав организации на распоряжение оборудованием и его использование. Продолжением описываемого информационного нападения могут быть следующие действия различных субъектов, использующие созданную неопределенность и наносящие деятельности организации ущерб:

- действия банка, в залоге у которого находится оборудование;
- предъявление прав на оборудование третьим лицом;
- невозможность проведения разрешительных и контролирующих действий органами власти из-за отсутствия правоустанавливающих документов.

При этом используется фундаментальное свойство процесса и результата (реализовавшейся цели) целенаправленной деятельности, а именно их зависимости от качества и количества потребленной информации. Действительно, цель как состояние будущего есть не что иное, как прогноз, и он не может быть точным. Процесс принятия различных решений, использующий для этих целей информацию о состоянии задействованных активов и среды, наоборот, основывается на информационных образах активов и среды, которые уже неактуальны («устаревшие»). Непрерывная актуализация информационных образов активов и среды для системы принятия решений «поглотит» весь полезный ресурс процесса, а для некоторых видов активов (ресурсов) она вообще нереализуема.

Таким образом, процесс целенаправленной деятельности сам по себе без всякого противоборства и злоумышленников содержит риск успешной реализации цели, и это риск информационной природы. Теоретически, как предельный случай, существует и безрисковая реализация таких процессов, но для этого необходимо наличие бесконечно большого ресурса и бесконечное время реализации процесса. Понятно, что на практике такой процесс нереалистичен.

В связи с этим процесс целенаправленной деятельности всегда содержит естественно (natural) присущий ему риск достижения заявленной цели. Этот риск часто называют стохастической составляющей процесса. Очевидно, что все происходящие события в пределах этого риска будут восприниматься как правдоподобные, независимо от их настоящей природы. Это и создает возможность манипулирования информацией для противоборствующей стороны и поясняет одну из «типовых злоумышленных стратегий». Она состоит в том, чтобы, навязывая ложные представления о состоянии процесса и реализуемой цели, «увести» от нее как можно «дальше» и создать ресурсные сложности, чтобы вывести процесс за интервал времени, когда истинная (задуманная, заявленная) цель еще актуальна, и потратить на ее реализацию как можно больше ресурса. То есть понизить его эффективность до уровня, когда естественное «воспроизводство» процесса окажется невозможным, что и приведет в конечном счете к уничтоже-

нию противоборствующей стороны и последующему захвату его ресурсов и инфраструктуры.

НПС позиционируется как совокупность очень большого количества относительно независимых субъектов-участников (операторов по переводу, банковских и небанковских платежных агентов (субагентов), организаций Федеральной почтовой связи при оказании ими платежных услуг, операторов платежных систем, операторов услуг платежной инфраструктуры), предоставляющих пользователям достаточно ограниченный набор сервисов (услуг) и функционирующих фактически на рыночных принципах. Такое устройство изначально предполагает сильный конфликт интересов между участниками и, как следствие, высокий уровень противоборства сторон.

Информационный в основном характер их деятельности автоматически переводит противоборство в информационную сферу. Для этого у них имеются все необходимые предпосылки и возможности, а также глубокие знания предметной области.

Исходя из этого теперь можно сформулировать в общем виде стратегию поведения и критерий успеха для противоборствующих сторон. Очевидно, что необходимо хорошо прогнозировать не только собственные цели и состояние «своих» процессов, но также и «чужих», тех, которые состоят в «конфликте интересов» с собственными целями и процессами; своевременно и адекватно реагировать на выявляемые изменения; уметь «извлекать пользу» из этих изменений.

Соответственно можно сформулировать и критерии успеха в противоборстве. Действительно, успех будет достигнут той стороной, которая лучше реализует заявленные цели деятельности, т.е. лучше (точнее и на больший интервал времени) прогнозирует, лучше (быстрее и адекватнее) приспосабливается (адаптируется) к сложившимся условиям.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СУБЪЕКТА НПС

Основой (платформой) для лучшего соответствия требованиям критериев успеха деятельности организации — субъекта национальной платежной системы является, с одной стороны, способность к извлечению (добыванию) полезной информации, ее систематизации, накоплению и анализу, а с другой — способность к ее обобщению, формированию сильного знания. Именно знания и являются основанием для уверенности в качестве и точности реализации целей деятельности. Но необходимы не просто знания, а знания, обобщенные до уровня хорошей (лучшей) практики (*good practice*), пригодные к прямому их использованию в конкретных условиях (рис. 8.2).

Естественно, возникает вопрос о том, какие знания нужны, в какой сфере, в рамках каких моделей и процедур они могут быть получены, каким образом они должны использоваться. Ответы на эти вопросы фактически и определяют основной состав и содержание деятельности службы информационной безопасности организации.

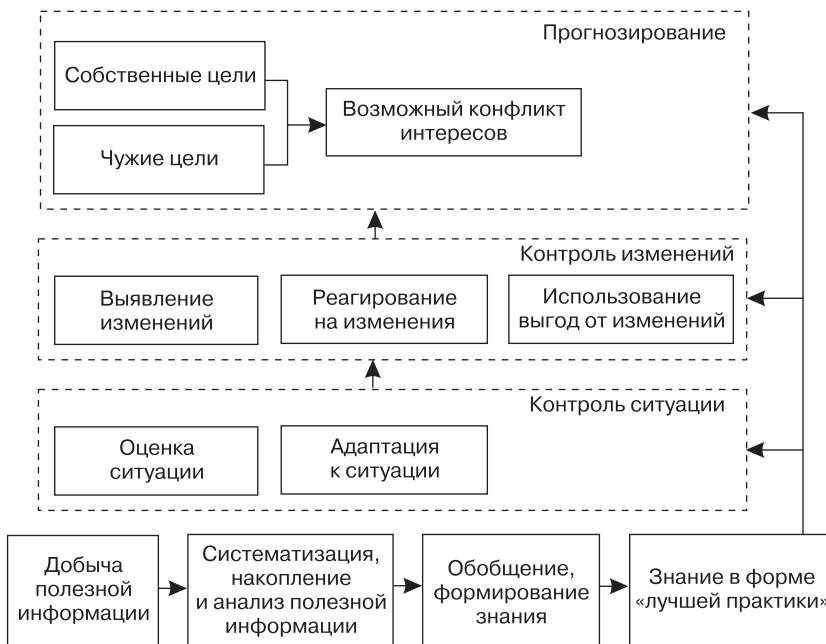


Рис. 8.2. Стратегия действий собственника

Чтобы на них ответить, рассмотрим изначально уже «классическое» определение понятия ИБ для организаций банковской системы (БС) России.

Информационная безопасность: состояние защищенности целей деятельности организации от угроз в ее информационной сфере. Отметим, что ИБ есть состояние, т.е. она рассматривается как процесс, состояние которого может изменяться, может быть «лучше» предыдущего, «хуже» предыдущего или вообще «плохим». Предполагается, что оно может быть измерено и что процессом можно управлять, переводя его из «плохого» состояния в «хорошее», воздействуя на различные параметры процесса. Такое предположение является на самом деле довольно сильным допущением, так как прямые измерения безопасности даже теоретически невозможны в силу сформулированных выше критериев.

Другими словами, проблемой измерений в сфере безопасности является задача измерения отсутствия инцидентов. Сегодня их нет, и через неделю, и через месяц. Так адекватна ли ИБ объекта (организации, вида бизнеса и т.п.), оперативна ли, функциональна ли?

Понять, какая у вас реально безопасность, можно только по факту нападения и нанесения объекту ущерба. В связи с этим всегда, когда говорят об оценках безопасности, надо понимать, что речь идет о некоторых косвенных оценках большого количества измеряемых параметров (их метриках и шкалах) с последу-

ющим их агрегированием в общую оценку, основанную на методах (методиках) с сильной экспертной составляющей.

Учитывая существенную значимость оценки для проблемы обеспечения ИБ, она является одной из областей накопления знаний и по мере их накопления пересматривается для большей ее адекватности реальному состоянию дел.

Следующая используемая в определении ИБ сущность — защищенность (обратное ей — уязвимость) — способность противостоять (противодействовать) действиям противоборствующей стороны — наиболее просто объясняется через величину ущербов, наносимых действиями противной стороны.

Каждый раз, когда реализуется негативно влияющее событие на наши цели деятельности, мы пытаемся понять величину нанесенного нам или ожидаемого в ближайшем будущем ущерба. Не вдаваясь в детали этого понятия (рассмотрим далее), отметим, что каждый раз мы оцениваем потенциально возможный в данной конкретной ситуации ущерб и реально нанесенный. Пусть Y_n — потенциально возможный ущерб, а Y_p — реальный.

Понимая под защищенностью Z отношение

$$Z = \frac{Y_p}{Y_n}, \quad Y_n \geq Y_p,$$

видим, что Z находится в пределах $0 < Z \leq 1$.

Два предельных случая, когда $Z = 0$ и $Z = 1$ интерпретируются как случаи сильной и ничтожной защищенности соответственно.

Говоря далее о целях деятельности организации и ущербе, который может быть нанесен целям деятельности, необходимо прежде всего отметить проблему измерений и оценки как цели, так и ущерба. Она практически аналогична уже рассмотренной проблеме оценки ИБ с той разницей, что оценка целей основывается на ее формализации как минимум до уровня, пригодного до оценки; ущерб же — это экономическая категория и требует более точных и «тонких» моделей. Наиболее опасными (значимыми) видами нанесенного ущерба являются различные неисполненные обязательства. Важно то, что ущерб является для ИБ фундаментальным понятием, система безопасности для того и создается, чтобы избежать ущербов в ситуации противоборства. В связи с этим до тех пор, пока не формализована эта сущность (ущерб), говорить о возможности создания системы безопасности (или об оценке уже существующей системы) затруднительно.

Также фундаментальным понятием является и понятие угрозы. В общем случае к угрозам должны быть отнесены все факторы и обстоятельства, способные оказать ощутимое негативное влияние на реализацию цели. Их описывают, классифицируют по разным признакам. Например, могут быть угрозы, связанные с внешним злоумышленником, а могут быть угрозы со стороны собственного персонала, угрозы, связанные со стихийными бедствиями, терроризмом и т.д.

Говоря об угрозах, необходимо прежде всего отметить их информационный аспект, о них нужно знать, и тем более о тех, которые могут нанести существен-

ный ущерб. Причем это знание для возможности его практического использования должно быть достаточно детальным. Существуют различные классификаторы (перечни) угроз, и они достаточно стабильны, однако факторы, обуславливающие проявление и влияние этих угроз на конкретные процессы и объекты, равно как и сами объекты, непрерывно изменяются, поэтому требуется постоянная актуализация связанных с этими источниками данных, их анализ и идентификация новых рисков (факторов рисков) целям деятельности организации в связи с выявленными изменениями. Такому исследованию должна подвергаться как информация внутри объекта, так и вне его. Цель — добыть (извлечь) полезную информацию для обеспечения безопасности объекта. Реально это представляет целенаправленный процесс поиска различных закономерностей в больших неструктурированных объемах данных с последующим документированием выводов и предположений, подтверждающих или уточняющих имевшиеся сценарии (модели) «хорошего» и «плохого».

И наконец, последняя сущность, определяющая понятие ИБ, — информационная сфера организации. К ней относится все, что используется организацией в информационном виде для достижения ее целей, а также инфраструктура, обеспечивающая информационные процессы организации. Один из компонентов информационной среды — описание (информация относительно) объектов материального мира, задействованных в процессах организации. Кроме того, она включает нормативную базу, соглашения и договоры с вовлеченными сторонами, отчетность, как внутреннюю, так и внешнюю, системы документооборота, планы и т.д.

АСПЕКТЫ ИЗМЕНЧИВОСТИ ИНФОРМАТИКИ И МАТЕРИАЛЬНОЙ СРЕДЫ ОРГАНИЗАЦИИ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НПС

Очевидно то, что информационный мир зачастую существенно сложнее, шире и глубже, чем материальный, и для успешной деятельности организации материальный мир и информационный мир должны быть максимально адекватны друг другу.

Понятно, что если материальный объект реально существует, но его отображение в информационном мире отсутствует, то объект может быть «изъят» из оборота собственника без всяких последствий. Тем самым будет нанесен ущерб. Такая ситуация может быть создана искусственно, так как для операций с описанием реальных объектов их фактическое наличие при этом не требуется¹.

Это один из инструментов противоборства субъектов. Обычно процесс противоборства рассматривают с позиций одной из взаимодействующих сторон. Как правило, один из субъектов — это собственник, а другой — злоумышленник,

¹ Примерами материальных объектов в платежной системе могут быть «физические деньги», ценные бумаги, любые обязательства, представленные в виде документов, драгоценные металлы, драгоценные камни, материальные объекты платежей и т.д.

стремящийся получить контроль над активами собственника в своих целях. Хотя конфликт интересов, разрешающийся в форме противоборства, является самым опасным, современные представления об ИБ этим не исчерпываются и охватывают все возможные виды и источники ущербов целям организации, включая непреднамеренные.

Важно лишь то, что нанесенный ущерб имел «информационную природу», был связан с различными аспектами создания и применения информационной сферы. Так, например, некий субъект, реализовав свою цель, может тем самым существенно повлиять на цели других субъектов, вследствие чего у последних существенно вырастут издержки. В силу того, что такие издержки не прогнозировались, они будут рассматриваться как ущерб. То есть субъекты, реализуя свои цели, могут наносить ущерб друг другу, государству (если деятельность осуществляется в зоне ответственности государства), государство может нанести ущерб субъектам, изменяя условия лицензирования и надзора, изменяя гражданско-правовую систему, и наконец, субъект может нанести ущерб «сам себе», некорректно приняв неадекватный риск. Все указанные аспекты связаны с целеполаганием и процедурами принятия решений и поэтому имеют информационную природу.

Одна из основных причин такого расширенного толкования ИБ связана с существенным качественным и количественным увеличением информационной сферы, увеличением ее сложности, а также степенью ее влияния на цели деятельности любого субъекта. Это привело к тому, что если ранее успех или неуспех дела связывался с различного рода ресурсными ограничениями, то сейчас все более связывается с качеством и номенклатурой сущностей информационной составляющей процессов.

Одним из последствий такого положения является то, что зачастую затруднительно идентифицировать прямых и косвенных выгодоприобретателей от результатов операций в информационной сфере, в том числе и платежных. Вас могут вынудить осуществить платеж анонимному лицу, когда вы не имеете таких намерений, или же, наоборот, вы намерены осуществить платеж и выполнили все необходимые от вас операции, но возникают непредвиденные и неизвестные вам обстоятельства, которые не позволяют завершить операцию успешно. В итоге получатель не располагает сведениями о приходе от вас платежных средств, и это может привести к конкретному ущербу (штрафам, пеням и т.д.).

В общем случае предметом ИБ становится любая деятельность в рамках информационной сферы, способная порождать риски целям деятельности. Учитывая то, что, как уже отмечалось ранее, этот риск нельзя сделать пренебрежительно малым, необходимо создать систему, способную контролировать этот риск и удерживать его на уровне, приемлемом для успеха реализации целей деятельности. Понятно, что система должна представлять собой комплекс различных взаимоувязанных мер противодействия риску.

Однако создать систему безопасности можно с одним на самом деле очень сильным допущением. Оно состоит в том, что созданная система безопасности

неизбежно будет отражать наше же понимание пределов возможного (допустимого) поведения субъектов в информационном мире. Однако информационный мир сам есть отображение сущностей, которые изначально не могут быть строго регламентированы. Так, например, отношения «субъект — субъект» могут быть любыми и определяться взаимными обязательствами практически любых форм и природы. Здесь важно лишь то, что эти обязательства признаются взаимодействующими субъектами. Можно лишь говорить о соответствии этих обязательств целям взаимодействия субъектов, но и цели могут быть самыми разнообразными. Эти аспекты относятся к естественно (*natural*) присущим правам субъектов. Их нельзя (невозможно) директивно (законодательно) отменить, за исключением достаточно очевидных и идентифицируемых на основе простых и однозначно всеми интерпретируемых критериев ситуаций (случаев) заведомого нанесения ущерба (вреда) другим субъектам. В остальных случаях все эти «нюансы», отображаясь на информационную сферу и ее инструменты, будут порождать «серую» (быть может, бессмысленную) для стороннего наблюдателя систему реализующихся видов деятельности, на самом деле целенаправленную.

В указанном смысле построить изначально корректную (непротиворечивую) систему правил поведения субъектов в информационной сфере не представляется возможным. Практически же любые действия приходится признавать допустимыми, т.е. это среда без существенных ограничений, в которой «все средства хороши». А это значительное преимущество противоборствующей стороны, так как злоумышленник продумывает конкретную атаку (вторжение) в конкретных условиях, в то время как собственник пытается построить систему безопасности от всех, в том числе и заранее ему неизвестных, атак. С этими же особенностями связано еще одно важное обстоятельство. Оно состоит в том, что собственник для идентификации действий противоборствующей стороны должен обязательно накопить некоторый объем информации, т.е. в течение некоторого интервала времени (времени идентификации) он не видит уже предпринятой против него атаки. Если это новая атака, то, скорее всего, она будет идентифицирована после нанесения ущерба. То есть собственник приобретает знание «в обмен» на понесенный ущерб. Это его «плата» за знание.

У собственника и злоумышленника существенно разные подходы к проблеме накопления и обобщения знаний. Так, злоумышленник, разрабатывая свою атаку (вторжение), вынужден изучать систему безопасности собственника, в том числе и путем ее исследования, т.е. эксперимента на реальном объекте. Это особо ценное знание.

В свою очередь задача собственника состоит в том, чтобы, во-первых, воспрепятствовать процессу изучения, удлинить во времени этот процесс и, во-вторых, своевременно его идентифицировать, задокументировать и исследовать. Задача данного исследования — установить цель атаки злоумышленника и в конечном счете нейтрализовать ее, приняв соответствующие превентивные меры.

Понятно, что процесс накопления знаний собственника о злоумышленнике содержит существенное ограничение. Оно состоит в том, что собственник не может сам поставить «чистый» эксперимент на злоумышленнике. Его возможности ограничиваются имитацией злоумышленника, как правило, им самим же придуманной. Ценность такого знания существенно ниже.

В общем случае в безопасности рассматриваются две разновидности знаний — знание информационное и знание эмпирическое. Информационное знание получается на абстрактных информационных моделях, либо это знание, полученное от других лиц (субъектов). Такой тип знания может быть получен быстро и в больших объемах. Однако это «слабое» знание. Эмпирическое знание, напротив, — это обобщение собственной практики. Оно основано на реальной фактуре, реально произошедших событиях в конкретных условиях. Однако это очень «медленное» знание. На практике необходимо использовать оба вида знаний. Во многих случаях чужой опыт может принести пользу, «напрямую» им практически никогда не удастся воспользоваться, так как контекст (условия, факторы и обстоятельства), в котором знание было получено, не совпадает с собственным контекстом, в котором оно будет применено. Наилучшей с точки зрения информационного противоборства можно считать ситуацию, когда примерно 70% знания составляет эмпирическое знание, а остальные 30% — информационное.

Этим в основном и определяются как востребованные в безопасности источники знаний, так и процедуры их накопления и обобщения.

В связи с этим, возвращаясь к подходам накопления знаний собственника и злоумышленника, знания собственника о злоумышленнике в основном информационные. Чтобы их усилить, собственник, как правило, привлекает экспертов, осуществляет экспертизы принятых им решений, стремится использовать в своей системе безопасности лучшую практику.

Однако недостаточно только создать систему ИБ. Необходимо также уметь ее пересматривать и совершенствовать, притом так, чтобы обеспечить ее высокую и (или) надлежащую эффективность в «фарватере» осознаваемых рисков. Очевидно, что система, которая стоит дороже, чем суммарный видимый ущерб, который она потенциально способна предотвратить (как правило, не полностью), никому не нужна.

Проблема пересмотра и совершенствования системы безопасности — одна из самых сложных. Практически приходится разрешать коллизию, состоящую в том, что система безопасности, с одной стороны, консервативна по своей природе, а с другой — деградирует во времени.

Консерватизм системы связан со спецификой ее оценки, а деградация обусловлена процессами накопления знаний и естественной изменчивостью объекта защиты и его внешней среды. Для национальной платежной системы проблема преодоления «проклятия изменчивости» особенно актуальна. Области информационной сферы организации и источники изменчивости иллюстрирует рис. 8.3.

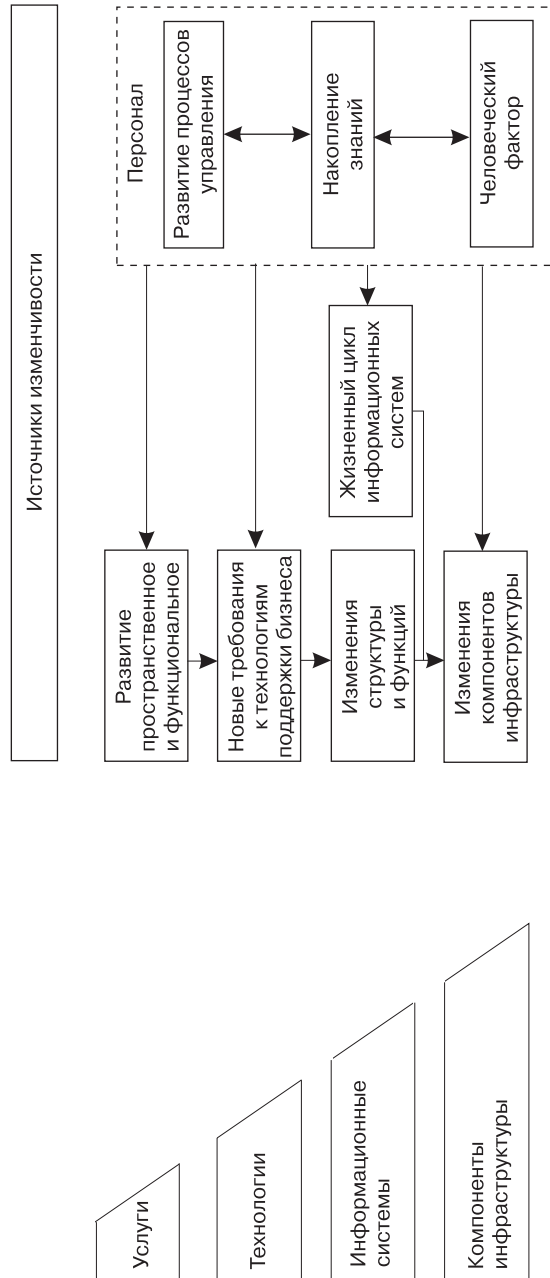


Рис. 8.3. Области информационной сферы организации и источники изменчивости

В примере, приведенном на рис. 8.3, выделяются пять элементов информационной сферы организации. К ним относятся:

- 1) информационно-технологические (ИТ) услуги, предоставляемые организацией;
- 2) информационные технологии организации;
- 3) информационные системы, реализующие технологии и обеспечивающие предоставление ИТ-услуг;
- 4) технические и программные компоненты информационных систем;
- 5) персонал организации, как использующий ИТ-услуги, так и обеспечивающий их предоставления.

На каждом уровне действуют свои факторы изменчивости, в результате чего вся информационная сфера может претерпеть значительные изменения. Необходимость изменений на одном из уровней информационной среды порождает необходимость изменений на всех нижележащих уровнях информационной сферы. Лавинообразный рост количества изменений, требующих реагирования, и их источников — так называемое проклятье изменчивости порождает «разрывы» в информационной сфере и ведет к деградации системы безопасности, становится серьезной проблемой для менеджмента организации.

На уровне ИТ-услуг необходимость изменений порождается потребностью основной деятельности в их функциональном (создание нового функционала и совершенствование существующего) и пространственном (расширение количества и географии потребителей услуг) развитии. Изменение бизнеса влечет изменение технологии деятельности организации, в том числе информационных технологий. Это источники изменчивости на верхнем уровне.

Изменение структуры и функций информационной системы может быть вызвано не только изменениями на более высоких уровнях, но и особенностями ее жизненного цикла, влекущими необходимость обновления технических и программных средств и их компонентов, реинжиниринг структуры и функционала системы, интеграцию с новыми системами.

Персонал организации может стать источником изменчивости на любом из перечисленных уровней. Источниками изменчивости на уровне персонала являются развитие процессов управления (планирования, организации, координации, контроля и др.), накопление знаний (например, новые знания могут сделать ненужными часть функций системы или упростить процессы эксплуатации), а также другие факторы, связанные с деятельностью персонала, включая особенности личности и группового поведения (ошибки, халатность, отсутствие должной координации работ, высокая активность и т.д.).

Так, например, проводя аналогии с платежной системой Банка России, можно утверждать, что инфраструктура национальной платежной системы будет содержать несколько сотен тысяч компьютеров разного назначения. Компьютер полностью амортизируется и подлежит замене через четыре года эксплуатации.

Таким образом, ежегодно должна производиться замена нескольких десятков тысяч компьютеров (скорее всего, более ста тысяч), и это только в порядке поддержки жизненного цикла без учета функционального и пространственного развития системы. Причем все это должно будет осуществляться в рамках деятельности сотен и тысяч организаций, вовлеченных в операции системы на фоне перманентной эволюции платежного инструментария, доступного на рынке для миллионов пользователей услуг национальной платежной системы.

Внешняя среда, и прежде всего нормативная база, не менее изменчива. Отображаясь на прикладной программный продукт как наиболее чувствительный для подобного рода изменений, она породит десятки тысяч изменений в год. Учитывая, что изменения «один в один» невозможны (через четыре года точно такого же компьютера, как старый, уже не найти), они будут создавать риски и, быть может, значимые. Так как для систем большой размерности и сложности характерны различные неоднородности, т.е. изменчивость может концентрироваться на ограниченных пространственно-временных и функциональных областях, то при слабом управлении (менеджменте) ИБ будут образовываться и достаточно долго существовать «черные дыры», которые могут быть использованы для вторжения и установления контроля над активами. В связи с этим без постоянных локальных изменений системы безопасности, без все более тонкой ее «привязки» к объекту не обойтись. При этом основополагающие принципы построения системы, ее организационно-техническое устройство и менеджмент остаются достаточно стабильными.

Как очевидно следует из изложенного, эффективная система обеспечения ИБ должна непременно содержать сильный центр и мобильный ресурс (в организационном смысле). Сильный центр компетенции кроме проблем реагирования должен обеспечивать наработку хорошей практики и ее распространение. Его деятельность должна быть хорошо интегрирована в общий менеджмент, так как она затрагивает и обеспечивает интересы всех организаций и клиентов.

Особое положение служб безопасности организаций заключается в том, что они (ее сотрудники) накапливают высокочувствительные знания об уязвимостях процессов деятельности организаций, а также в том, что они используют для этого «специфический информационный ресурс» и инструменты, поэтому очевидно, что как сами знания, так и информация и инструменты должны быть хорошо (в организационном и техническом смысле) изолированы.

В силу специфики своей деятельности безопасность в любой организации является основным организатором деятельности по внедрению высокой информационной культуры. Фактически это выработка и внедрение в практику деятельности системы правил, определяющих модель «безопасного» поведения в условиях агрессивной среды. Они включают в себя правила и рекомендации по идентификации опасных состояний и реагированию на них, в том числе и эскалации (информированию вышестоящей инстанции и передаче ей ответственности).

МОДЕЛЬ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ НПС

Другой фундаментальной задачей, лежащей в сфере внимания безопасности, является контроль работоспособности процедур «синхронизации» изменений в информационной сфере с изменениями в материальном мире (изменениями в активах и т.п.). Каждая транзакция в информационном поле платежных технологий имеет отражение в изменении материального мира (рис. 8.4).

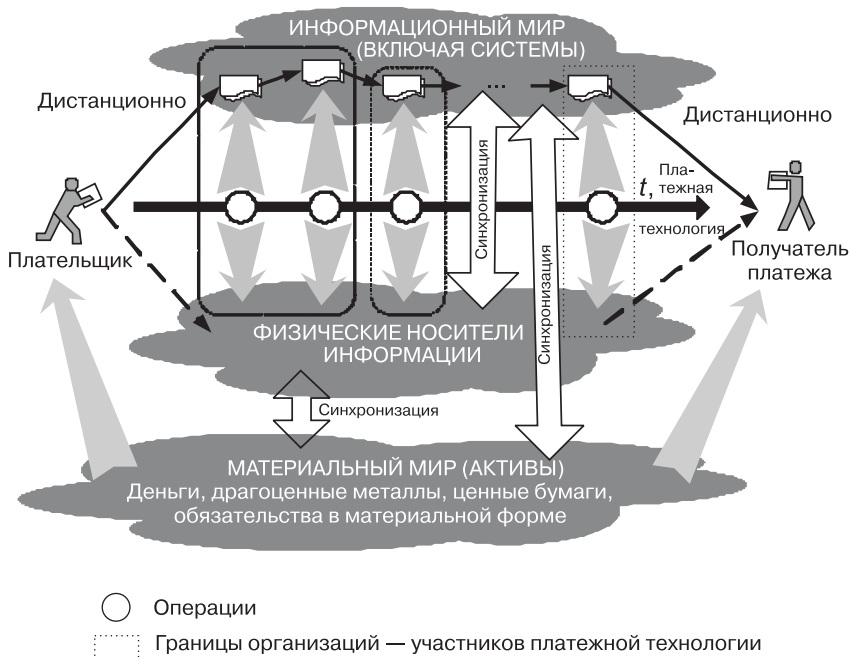


Рис. 8.4. Общая информационно-логическая модель платежной технологии

В современном мире центром притяжения злоумышленников все чаще становится информационная сфера, посредством манипуляции в которой они пытаются присвоить некие сущности материального мира.

Информационная культура очень значима. Она совместно с регламентацией основной деятельности в виде ролей и ответственностей участвующих сторон позволяет существенно сузить стохастическую составляющую процессов деятельности и упростить проблему обеспечения ИБ. В ситуации, когда, наоборот, порядок в основной деятельности слаб и она представляется как слабодетерминированный (плохо предсказуемый) процесс, говорить о возможности адекватного и эффективного обеспечения ИБ нельзя, так как нельзя разделить «плохое» и «хорошее» и непонятно, чему же нужно противодействовать, что является риском, а что нет.

Весьма чувствительным для системы безопасности является вопрос о том, в рамках каких организационных форм она должна быть обеспечена. Если мы говорим о какой-либо сущности как о системе, то первым ее признаком, по крайней мере с точки зрения безопасности, является наличие в ней развитого менеджмента. Говорить о системе как о множестве независимых субъектов, действующих на основе соглашений, тем более юридически не обязывающих, крайне сложно, и если можно, то с очень сильными ограничениями, потому что какие-то, хотя бы и слабые, обязательства всеми субъектами должны быть приняты.

Должен существовать эталон этих обязательств, например, в виде стандарта (системы взаимоувязанных стандартов) безопасности. Должны быть организованы контрольные механизмы соблюдения всеми обязательств, действующие на принципах доверия и прежде всего независимости и незаинтересованности контролера, например, в форме аудита безопасности. Должно быть понимание того, что слабое звено у одного субъекта есть слабость всех участвующих субъектов и любому из них может быть нанесен ущерб. Одним из способов обеспечения ИБ может быть также перенос риска на третьих лиц (страхование риска безопасности) или же самостоятельное формирование такого фонда самострахования системы. В рамках национальной платежной системы в зависимости от того, как она будет развиваться, потребуется разработка стратегии обеспечения ИБ как одного из важнейших ее аспектов.

Понятно, что система, в которой часто происходят крупные инциденты ИБ, будет иметь очень низкий уровень доверия. В этом случае риски ИБ будут очень сильно влиять на риски основной деятельности, так же как потеря доверия к банку со стороны его клиентов практически всегда приводит к катастрофическим последствиям для банка. В связи с этим высокие риски ИБ опасны не только «сами по себе», но более как сильный источник влияния на риски основной деятельности.

Для национальной платежной системы, видимо, технологии безопасности сформируют один из основных инструментов обеспечения доверия, поэтому особенно важно с самого начала обеспечить приемлемый ее уровень, иначе потом придется длительное время и с большими затратами восстанавливать статус-кво системы.

В этой связи большое значение будет иметь организационно-техническое устройство национальной платежной системы. Если исходить из того, что в нее окажутся вовлечены тысячи независимых субъектов, предоставляющих инфраструктуру и инструменты пользователям, то проблема менеджмента в такой «аморфной» среде окажется центральной проблемой. Единственная подходящая форма, предусмотренная в отечественной гражданско-правовой системе, — это саморегулируемая организация (СРО). Она предполагает возможность применения достаточно сильных мер при аккредитации субъекта в организации, развитые возможности по контролю деятельности субъекта со стороны организации, механизмы оперативного рассмотрения и урегулирования коллизий, ответствен-

ность за результаты деятельности. В отдельных случаях в соответствии с законодательством исключение субъекта из соответствующей СРО тождественно запрету на легальную профессиональную деятельность.

Если реализуется такой или подобный этому алгоритм устройства общего менеджмента НПС, то в этих рамках после соответствующей адаптации вполне могут быть реализованы основные принципы корпоративного устройства системы обеспечения ИБ. Адаптация при этом сведется в основном к эквивалентной замене директивного управления на независимый аудит (аудит третьей стороной) и последующее реагирование организации в виде управления допустимыми полномочиями субъекта (через ограничение возможностей) на основе риск-ориентированных моделей. Очевидно, что для этого должна быть создана соответствующая инфраструктура. Она должна содержать механизмы подготовки и аккредитации достаточного количества аудиторов и аналитиков, необходимое нормативно-методическое и информационное обеспечение и инструментарий.

При этом очень важно иметь в виду, что ИБ не самодостаточная область деятельности, а всего лишь часть общего менеджмента.

Цели и задачи обеспечения ИБ, если они прямо не предусмотрены законом (например, Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»), формируются общим менеджментом на основе того, какие процедурные и иные гарантии пользователям будут предоставляться функционалом НПС. Данные цели и задачи должны быть обращены на то, чтобы кому-нибудь, например, не был «продан» несуществующий товар или оказана несуществующая услуга либо заблокированы активы пользователей вследствие, например, «информационных разборок» конкурирующих операторов НПС и т.д.

Все это — предмет серьезной проработки в конкретных практических условиях.

Реально складывающиеся условия в большей или меньшей степени отличны от теоретически предполагаемых, поэтому не всегда возможно предвидеть каждую реальную ситуацию и отразить это в форме системы точных требований. В этом случае формулируется система принципов¹, отражающая основное содержание и модель восприятия, а также ожидаемые действия в некоторой предметной области.

Это утверждение справедливо не только для бизнес-уровня, где, например, КПРС Банка международных расчетов сформулировано 14 принципов для международной гармонизации процесса разработки и развития национальных платежных систем в разных странах. Накопленный за последние два десятилетия опыт, подкрепленный широкой практикой, нашел отражение и в области безопасности. В числе авторитетных руководств, отражающих принципы безопасности для различных видов деятельности, можно выделить как универсальные

¹ Принцип или «начало» (от лат. *principium*, греч. αρχή) — в теоретической философии то, чем объединяется в мысли и в действительности известная совокупность фактов.

международные стандарты, такие как ISO/IEC 27000¹, так и отраслевые решения, например, изложенные в Руководстве ЕРС (European Payment Council) EPC397-08v1.1 по хорошим практикам безопасности дистанционного банковского обслуживания.

Использование принятой в профессиональном сообществе системы принципов обеспечения информационной безопасности позволит сформировать условия для взвешенного и рационального решения практических задач.

8.2. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ

Системы принципов обеспечения информационной безопасности в задачах корпоративного управления участников НПС

Принципы осознанного решения задач обеспечения информационной безопасности (отдельного бизнеса, деятельности организации, взаимодействующих сторон, профессионального сообщества и пр.) основываются на понимании природы факторов рисков (угроз) и структуры рисков, а также подходов по их модификации (переноса, принятия, снижения, ухода). Существенная часть рисков информационной безопасности порождается процессами операционной среды организации и среды ее корпоративного управления, а также при взаимодействии сторон как внутри организации, так и вне ее.

Рассмотрим данный срез на примере принципов обеспечения информационной безопасности организации и одного из срезов взаимодействия при обслуживании клиентов банков.

Основными факторами осознанного внимания высшего руководства организации к задачам обеспечения ИБ являются:

- понимание необходимости наличия прогнозируемой, эффективной и управляемой системы обеспечения информационной безопасности;
- совершенствование делового климата в организации и повышение эффективности работы с персоналом;
- стремление к повышению эффективности системы управления операционными и иными специфичными рисками, которые «сопровожают» деятельность организации;
- понимание необходимости соответствия установленным профессиональным нормам контроля рисков, эффективная реализация которых может

¹ Международный стандарт ISO/IEC 27000 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология». Обеспечивает введение, обзор и терминологию для серии стандартов ISO/IEC 270XX на системы управления информационной безопасностью организаций и сопутствующие технологии обеспечения информационной безопасности.

быть осуществлена технологиями обеспечения информационной безопасности;

- формирование основ повышения стоимости организации при слияниях и поглощениях, а также повышения рыночной стоимости в глазах рыночных инвесторов;
- повышение привлекательности для зарубежных инвесторов и партнеров.

В профессиональной среде выделяют два подмножества принципов безопасного функционирования: «общие» и «специальные» («настроечные»), формирующие основное концептуальное содержание видов деятельности в данной предметной области.

В состав общих принципов безопасного функционирования организации входят следующие:

- своевременность обнаружения проблем. Организация должна своевременно обнаруживать проблемы, потенциально способные повлиять на ее бизнес-цели;
- прогнозируемость развития проблем. Организация должна выявлять причинно-следственную связь возможных проблем и строить на этой основе точный прогноз их развития;
- оценка влияния проблем на бизнес-цели. Организация должна адекватно оценивать степень влияния выявленных проблем на ее бизнес-цели;
- адекватность защитных мер. Организация должна выбирать защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от выполнения угроз;
- эффективность защитных мер. Организация должна эффективно реализовывать принятые защитные меры;
- использование опыта при принятии и реализации решений. Организация должна накапливать, обобщать и использовать как свой опыт, так и опыт других организаций на всех уровнях принятия решений и их исполнения;
- непрерывность действия принципов безопасного функционирования. Организация должна обеспечивать последовательность в реализации принципов безопасного функционирования;
- контролируемость защитных мер. Организация должна применять только те защитные меры, правильность работы которых может быть проверена. При этом организация должна регулярно оценивать адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на бизнес-цели организации.

Реализация специальных принципов обеспечения ИБ направлена на повышение уровня зрелости процессов управления ИБ в организации. В состав специальных принципов обеспечения информационной безопасности организации входят следующие:

- определенность целей. Функциональные цели организации и цели ее системы обеспечения ИБ должны быть явно определены во внутрикорпоратив-

тивных нормативных актах. Неопределенность приводит к «размыванию» организационной структуры, ролей и обязанностей персонала, неконструктивности политик ИБ и невозможности оценки адекватности принятых решений и защитных мер;

- знание своих клиентов и служащих. Организация должна обладать информацией о своих клиентах, тщательно подбирать персонал (служащих), выработать и поддерживать корпоративную этику, что создает благоприятную доверительную среду для деятельности организации по управлению активами. Знание клиентов в современном мире может иметь различное наполнение (от физической личности до виртуальных (информационных) ее атрибутов). В любом случае степень необходимого и достаточного «знания» должна быть определена;
- персонификация и адекватное разделение ролей и ответственности. Ответственность должностных лиц организации за решения, связанные с ее активами, должна персонифицироваться. Она должна быть адекватной степени влияния должностных лиц на цели организации, фиксироваться в политиках, контролироваться и совершенствоваться;
- адекватность ролей функциям и процедурам и их сопоставимость с критериями и системой оценки. Роли должны адекватно отражать исполняемые функции и процедуры их реализации, принятые в организации. При назначении взаимосвязанных ролей должна учитываться необходимая последовательность их выполнения. Роль должна быть согласована с критериями оценки эффективности ее выполнения. Основное содержание и качество исполняемой роли реально определяются применяемой к ней системой оценки;
- доступность услуг и сервисов. Организация должна обеспечить доступность для своих клиентов и контрагентов услуг и сервисов в установленные сроки, определенные соответствующими договорами (соглашениями) и (или) иными документами;
- наблюдаемость и оцениваемость обеспечения ИБ. Любые предлагаемые защитные меры должны быть устроены так, чтобы результат их применения был явно наблюдаем (прозрачен) и мог бы быть оценен подразделением организации, имеющим соответствующие полномочия.

«Роль: Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом»

Изложенная система принципов безопасного функционирования организации имеет преимущественно отношение к среде корпоративного управления и на практике реализуется в систему взаимосвязанных, как правило, не выраженных явно, но идентифицируемых процессов, осуществляемых в рамках управленческой деятельности организации. В «продвинутых» организациях центром компетенции данных работ является совет (координационный совет) по информационной безопасности, функционирующий при первом исполнительном лице (его заместителе) организации.

Применительно к действиям руководства организации это предполагает инициирование и поддержку следующих мероприятий:

- создание, внедрение и актуализация политики ИБ;
- внедрение мер, направленных на обеспечение уверенности в том, что цели и планы ИБ установлены и работоспособны;
- определение ролей и ответственности в области информационной безопасности;
- осведомленность всех сотрудников организации информации о важности достижения целей информационной безопасности и подчинения требованиям политики информационной безопасности, об их ответственности перед законом, а также о необходимости непрерывного совершенствования;
- обеспечение достаточных ресурсов для эксплуатации, анализа и совершенствования системы обеспечения ИБ организации;
- наличие решений о критериях принятия рисков и о приемлемых уровнях риска безопасности;
- проведение контроля и анализа (самооценки, аудиты, выводы из результатов разбора инцидентов и т.п.);
- обеспечение уверенности в достаточной компетентности персонала, на который возложены определенные в рамках системы обеспечения ИБ обязанности.

Указанные мероприятия реализуются в рамках следующих процессов деятельности на уровне корпоративного управления организации:

- анализ проблем ИБ и определение потребности организации в обеспечении ИБ;
- рассмотрение и санкционирование руководством деятельности по планированию мероприятий обеспечения ИБ организации;
- сопровождение операционной деятельности системы обеспечения ИБ;
- поддержка и анализ результатов мероприятий по проверке системы обеспечения ИБ;
- определение стратегий совершенствования системы обеспечения ИБ.

Анализ проблем ИБ даже на высшем уровне невозможен без охвата общего контекста бизнеса организации, ее стратегий, целей деятельности и основных показателей эффективности существования. Процессы по обеспечению ИБ составляют один из видов вспомогательных процессов, реализующих поддержку основной деятельности организации для достижения максимально возможного результата.

Здесь должны рассматриваться как факторы целесообразности и эффективности в части соотношений «прибыли» от защищенности критичных активов и расходов на разворачивание системы ИБ, так и комплаенс факторы процессов деятельности организации. Для этих целей должны быть учтены:

- характеристики информационных активов организации, их размещение, владелец (обладатель), пользователь, важность их для бизнеса организации, категории классификации, уровни защиты и иные необходимые сведения;

- результаты менеджмента активов организации, выраженные в оценке влияния инцидентов ИБ на активы: финансовой восстановительной стоимости, стоимости остановки бизнес-операций в результате потери (повреждения) актива, издержек упущенных возможностей и т.д.;
- спецификации бизнес-процессов организации;
- критерии достижения бизнес-целей;
- отчетность и производственные показатели основной деятельности (бизнеса) организации;
- данные о потерях, о нанесенном бизнесу ущербе (материальном и ином);
- информация о среде бизнес-процессов организации, включающая данные о внешних и внутренних угрозах, информацию о персонале, внешних контактах и взаимодействиях, информацию от заинтересованных сторон относительно бизнес-процессов, активов, информационной безопасности и т.д.;
- отчетность об ИБ организации, о текущем состоянии процессов менеджмента ИБ.

Реализация иных процессов деятельности на уровне корпоративного управления организации в контексте принципов безопасного функционирования организации формирует необходимые основы развертывания и совершенствования процессов системы менеджмента ИБ (СМИБ) организации, включая решения:

- по определению целей ИБ, адекватности и контролируемости защитных мер;
- по закреплению ответственностей по ИБ, связанных со СМИБ;
- по адекватности разделения ролей и ответственности;
- о взаимодействии между структурными подразделениями организации;
- о выделении необходимых ресурсов для обеспечения ИБ;
- по критериям оценки эффективности защитных мер, мерам доверия клиентов и служащих и обеспечению доступности услуг и сервисов.

Данные процессы, являясь фактически частью основной управленческой деятельности организации, имеют отношение ко всей организации. Они «работают» со сведениями, имеющими отношение к результатам основной деятельности организации, но необходимы для принятия адекватных потребностям решений относительно ИБ и осуществления менеджмента ИБ организации в целом.

По результатам этой деятельности вырабатываются ключевые решения относительно всех областей обеспечения ИБ организации, реализуемые в среде организации — участника НПС.

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ДИСТАНЦИОННОМ БАНКОВСКОМ ОБСЛУЖИВАНИИ

Отдельные сферы в основной деятельности организации могут быть сопряжены со специфичными, типичными и чувствительными рисками для ее деятельности. Применительно к финансовой индустрии одной из таких сфер является интерфейс на стыке взаимодействия «банк — клиент». Все более широкое ис-

пользование электронных (дистанционных) средств и технологий доступа к финансовым услугам, включая и платежные операции, сопряжено с существенными специфическими рисками. Здесь затрагиваются интересы не только принимающей «заказ» на финансовую услугу (операцию) организации, но и иных участников системы. Это в свою очередь и определяет потребность в целевом рассмотрении данной области.

Российская практика в данной области пока еще не столь систематизирована для выработки унифицированных рецептов лучших практик. В то же время в ряде стран и сообществ подобные решения предложены и они достаточно работоспособны в соответствующей среде. Среди них можно выделить Рекомендации ЕРС¹, предлагающие руководствоваться 12 принципами, отражающими хорошую практику обеспечения безопасности при дистанционном банковском обслуживании. Данные Рекомендации развивают ранее изданные Европейским комитетом по банковским стандартам рекомендации, нашедшие отражение в TR 411v2 «Руководство по обеспечению безопасности для электронных банковских услуг» (*Security guidelines for e-banking: application of basel risk management principles*) применительно к взаимодействию «клиент — банк».

В рекомендациях ЕРС представлены принципы и руководства по хорошим практическим приемам обеспечения безопасности во взаимодействиях «клиент — банк» по отношению к дистанционному инициированию электронных операций для схем прямого дебетового и кредитного трансферта в едином европейском платежном пространстве. Данные принципы по мнению ЕРС применимы для решений по электронным или мобильным платежным каналам в Европе, а также могут применяться для участников системы электронного выставления счетов-фактур. Эти принципы рекомендуются для использования в качестве инструментальных средств банками, поставщиками электронных банковских услуг или любой стороной, действующей от их имени. Они направлены на установление общего базового уровня безопасности для всех удаленных операций «клиент — банк» единого европейского платежного пространства.

Принцип 1. Совет директоров и высшее руководство финансовых институтов, предоставляющих электронные банковские услуги, должны установить эффективный надзор руководства за рисками, связанными с этой деятельностью, включая конкретную ответственность, политики и меры и средства контроля и управления для осуществления действий в отношении информации о рисках. Например, до начала трансграничной электронной банковской деятельности они должны провести соответствующую оценку риска и должную проверку.

Принцип 2. Финансовые институты, предоставляющие электронные банковские услуги, должны принимать соответствующие меры для идентификации и регистрации клиентов, с которыми они осуществляют дистанционное взаимодействие.

¹ ЕРС397-08v1.1, March 15th 2009, Customer-to-bank. Security good practices guide.

Принцип 3. Финансовые институты, предоставляющие электронные банковские услуги, должны принимать соответствующие меры для обеспечения взаимной аутентификации, осуществляемой между ними и клиентами, с которыми они осуществляют дистанционное взаимодействие.

Принцип 4. Финансовые институты, предоставляющие электронные банковские услуги, должны принимать соответствующие меры для обеспечения методов аутентификации транзакций, способствующих неотказуемости и учетности электронных банковских транзакций.

Принцип 5. Финансовые институты, предоставляющие электронные банковские услуги, должны принимать соответствующие меры для обеспечения защиты чувствительных данных в электронных банковских транзакциях.

Принцип 6. Финансовые институты, предоставляющие электронные банковские услуги, должны обеспечить наличие соответствующих мер и средств контроля и управления санкционированием(-я) и привилегий доступа для систем, баз данных и приложений электронных банковских услуг.

Принцип 7. Финансовые институты, предоставляющие электронные банковские услуги, должны обеспечить наличие соответствующих мер для защиты данных электронных банковских транзакций, регистрационных данных и информации.

Принцип 8. Финансовые институты, предоставляющие электронные банковские услуги, должны обеспечить наличие подробных контрольных журналов для всех электронных банковских транзакций.

Принцип 9. Финансовые институты, предоставляющие электронные банковские услуги, должны иметь эффективные процессы планирования мощностей, обеспечения непрерывности бизнеса и действий в чрезвычайных ситуациях для содействия обеспечению доступности электронных банковских систем и услуг.

Принцип 10. Финансовые институты, предоставляющие электронные банковские услуги, должны разработать соответствующие планы реагирования для осуществления менеджмента, сдерживания и минимизации проблем, возникающих из-за неожиданных событий, включая внутренние и внешние атаки, которые могут препятствовать обеспечению электронных банковских услуг и работе систем.

Принцип 11. Финансовые институты, предоставляющие электронные банковские услуги, должны обеспечить предоставление достаточного количества информации на своих web-сайтах, чтобы дать возможность потенциальным клиентам принять взвешенное решение до инициирования электронных банковских транзакций. Например, финансовые институты, намеревающиеся заняться трансграничной деятельностью, должны раскрыть на своем web-сайте достаточный объем сведений, чтобы позволить потенциальным клиентам определить страну его расположения и тип выданной лицензии.

Принцип 12. Финансовые институты, предоставляющие электронные банковские услуги, должны принять соответствующие меры для обеспечения стро-

того соблюдения требований законодательства страны, где они предоставляют электронные банковские услуги и продукты.

В качестве хорошей отправной точки для реализации указанных принципов обеспечения (информационной) безопасности для удаленных операций «клиент — банк» ЕРС рекомендуется рассматривать ряд мер и средств контроля и управления, проистекающих из норм законодательства и иных практик, в том числе нашедших отражение в международных стандартах, таких как стандарты серии ISO/IEC 270XX.

Меры и средства контроля и управления, считающиеся важными для организации с законодательной точки зрения, включают:

- а) обеспечение защиты данных и приватности персональной информации;
- б) обеспечение безопасности регистрационных данных в организации;
- в) права на интеллектуальную собственность.

Меры и средства контроля и управления, считающиеся установившейся практикой для обеспечения информационной безопасности, включают:

- а) документацию политики информационной безопасности;
- б) классификацию данных по уровню чувствительности;
- в) распределение обязанностей по обеспечению информационной безопасности;
- г) осведомленность, образование и обучение в сфере информационной безопасности;
- д) безопасную разработку, тестирование (безопасности) и поддержку ИТ-инфраструктуры, устройств, приложений и процессов;
- е) менеджмент уязвимостей;
- ж) менеджмент непрерывности бизнеса;
- з) менеджмент инцидентов информационной безопасности.

Нижеследующая таблица иллюстрирует рекомендации ЕРС по поддержке реализации принципов теми или иными категориями мер и средств контроля и управления безопасности из стандарта ISO/IEC 27002.

| Категория требований ISO/IEC 27002 | ЕРС-принципы | | | | | | | | | | | |
|---|--------------|----|----|----|----|----|----|----|----|-----|-----|-----|
| | П1 | П2 | П3 | П4 | П5 | П6 | П7 | П8 | П9 | П10 | П11 | П12 |
| Политика безопасности | X | – | – | – | – | – | – | – | – | – | – | – |
| Организация обеспечения информационной безопасности | X | – | – | – | – | – | – | – | – | – | – | – |
| Менеджмент активов | – | X | – | – | – | X | X | X | – | – | – | – |

Окончание

| Категория требований ISO/IEC 27002 | ЕРС-принципы | | | | | | | | | | | |
|--|--------------|----|----|----|----|----|----|----|----|-----|-----|-----|
| | П1 | П2 | П3 | П4 | П5 | П6 | П7 | П8 | П9 | П10 | П11 | П12 |
| Кадровая безопасность | – | – | – | – | – | Х | – | – | – | – | – | – |
| Физическая безопасность и защита от влияния внешней среды | Х | – | – | – | – | – | – | – | – | – | – | – |
| Менеджмент связи и операций | Х | Х | Х | Х | Х | Х | Х | Х | – | – | Х | – |
| Управление доступом | – | Х | Х | – | – | Х | – | – | – | – | – | – |
| Приобретение, разработка и поддержка информационных систем | Х | Х | Х | Х | Х | Х | Х | Х | – | – | Х | – |
| Менеджмент инцидентов информационной безопасности | – | – | – | – | – | – | – | – | – | Х | – | – |
| Менеджмент непрерывности бизнеса | – | – | – | – | – | – | – | – | Х | – | – | – |
| Соответствие требованиям | Х | Х | – | – | – | – | – | – | – | – | Х | Х |

В национальной платежной системе практически все из изложенных принципов в определенной степени применимы для соответствующих видов деятельности. Конкретные решения подлежат определению органом регулирования и надзора (наблюдения) за деятельностью участников НПС в установленном порядке.

Использование лучших практик корпоративного управления и контроля, включая практику управления и контроля в информационной сфере, существенным образом снижает стохастическую составляющую в деятельности организации, что качественным образом влияет на эффективность мер обеспечения информационной безопасности. Это также обеспечивает базу для «сходимости» различных форм и методов контроля, используемых как для целей управления, так и для надзора и наблюдения за деятельностью участников НПС.

К лучшим практикам корпоративного управления и контроля в информационной сфере относятся как отдельные модельные решения, подобно рекомендациям COSO, Базельского комитета и его структур, так и стандарты обеспечения информационной безопасности, включая уже отмеченные и иные международные и отраслевые стандарты.

8.3. МОДЕЛЬНЫЕ РЕШЕНИЯ И СТАНДАРТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОБЩАЯ СТРУКТУРА

Основу доверия в среде участников НПС формирует использование общепризнанных лучших практик, нашедших отражение в соответствующих нормах и стандартах организации и реализации деятельности.

Соответствие участника системы тем или иным признанным стандартам и (или) лучшим практикам, подтвержденным независимой оценкой (аудитом), формирует основание для уверенности в нем его партнеров и клиентов и доверие к системе в целом. Например, когда финансовый институт присоединяется к некоторому сообществу (вступает в платежную систему), он тем самым подтверждает свою готовность и берет на себя обязательство следовать правилам этого сообщества (платежной системы), определяющим технические, юридические и финансовые аспекты его функционирования в системе. Такое признание правил системы является основой для взаимного доверия между неизвестными друг другу сторонами и иными участниками при организации ими безналичных расчетов для своих клиентов.

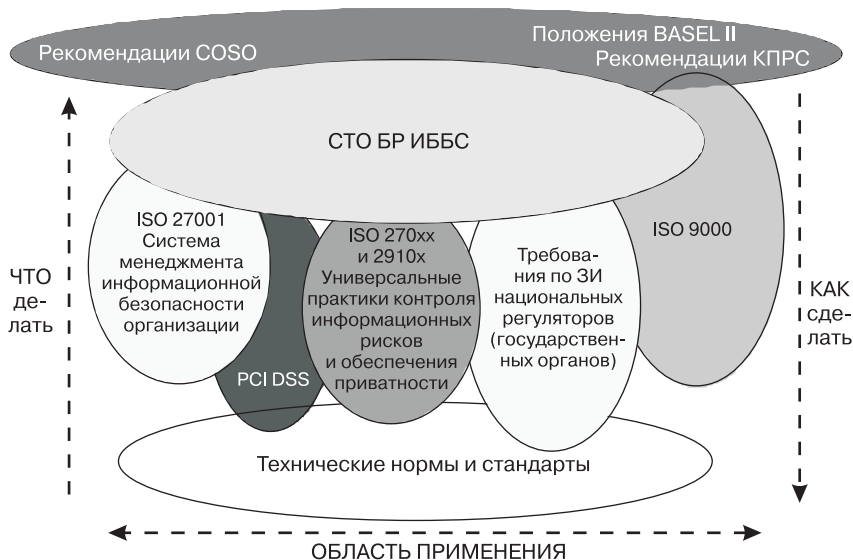
Из всего многообразия доступных решений должны быть выбраны те, что обеспечивают совместимость в операционной среде организации и условия эффективного корпоративного контроля и управления. Для российских финансовых организаций это может представлять собой множество взаимодополняющих решений, охватывающих как корпоративный менеджмент, так и операционную среду. На рисунке 8.5 представлена общая структура данного подхода.

Следование рекомендациям COSO и рекомендациям банковских регуляторов в среде корпоративного менеджмента обеспечивает условия реализации принципов обеспечения информационной безопасности организации.

Использование адаптированных к национальным условиям практик и методологии обеспечения информационной безопасности финансовой организации, закрепленных в документах по стандартизации Банка России «СТО/РС БР ИББС» (стандарт (рекомендации) в области стандартизации Банка России информационная безопасность организаций банковской системы), обеспечивает основное содержание практических шагов. Требования данных документов Банка России не претендуют на всеобъемлющий охват и при необходимости могут быть дополнены соответствующими дополнительными мерами и средствами контроля и управления безопасностью из иных источников.

В качестве таких источников рекомендуется использовать международные стандарты ISO/IEC комплексов 270XX и 2910X, а также национальные нормы органов регулирования в области безопасности и защиты информации. О стан-

дартах 270XX отмечалось ранее и более подробно будет изложено далее. Стандарты комплекса 2910X начали формироваться в 2008 г. в ответ на все более широкое и глубокое проникновение информатики в общественные связи и частную жизнь, а также увеличение объемов трансграничных операций с данной информацией. Требования стандартов комплекса 2910X отражают лучшие приемы и сложившиеся практики обеспечения так называемой *privacy&security* в современном электронном мире.



- COSO — Комитет спонсорских организаций
 КППС — Комитет по платежным и расчетным системам
 Банка международных расчетов
 СТО БР ИББС — Стандарты Банка России в области
 информационной безопасности
 ISO 9000 — Стандарты Международной организации
 по менеджменту качества
 ISO 270xx — Стандарты Международной организации стандартизации
 по управлению информационной безопасностью
 PCI DSS — Стандарт безопасности данных индустрии платежных карт

Рис. 8.5. Структура практик и стандартов обеспечения информационной безопасности для НПС

Включение PCI DSS в структуру стандартов рис. 8.5 отражает ситуацию де-факто. Комплекс документов, именуемый как PCI DSS, изданный уполномоченным органом международных платежных систем, является обязательным к реализации стандартом для участников этих платежных систем. Требования PCI DSS имеют более техническую направленность. Для объектов национальной платежной системы, сопоставимых с объектами регулирования PCI DSS, могут быть использованы те же требования или аналогичные им.

МОДЕЛЬ COSO

Структура, получившая широкую известность под аббревиатурой COSO (The Committee of Sponsoring Organizations (of the Treadway Commission)) была создана для финансирования работ независимой национальной (американской) комиссии, образованной для выработки мер противодействия мошенничеству с финансовой отчетностью.

Целью деятельности комиссии являлось изучение факторов, которые могут приводить к мошенничеству с финансовой отчетностью, и выработка соответствующих рекомендаций для частных компаний и их независимых аудиторов, для инспекторов Комиссии США по ценным бумагам и биржевым операциям (SEC) и других инспекторов и образовательных учреждений.

Спонсорами (членами COSO) выступили пять профессиональных ассоциаций, располагавшихся в США: Американская ассоциация бухгалтеров, Американский институт дипломированных общественных бухгалтеров, Международная ассоциация финансовых руководителей, Институт внутренних аудиторов и Национальная ассоциация бухгалтеров (ныне известен как Институт бухгалтеров-управленцев). Первый отчет комиссии был опубликован в 1987 г.

К настоящему времени основные направления деятельности комиссии COSO отражены в документах, посвященных следующим вопросам:

- анализ фактов мошенничества в финансовой отчетности;
- внутренний контроль;
- менеджмент риска в организации.

Документы комиссии по вопросам организации внутреннего контроля и риск-менеджмента в компаниях наиболее востребованы практикой в сфере корпоративного управления и контроля (аудита). Процессы глобализации финансовых, сырьевых, товарных рынков послужили дополнительным стимулом поиска универсальных методологических (модельных) платформ функционирования организаций (моделей деятельности организаций).

Модель системы внутреннего контроля COSO уже де-факто стала эталоном организации внутрикорпоративной деятельности.

В то же время первое поколение модельной формы требований документов COSO оставляли не охваченными сложные для регулирования ниши, чем со временем смогли воспользоваться недобросовестные управленцы. Это в свою очередь послужило толчком для развития методологии COSO и перевода ее на обновленную платформу — платформу риск-менеджмента. В 2001 году рабочий орган COSO инициировал проект по разработке концептуальных основ управления риском для использования руководством компаний при оценке своей системы управления рисками и ее дальнейшем совершенствовании.

Суть обновленного подхода проста: руководство организации самостоятельно определяет и оценивает факторы и источники рисков целям своей деятельности и принимает необходимые меры. Проверяющая сторона рассматривает эти

материалы и выносит свой вердикт. Следует заметить, что эта же методология используется и для управления рисками информационной безопасности.

Одним из самых важных вопросов, решаемых высшим руководством организаций, как отмечается в материалах COSO, является определение величины риска, который организация готова принять и принимает в процессе своей деятельности по созданию добавленной стоимости (материалы комиссии, финансируемой COSO, обращены к коммерческим структурам, в этой связи в ее материалах делается акцент на прибыль (добавленную стоимость)).

Основная предпосылка при управлении рисками деятельности организации заключается в том, что каждая организация существует, чтобы создавать добавленную стоимость для сторон, заинтересованных в ее деятельности. При этом все организации сталкиваются с неопределенностью, и задачей руководства является принятие решения об уровне неопределенности, с которым организация готова смириться, стремясь увеличить стоимость для заинтересованных сторон. В этой связи неопределенность, с одной стороны, таит в себе риск (потери), а с другой — может открыть новые возможности, поэтому принятые в условиях неопределенности решения могут привести как к снижению, так и к увеличению стоимости.

Управление риском, как отмечается в материалах COSO, позволяет руководству эффективно действовать в условиях неопределенности и связанных с ней рисков и использовать возможности, увеличивая потенциал для роста стоимости компании.

В соответствии с методологией COSO управление риском организации включает в себя следующие ключевые задачи:

- определение уровня риска, на который готова идти организация в соответствии со своей стратегией развития;
- совершенствование процесса принятия решений по реагированию на возникающие риски;
- сокращение числа непредвиденных событий и убытков в хозяйственной деятельности;
- определение и управление всей совокупностью рисков в хозяйственной деятельности;
- использование благоприятных возможностей;
- рациональное использование капитала.

Влияние событий в сфере неопределенности может быть положительным, отрицательным или одновременно и тем и другим. События, влияние которых является отрицательным, методологией COSO предлагается относить к риску, который мешает созданию или ведет к снижению стоимости. События, влияние которых является положительным, могут компенсировать отрицательное влияние рисков, а также положительно влиять на достижение результата.

По COSO управление рисками организации:

- представляет собой непрерывный процесс, охватывающий всю организацию;

- осуществляется сотрудниками на всех уровнях организации;
- используется при разработке и формировании стратегии;
- применяется во всей организации, на каждом ее уровне и в каждом подразделении и включает анализ портфеля рисков на уровне организации;
- нацелен на определение событий, которые могут влиять на организацию и управление рисками таким образом, чтобы они не превышали порог готовности организации идти на риск;
- дает руководству и совету директоров организации разумную гарантию достижения целей;
- связан с достижением целей по одной или нескольким пересекающимся категориям.

Существует прямая взаимосвязь между целями или тем, чего организация стремится достичь, и компонентами процесса управления рисками организации, представляющими собой действия, необходимые для их достижения. Данная взаимосвязь иллюстрируется в материалах COSO трехмерной матрицей (кубом), представленной на рис. 8.6.

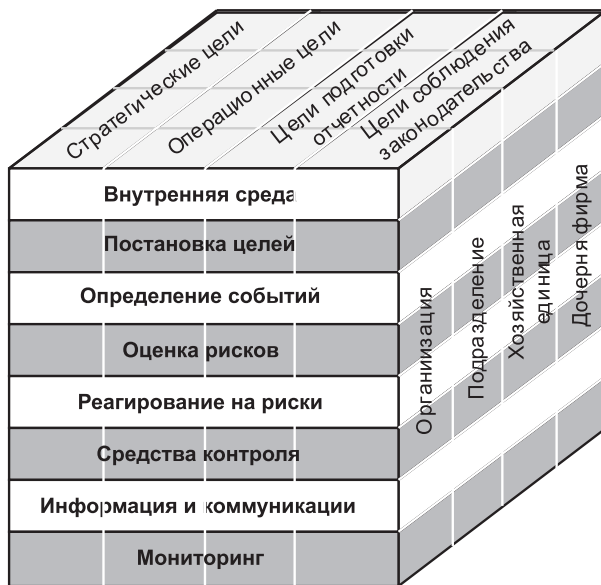


Рис. 8.6. Связь между целями организации и компонентами процесса управления рисками организации

Данный рисунок отражает пересмотренный подход руководств Комитета COSO (называемый еще COSO II), который является более детализированным по сравнению с материалами, лежащими в основе первого поколения руководства Комитета COSO, датируемого началом 1990-х гг. Для реализации данного подхо-

да на практике организация должна разработать (принять) удовлетворяющую ее целям понятийную базу, установить цели, задачи, объемы, распределить ответственность, а также утвердить методологию управления операционными рисками.

По методологии Комитета COSO восемь взаимосвязанных компонентов системы управления рисками организации (см. рис. 8.6) имеют следующее назначение.

- **Внутренняя среда.** Внутренняя среда представляет собой атмосферу в организации и определяет, каким образом риск воспринимается сотрудниками организации и как они на него реагируют. Внутренняя среда включает философию управления рисками и уровень риска, на который готова идти организация, честность и этические ценности, а также ту среду, в которой они существуют.
- **Постановка целей.** Цели должны быть определены до того, как руководство начнет выявлять события, которые потенциально могут оказать влияние на их достижение. Процесс управления рисками предоставляет «разумную» гарантию (если более точно, то некие свидетельства как основание для уверенности) того, что руководство компании имеет правильно организованный процесс выбора и формирования целей и эти цели соответствуют задачам организации и ее готовности идти на риск.
- **Определение событий.** Внутренние и внешние события, оказывающие влияние на достижение целей организации, должны определяться с учетом их разделения на риски (потери) или возможности (благоприятное стечение обстоятельств, «улыбнулась удача» и т.п.). Возможности должны учитываться руководством в процессе формирования стратегии и постановки целей.
- **Оценка рисков.** Риски анализируются с учетом возможности (правдоподобности) их возникновения и влияния с целью определения того, какие действия в отношении них необходимо предпринять. Риски оцениваются с точки зрения присущего (характерного) и остаточного риска.
- **Реагирование на риск.** Руководство выбирает метод реагирования на риск — уход от риска, принятие, снижение или перенос (перераспределение) риска, разрабатывая ряд мероприятий, которые позволяют привести выявленный риск в соответствие с допустимым уровнем риска и готовностью организации рисковать.
- **Средства контроля.** Политики и процедуры разработаны и установлены таким образом, чтобы обеспечивать «разумную» гарантию того, что реагирование на возникающий риск происходит эффективно и своевременно.
- **Информация и коммуникации.** Необходимая информация определяется, фиксируется и передается в такой форме и в такие сроки, которые позволяют сотрудникам выполнять их функциональные обязанности. Также осуществляется эффективный обмен информацией в рамках организации как по вертикали сверху вниз и снизу вверх, так и по горизонтали.

- Мониторинг. Весь процесс управления рисками организации отслеживается и по необходимости корректируется и совершенствуется. Мониторинг осуществляется в рамках текущей деятельности руководства или путем проведения периодических оценок.

Система внутреннего контроля организации позиционируется как составная часть процесса управления риском организации. Управление риском на уровне организации рассматривается как более широкий, чем внутренний контроль, процесс. Он включает и развивает систему внутреннего контроля, преобразуя ее в более эффективную форму, акцентированную на риск. В свою очередь менеджмент риска рассматривается как часть системы общекорпоративного менеджмента.

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ МЕНЕДЖМЕНТА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ КОМПЛЕКСА ISO/IEC 270XX

Весь комплекс стандартов, представленный на рис. 8.7, направлен на обеспечение осуществления эффективного управления информационной безопасностью в организации. Каждый из стандартов, входящих в комплекс стандартов СМИБ, направлен на рассмотрение определенного вопроса в рамках управления информационной безопасностью в организации. Далее представлено краткое описание стандартов, входящих в рассматриваемый комплекс.

ISO/IEC 27000 «СМИБ — Обзор и терминология» (Information security management systems — Overview and vocabulary). Данный стандарт был разработан с целью обеспечить единый и понятный базис для всех стандартов, имеющих отношение к СМИБ. В него включен систематизированный перечень терминов и определений, используемых в комплексе стандартов СМИБ. Стандарт является ключевым документом в рассматриваемом комплексе стандартов СМИБ, поскольку содержит изложение основных вопросов, связанных с информационной безопасностью, а также точные формулировки принципов, терминов и определений.

ISO/IEC 27001 «СМИБ — Требования» (Information security management systems — Requirements). Данный стандарт является центральным в семействе стандартов СМИБ. Он определяет требования по созданию, реализации, использованию, мониторингу, пересмотру, поддержке и усовершенствованию документированной СМИБ в контексте рисков для бизнеса организации, по реализации мер и средств контроля и управления, «настроенных» в соответствии с потребностями отдельных организаций или их подразделений.

ISO/IEC 27002 «Свод практик по информационной безопасности» (Code of practice for information security management). Данный стандарт содержит полное руководство по реализации мер и средств контроля и управления информационной безопасностью и напрямую поддерживает ISO/IEC 27001. Ряд вопросов, затронутых в данном стандарте, связаны со стандартами ISO/IEC 27003 и ISO/IEC 27005.

ISO/IEC 27003 «Руководство по реализации СМИБ» (Information security management systems implementation guidance). Данный стандарт представляет ру-

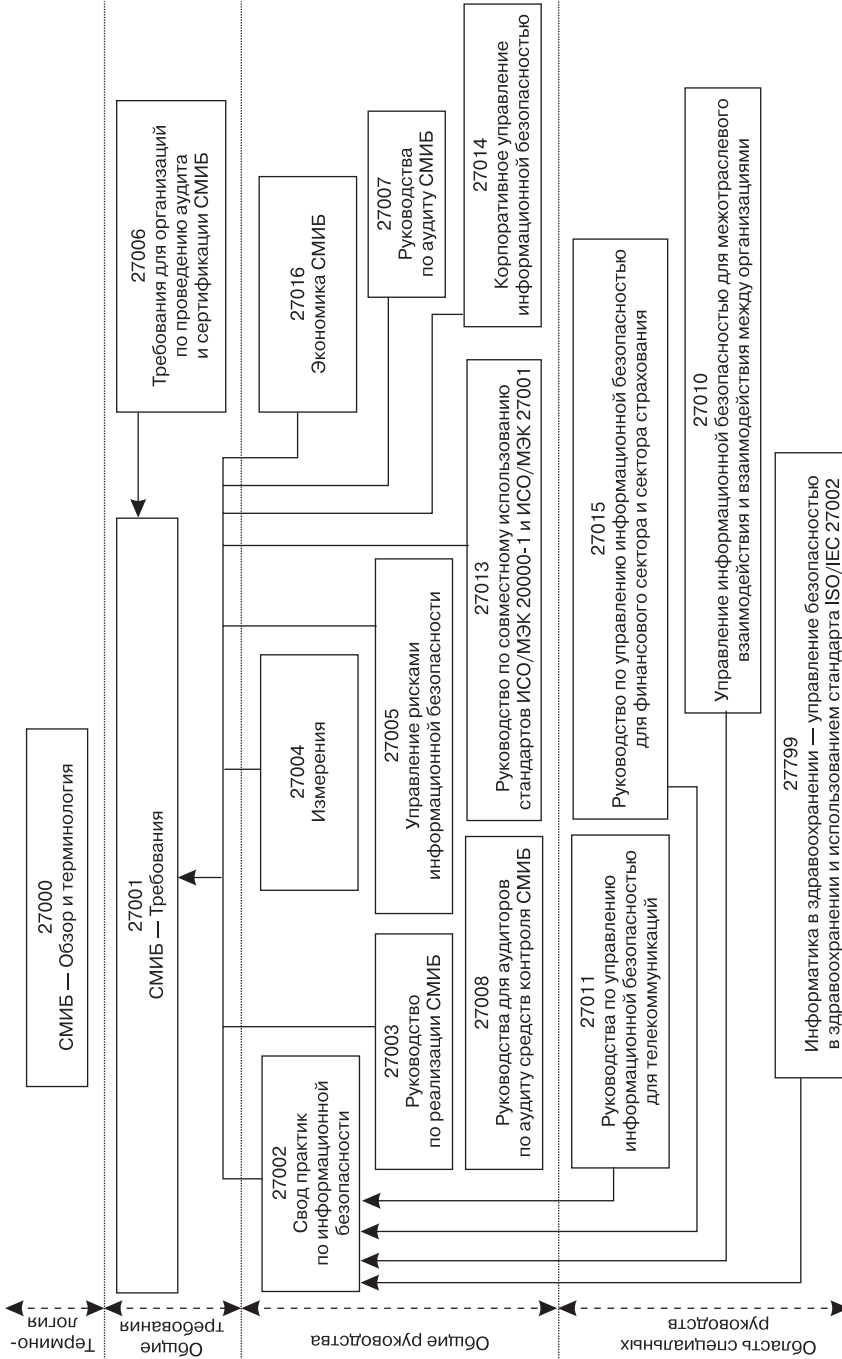


Рис. 8.7. Структура семейства стандартов СМИБ

ководство по реализации СМИБ и напрямую поддерживает ISO/IEC 27001. Он также включает основные положения, модели и руководящие материалы по информационной безопасности для обеспечения независимого руководства для организации в части выбора мер и средств контроля и управления из соответствующего раздела ISO/IEC 27002 и улучшения уже реализованных мер и средств контроля и управления безопасностью с учетом меняющихся условий.

ISO/IEC 27004 «Измерения» (Information security management measurements). Данный стандарт дает возможность эффективно выполнять измерения уровня эффективности реализованных мер и средств контроля и управления и процессов, описанных в ISO/IEC 27001. Для обеспечения эффективности данный стандарт рассматривает ряд измерений, включая правомерность применения в конкретном случае, эффективность затрат, эффективность и уровень реализации мер и средств контроля. В дополнение к этому, используя требования данного стандарта, можно получить сведения и понять, в каких случаях применение положений стандарта ISO/IEC 27001 было адекватно потребностям организации и способствовало достижению ее постоянного улучшения, а в каких случаях необходимы изменения.

ISO/IEC 27005 «Менеджмент рисков информационной безопасности» (Information security risk management). Данный стандарт представляет руководство по менеджменту рисков информационной безопасности и затрагивает принципы менеджмента риска информационной безопасности, методы оценки риска информационной безопасности, обработки и принятия риска, обмена сведениями о рисках, мониторинга и пересмотра риска, предоставляя информацию по применению ISO/IEC 27001.

ISO/IEC 27006 «Требования для организаций, осуществляющих аудит и сертификацию СМИБ» (Requirements for bodies providing audit and certification of information security management systems). Данный стандарт определяет требования для организаций, осуществляющих аудит и сертификации СМИБ. Стандарт организован как дополнение (надстройка) к универсальным требованиям для органов, осуществляющих аудит и сертификацию систем менеджмента организаций, содержащимся в стандарте ISO/IEC 17021.

ISO/IEC 27007 «Руководство для аудита СМИБ» (Guidelines for information security management systems auditing). Данный стандарт представляет руководство по проведению аудитов СМИБ. Стандарт обеспечивает специфичное руководство, необходимое аудиторам СМИБ. Он обеспечивает поддержку реализации требований ISO/IEC 27006 и требований универсального руководства по аудиту систем менеджмента, представленного в ISO 19011.

ISO/IEC 27008 «Руководство для аудиторов по аудиту средств контроля СМИБ» (Guidance for Auditors on ISMS Controls). Данный технический отчет представляет руководство по проверке свидетельств работы и качества реализации мер и средств контроля и управления СМИБ. Данный стандарт поддерживает задачи планирования и осуществления оценивания мер и средств контроля и управления СМИБ, других процессов обеспечения уверенности в эффектив-

ности СМИБ, процессов менеджмента риска информационной безопасности и управления информационной безопасностью в рамках организации.

ISO/IEC 27010 «Менеджмент информационной безопасности для межотраслевого взаимодействия и взаимодействия между организациями» (Information security management guidelines for inter-sector communications). Данный стандарт представляет руководство по менеджменту информационной безопасности при взаимодействии и сотрудничестве между организациями государственного и (или) частного сектора.

ISO/IEC 27011 «Руководство по менеджменту информационной безопасности для телекоммуникаций» (Information security management guidelines for telecommunications). Данный стандарт устанавливает основные принципы и представляет руководство по инициации, реализации, поддержке и совершенствованию менеджмента информационной безопасности для телекоммуникационных компаний, основанное на ISO/IEC 27002.

ISO/IEC 27013 «Руководство по совместному использованию стандартов ИСО/МЭК 20000-1 и ИСО/МЭК 27001» (Guidance on the integrated implementation of 20000-1 and 27001). Данный стандарт представляет руководство по совместному использованию систем менеджмента информационной безопасности и систем менеджмента услуг ИТ в рамках одной и той же организации.

ISO/IEC 27014 «Корпоративное управление информационной безопасностью» (Information security governance framework). Данный стандарт представляет руководство по разработке и использованию структуры управления информационной безопасностью для оказания содействия организации в вопросах управления и контроля процессов СМИБ в соответствии с ISO/IEC 27001. Стандарт может применяться в организациях всех типов и размеров. Стандарт представляет руководящие принципы для руководителей организации в отношении результативности, эффективности и допустимого использования информационной безопасности в организации.

ISO/IEC 27015 «Руководство по менеджменту информационной безопасности для финансового сектора» (Information security management guidelines for financial services). Данный стандарт представляет руководство по поддержке реализации менеджмента информационной безопасности в секторе финансовых услуг.

ISO/IEC 27016 «Экономика СМИБ» (Information security management — Organizational economics). Данный технический отчет содержит руководство по представлению экономических подходов руководству организации по эффективному выделению или ограничению ресурсов в рамках менеджмента безопасности информационных активов.

ISO/IEC 27799 «Информатика в здравоохранении — управление безопасностью в здравоохранении с использованием стандарта ISO/IEC 27002» (Health informatics — Information security management in health using ISO/IEC 27002). Данный стандарт определяет руководство по поддержке интерпретации и реализации информатики в здравоохранении в соответствии с ISO/IEC 27002. Рассматриваемый

стандарт определяет набор детализированных мер и средств контроля и управления и представляет руководство по использованию лучших практик в области информационной безопасности в здравоохранении.

В группе стандартов ISO/IEC 270XX отдельным блоком выделен ряд стандартов, рассматривающих вопросы информационной безопасности, связанные с использованием определенных технологий, таких как:

- готовность информационных технологий к обеспечению непрерывности бизнеса (ISO/IEC 27031);
- безопасность сетей (ISO/IEC 27033);
- безопасность приложений (ISO/IEC 27034);
- менеджмент инцидентов информационной безопасности (ISO/IEC 27035);
- вопросы информационной безопасности при взаимодействии с поставщиками (ISO/IEC 27036);
- вопросы, связанные со свидетельствами, представленными в цифровой форме (ISO/IEC 27037);
- вопросы информационной безопасности при работе с электронными документами (ISO/IEC 27038).

ISO/IEC 27031 «Руководство по обеспечению готовности информационных и коммуникационных технологий к процессу обеспечения непрерывности бизнеса» (Guidelines for ICT readiness for business continuity). Данный стандарт описывает концепции и основные принципы, применяемые для обеспечения готовности информационных и коммуникационных технологий для бизнес-сообщества к процессу непрерывности бизнеса.

ISO/IEC 27033 «Безопасность сетей» (Network Security). Данный стандарт состоит из шести частей, каждая из которых представляет детальное руководство по определенным аспектам безопасности менеджмента, эксплуатации и использования сетей и их взаимодействий.

ISO/IEC 27034 «Безопасность приложений» (Application Security). Данный стандарт состоит из пяти частей, каждая из которых представляет процессно-ориентированное руководство для разработчиков программного обеспечения и средств обеспечения безопасности, аудиторов и менеджеров организации по определению, разработке (при необходимости), реализации, управлению, поддержке и исключению приложений из рассмотрения в качестве объектов информационной безопасности.

ISO/IEC 27035 «Менеджмент инцидентов информационной безопасности» (Information security incident management). Данный стандарт представляет руководство по менеджменту инцидентов информационной безопасности для менеджеров информационной безопасности и менеджеров информационных систем, сервисов и сетей. Стандарт подходит для использования в организациях любых размеров.

ISO/IEC 27036 «Информационная безопасность при взаимодействии с поставщиками» (Guidelines for security of outsourcing). Данный стандарт представляет руководство по оценке рисков безопасности, возникающих при приобретении

или использовании услуг аутсорсинга в соответствии с мерами и средствами контроля и управления из ISO/IEC 27001 и ISO/IEC 27002 в части аутсорсинга.

ISO/IEC 27037 «Руководство по идентификации, сбору и (или) получению и хранению юридически значимых свидетельств, представленных в цифровой форме» (*Guidelines for identification, collection and/or acquisition and preservation of digital evidence*). Данный стандарт представляет детальное руководство, описывающее процесс признания, идентификации, сбора и (или) сохранности цифровых данных, которые могут содержать информацию, потенциально выступающую в качестве доказательств.

Назначение и практику использования стандартов семейства ISO/IEC 270XX иллюстрирует рис. 8.8.

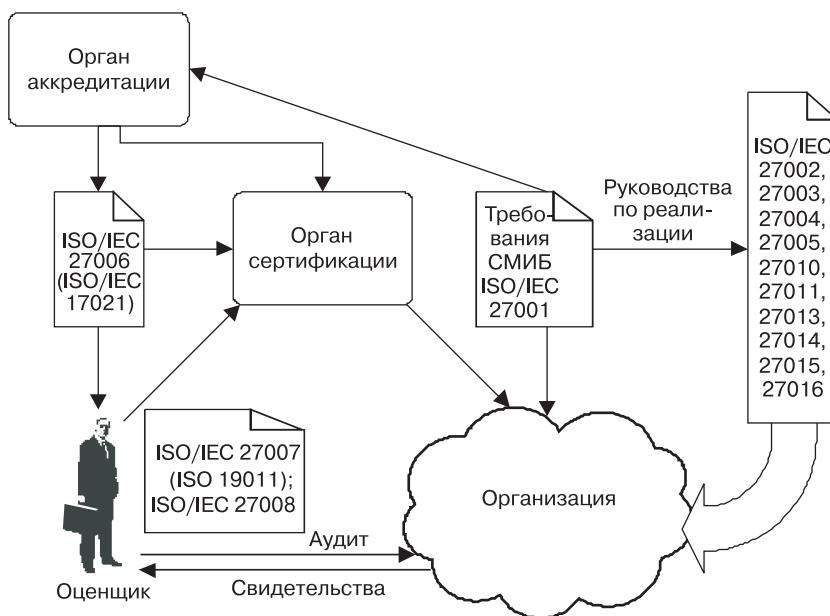


Рис. 8.8. Применение стандартов семейства ISO/IEC 270XX

Заявление о соответствии стандарту ISO/IEC 27001 предполагает, что:

- СМИБ организации (на практике, как правило, это функциональный объект (подразделение) в организации, определенный в так называемых границах СМИБ) отвечает требованиям, изложенным в ISO/IEC 27001;
- подготовлен документ «Положение о применимости» (см. п. 4.2.1 j) ГОСТ Р ИСО/МЭК 27001-2006), содержащий обоснование и комментарии, подготовленные на основе оценки и обработки рисков ИБ, об использовании или неиспользовании в границах СМИБ стандартизированных (более 120) мер и средств контроля и управления (в оригинале controls), представ-

ленных в приложении А к стандарту ISO/IEC 27001. Более подробно данные стандартизированные меры и средства контроля и управления рассмотрены в ISO/IEC 27002;

- основой оценки соответствия стандарту ISO/IEC 27001 являлась методика оценки соответствия, действующая в соответствующей системе оценки и сертификации СМИБ по критериям ISO/IEC 27001;
- результат соответствия стандарту ISO/IEC 27001 оформлен в соответствии с требованиями, действующими в соответствующей системе оценки и сертификации СМИБ по критериям ISO/IEC 27001;
- процесс оценки соответствия ISO/IEC 27001 осуществлялся в соответствии с требованиями к процессу аудита, действующими в соответствующей системе оценки и сертификации СМИБ по критериям ISO/IEC 27001. Для унификации и поддержки данных процедур разработан международный стандарт ISO/IEC 27007, требования которого предназначены установить единые процедуры аудита СМИБ. Для этих же целей дополнительно к международному стандарту ISO/IEC 27007 подготовлен стандарт ISO/IEC 27008;
- аудитор (аудиторская группа) являлись лицами, аккредитованными в соответствующей системе аккредитации персонала, и компетентен для оценки и сертификации СМИБ по критериям ISO/IEC 27001. Для унификации и поддержки данных процедур в 2006 г. был принят международный стандарт ISO/IEC 27006, установивший единые минимально достаточные требования по аккредитации аудиторов (аудиторских групп) и персонала органов сертификации СМИБ.

Как нетрудно заметить, все основные процедурные и методические аспекты лежат в плоскости компетенции учредителей соответствующих систем оценки соответствия и сертификации. На практике заявления о соответствии стандарту ISO/IEC 27001 имеют преимущественно утилитарную цель: демонстрации партнерам по бизнесу, клиентам и иным заинтересованным сторонам, что система контроля информационных рисков компании имеется и она обладает надлежащей функциональностью. Естественно, что «на слово» верить можно, но лучше иметь документальное подтверждение — сертификат соответствия. Именно поэтому стандарт ISO/IEC 27001 еще называют сертификационным стандартом.

Учитывая, что все бремя обеспечения компетентности оценщиков и качества аудита СМИБ ложится на систему оценки соответствия и систему аккредитации в соответствующей области деятельности, важнейшим фактором, влияющим на доверие к сертификату СМИБ, является принадлежность его к системе оценки и аккредитации. Например, биржи и финансовые рынки доверяют далеко не всем системам аккредитации и оценки соответствия в области СМИБ.

В случае необходимости независимого признаваемого подтверждения соответствия своей СМИБ ISO/IEC 27001 компании, включая российские, обращаются к специализированным органам сертификации, имеющим признанную потребителями аккредитацию. Одним из таких признаваемых органов по понятным

причинам является UKAS (United Kingdom Accreditation Service), а также иные органы.

На практике подготовка к сертификации СМИБ компании включает следующие этапы:

- определение области действия (границ) «стандартной» СМИБ. Эта фаза в зависимости от размера компании может занять срок от одной недели до полугода;
- проведение анализа рисков в границах СМИБ;
- выявление и анализ несоответствий применяемых в организации мер и средств контроля и управления, относительно представленных в приложении А к стандарту ISO/IEC 27001;
- разработка недостающих процедур и документации СМИБ;
- внедрение процедур СМИБ;
- опытная эксплуатация СМИБ;
- обучение персонала компании в объеме, необходимом для последующего сопровождения и развития СМИБ.

Соответствие СМИБ требованиям ISO/IEC 27001 с последующей сертификацией, осуществляющейся в признанных на международном уровне системах сертификации, сопряжено со значительными усилиями организации по приведению ее СМИБ в соответствие с требованиями стандарта. Например, в состав документов внутренней нормативной базы может потребоваться включение (с сопутствующей разработкой недостающих) следующих положений:

а) политики СМИБ (корпоративной политики ИБ), а также процедур и соответствующих внутренних нормативных актов по поддержке политики СМИБ (корпоративной политики ИБ) в актуальном состоянии;

б) частных политик для подсистем, технологий и подразделений и соответствующих процедур и внутренних нормативных актов по их поддержке в актуальном состоянии, включая (но не ограничиваясь этим):

- документы и требования по маркировке и обработке информации,
- документы по анализу и оценке рисков ИБ. Критериям принятия рисков,
- политику обеспечения ИБ на основных технологических и производственных участках,
- политику (матрицы (роли) управления доступом,
- политику мониторинга и реагирования на инциденты,
- антивирусную политику,
- политику использования Интернета,
- политику использования электронной почты в деятельности подразделения,
- политику лицензионного программного обеспечения,
- политику использования сети и протоколов проводной и беспроводной передачи данных,
- основные требования по физической безопасности,
- политику для жизненного цикла данных и т.д.;

в) планов обеспечения безопасности, включая:

- план обучения информационной безопасности,
- план осведомленности по информационной безопасности,
- план совершенствования эффективности СМИБ,
- план тестирования систем,
- план тестирования при приемке,
- план управления в чрезвычайных ситуациях,
- план мероприятий по достижению соответствия нормативным и регулирующим требованиям и т.д.;

г) корпоративных стандартов и нормативных актов для элементарных операционных задач, включая:

- инструкции ИБ (дополнение действующих инструкций) административному и обслуживающему персоналу,
- инструкции ИБ (дополнение действующих инструкций) пользователей систем и сетей,
- приведение в соответствие внутренних нормативных актов по жизненному циклу систем,
- приведение в соответствие внутренних нормативных актов по конфиденциальности и политики обслуживания потребителей,
- настроечные стандарты для конфигурации каждой из эксплуатируемых в подразделениях системы,
- настроечные стандарты, процедуры и политики обработки данных средствами телекоммуникаций,
- настроечные стандарты для конфигурации ключевых устройств каждой из эксплуатируемых в организации сетей и т.д.

В каждом конкретном случае номенклатура необходимых документов внутренней нормативной базы СМИБ будет различаться.

Для каждого из выпущенных организацией документов внутренней нормативной базы СМИБ должны поддерживаться данные об их исполнении (в западных стандартах такие данные проходят под термином *records*). Все это вместе должно быть представлено аудитору СМИБ (нормы и свидетельства их исполнения).

ДОКУМЕНТЫ ПО СТАНДАРТИЗАЦИИ БАНКА РОССИИ «СТО/РС БР ИББС»

В комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» входят следующие стандарты (СТО) и рекомендации по стандартизации (РС):

СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»;

СТО БР ИББС-1.1 «Обеспечение информационной безопасности. Аудит информационной безопасности»;

СТО БР ИББС-1.2 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС 1.0-20xx»;

РС БР ИББС-2.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0»;

РС БР ИББС-2.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0»;

РС БР ИББС-2.2 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности»;

РС БР ИББС-2.3 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации»;

РС БР ИББС-2.4 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации».

Стандарт Банка России СТО БР ИББС-1.0 распространяется на организации банковской системы Российской Федерации (БС РФ) и устанавливает требования по обеспечению ИБ в организациях БС РФ. Данный стандарт устанавливает требования к системе обеспечения информационной безопасности (СОИБ), СМИБ и системе информационной безопасности (СИБ) организаций БС РФ. Общую взаимосвязь СОИБ, СМИБ и СИБ организации БС РФ иллюстрирует рис. 8.9.

Стандарт Банка России СТО БР ИББС-1.1 распространяется на организации БС РФ, а также на организации, проводящие аудит ИБ организаций БС РФ, и устанавливает требования к проведению внешнего аудита ИБ организаций БС РФ.

Основными целями аудита ИБ организаций БС РФ являются:

- повышение доверия к организациям БС РФ;
- оценка соответствия ИБ организаций БС РФ критериям аудита ИБ, установленным требованиями стандарта Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

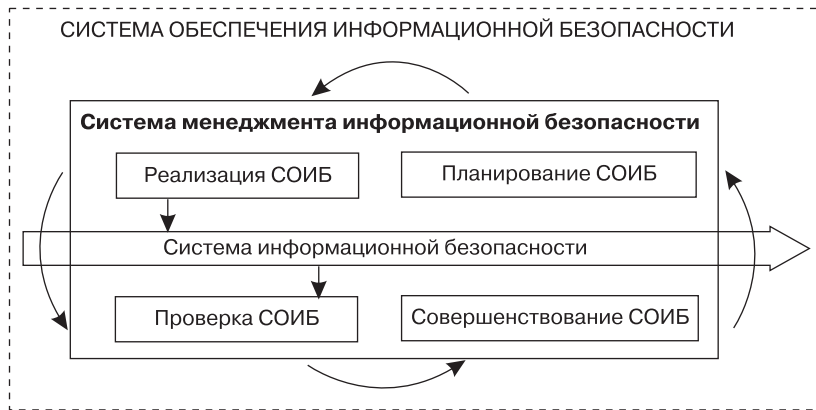


Рис. 8.9. Система обеспечения информационной безопасности организации БС РФ

В данном стандарте устанавливаются основные принципы и требования к проведению аудита ИБ организации БС РФ, а также общие требования проведения самооценки ИБ. В поддержку стандарта СТО БР ИББС-1.1 в части проведения самооценки ИБ организаций БС РФ используются рекомендации в области стандартизации Банка России РС БР ИББС – 2.1.

Стандарт Банка России СТО БР ИББС-1.2 устанавливает способы определения степени выполнения требований стандарта Банка России СТО БР ИББС-1.0, а также итогового уровня соответствия ИБ требованиям стандарта Банка России СТО БР ИББС-1.0 при проведении внутренней и (или) внешней оценки и (или) самооценки ИБ.

Данная методика оценки соответствия ИБ распространяется на организации БС РФ, а также на организации, проводящие оценку уровня обеспечения ИБ организации БС РФ в соответствии с требованиями стандарта Банка России СТО БР ИББС-1.0.

Целью методики оценки соответствия является установление подходов и способов оценки, используемых для определения уровня соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0 по направлениям оценки:

- текущий уровень ИБ организации;
- менеджмент ИБ организации;
- уровень осознания ИБ организации.

Для отображения результатов оценивания соответствия используется круговая диаграмма, представленная на рис. 8.10, секторы которой соответствуют так называемым групповым показателям оценки соответствия.

Групповые показатели (секторы на рис. 8.10) с 1-го по 10-й используются для отображения оценки текущего уровня ИБ организации, с 11-го по 27-й — для отображения оценки процессов менеджмента ИБ организации, с 28-го по 34-й — для отображения оценки уровня осознания ИБ организации.

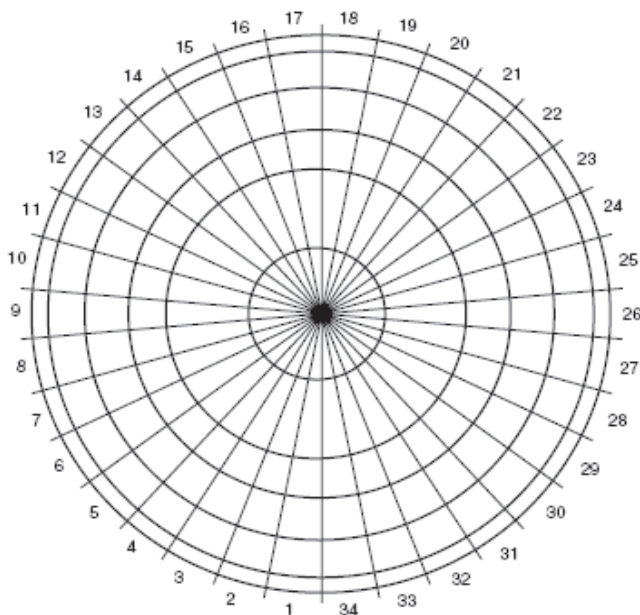


Рис. 8.10. Круговая диаграмма для отображения результатов оценивания

Каждый групповой показатель включает частные показатели, к которым применяются соответствующие оценочные шкалы, представленные в разделе 6 Методики оценки соответствия СТО БР ИББС-1.2. По решению оценщика может быть выбрана любая из трех шкал оценки для частных показателей ИБ Методики оценки соответствия СТО БР ИББС-1.2, отражающих как характер соответствующих свидетельств оценки ИБ, так и возможные цели оценки.

В том случае, если оценивается как степень документированности, так и степень выполнения, рекомендуется использовать следующий общий подход («универсальная шкала»).

| Оценка частного показателя ИБ | Критерий выставления оценки частного показателя ИБ |
|-------------------------------|--|
| 0 | Требования частного показателя ИБ не установлены во внутренних нормативных документах проверяемой организации и не выполняются |
| 0 | Требования частного показателя ИБ частично установлены в нормативных документах проверяемой организации, но не выполняются |
| 0,25 | Требования частного показателя ИБ полностью установлены в нормативных документах проверяемой организации, но не выполняются |

Окончание

| Оценка частного показателя ИБ | Критерий выставления оценки частного показателя ИБ |
|-------------------------------|--|
| 0,25 | Требования частного показателя ИБ не установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме |
| 0,25 | Требования частного показателя ИБ частично установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме |
| 0,5 | Требования частного показателя ИБ полностью установлены во внутренних нормативных документах проверяемой организации и выполняются в неполном объеме |
| 0,5 | Требования частного показателя ИБ не установлены во внутренних нормативных документах проверяемой организации, но выполняются в полном объеме |
| 0,75 | Требования частного показателя ИБ частично установлены во внутренних нормативных документах проверяемой организации, но выполняются в полном объеме |
| 1 | Требования частного показателя ИБ полностью установлены во внутренних нормативных документах проверяемой организации и выполняются в полном объеме |

При проведении оценки частных показателей, для которых оценивается только степень документированности, рекомендуется использовать следующий общий подход («документарная шкала»).

| Оценка частного показателя ИБ | Критерий выставления оценки частного показателя ИБ |
|-------------------------------|---|
| 0 | Требования частного показателя ИБ не установлены во внутренних нормативных документах проверяемой организации |
| 0,5 | Требования частного показателя ИБ частично установлены в нормативных документах проверяемой организации |
| 1 | Требования частного показателя ИБ полностью установлены в нормативных документах проверяемой организации |

При проведении оценки частных показателей, для которых оценивается только степень выполнения, рекомендуется использовать следующий общий подход («реализационная шкала»).

| Оценка частного показателя ИБ | Критерий выставления оценки частного показателя ИБ |
|-------------------------------|--|
| 0 | Требования частного показателя ИБ не выполняются |

Окончание

| | |
|-------------------------------|---|
| Оценка частного показателя ИБ | Критерий выставления оценки частного показателя ИБ |
| 0,5 | Требования частного показателя ИБ выполняются в неполном объеме |
| 1 | Требования частного показателя ИБ выполняются в полном объеме |

Полученные свидетельства оценки ИБ и источники их получения должны быть документально закреплены путем составления листов для сбора свидетельств оценки. Примером такого документа может являться следующая форма.

| Обозначение частного показателя ИБ | Источники свидетельств и свидетельства самооценки ИБ (документы, результаты опроса или наблюдений) | Кем предоставлены свидетельства самооценки ИБ | Подпись сотрудника (руководителя) | Дата |
|------------------------------------|--|---|-----------------------------------|------|
| | | | | |
| | | | | |
| | | | | |

При заполнении листов для сбора свидетельств оценки ИБ необходимо указать ссылки на соответствующие внутренние нормативные документы организации, результаты опроса сотрудников организации, а также результаты наблюдений членов группы аудита. Результаты опроса и наблюдений должны быть подтверждены подписью опрашиваемого сотрудника и члена группы оценки.

Состав частных показателей для каждого из 34 групповых показателей представлен в приложении А СТО БР ИББС-1.2. Формируемые оценщиком значения оценки для соответствующих частных показателей подлежат нормированию на основе приложения В Методики СТО БР ИББС-1.2 на коэффициенты, получаемые с использованием специализированной дополнительной шкалы раздела 10 Методики оценки соответствия. Данное приложение В Методики оценки соответствия СТО БР ИББС-1.2 есть инструмент учета требований законодательства в части защиты персональных данных. Не все частные показатели подлежат коррекции, а лишь те, что указаны в табл. 1 приложения В.

Каждый частный показатель оценки соответствия имеет отображение на требования стандарта СТО БР ИББС-1.0.

Каждое из требований стандарта рассматривает некоторую «сущность», которая должна быть определена (разработана, внедрена, использована, контролируема) и т.п. Причем могут быть различные комбинации:

- одно требование — одна «сущность» ;
- одно требование — несколько «сущностей» ;
- несколько требований — одна «сущность» и др.

Каждый из частных показателей Методики оценки предназначен для анализа той или иной «сущности» и (или) ее свойств, требования к которым установлены в одном пункте или нескольких пунктах требований стандарта СТО БР ИББС-1.0.

На рисунке 8.11 показаны различные сочетания отношений между требованиями СТО БР ИББС-1.0 и частными показателями методики оценки СТО БР ИББС-1.2.

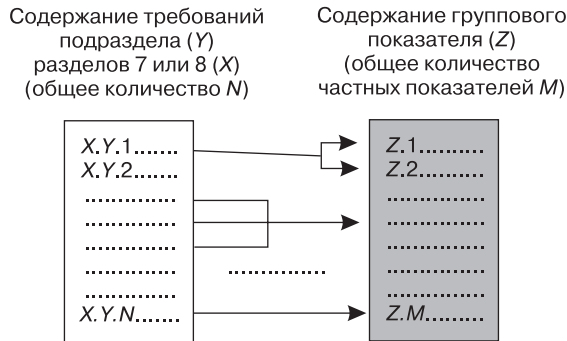


Рис. 8.11. Соответствие требований показателям оценки

Общий подход Методики оценки СТО БР ИББС-1.2 к формированию значе- ний оценки соответствия иллюстрирует рис. 8.12.

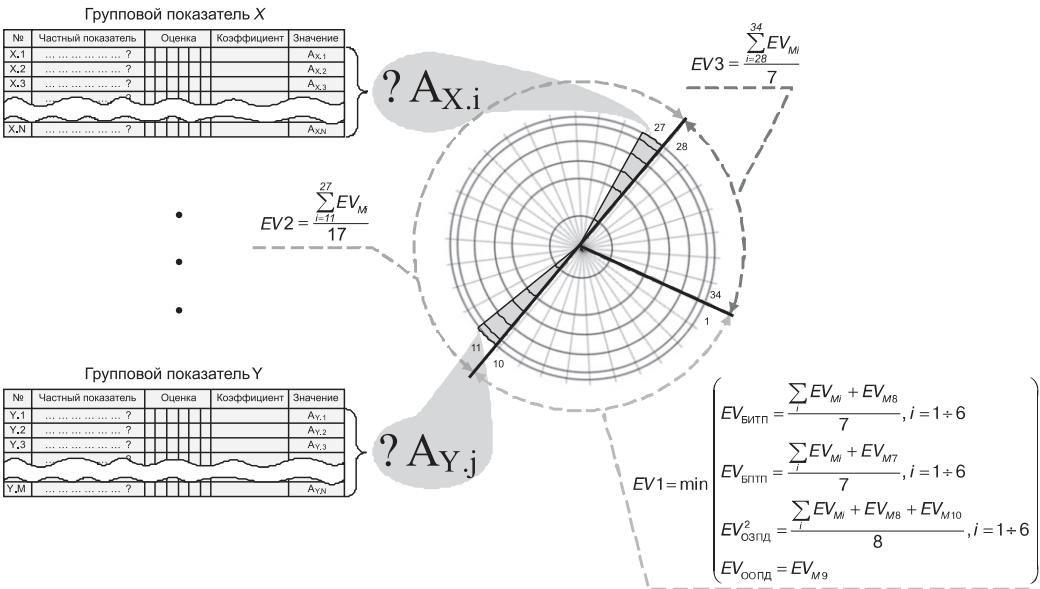


Рис. 8.12. Модель формирования значения оценок соответствия ИБ стандарта СТО БР ИББС-1.2

Рекомендации в области стандартизации Банка России РС БР ИББС-2.0 включают рекомендации к структуре, составу, назначению и содержанию внутренних документов по обеспечению ИБ организаций БС РФ в соответствии с требованиями стандарта Банка России СТО БР ИББС-1.0. Документы по обеспечению ИБ позволяют определить и довести до каждого работника правила и требования по обеспечению ИБ, которыми он должен руководствоваться в своей производственной деятельности, а также определить порядок контроля их соблюдения. Иерархия структуры внутренних документов организации БС РФ по обеспечению ИБ, рекомендуемая положениями РС БР ИББС-2.0, представлена на рис. 8.13.



Рис. 8.13. Структура внутренних документов организации БС РФ по обеспечению ИБ

Рекомендации в области стандартизации Банка России РС БР ИББС-2.1 распространяются на организации БС РФ, проводящие самооценку соответствия ИБ требованиям СТО БР ИББС-1.0, и устанавливают порядок проведения указанной самооценки ИБ. Самооценка соответствия информационной безопасности организации БС РФ требованиям СТО БР ИББС-1.0 должна проводиться в соответствии со стандартом Банка России СТО БР ИББС-1.2.

Рекомендации в области стандартизации Банка России РС БР ИББС-2.2 используются для проведения оценки рисков нарушения ИБ в рамках построения (совершенствования) СОИБ в соответствии с требованиями СТО БР ИББС-1.0.

В данной Методике определены способы и порядок проведения оценки рисков нарушения ИБ организации БС РФ. Положения Методики могут быть использованы для целей внутреннего контроля организаций БС РФ.

Порядок использования оценки рисков нарушения ИБ в рамках построения (совершенствования) СОИБ в соответствии с требованиями СТО БР ИББС-1.0 в организациях БС РФ представлен на рис. 8.14.

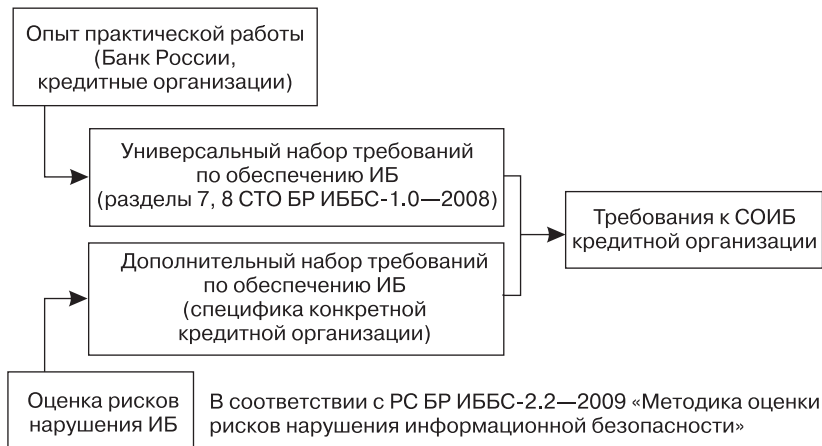


Рис. 8.14. Порядок использования результатов оценки рисков нарушения ИБ в организациях БС РФ

Рекомендации в области стандартизации Банка России РС БР ИББС-2.3 распространяются на организации БС РФ, реализующие требования стандарта СТО БР ИББС-1.0 в части обеспечения безопасности персональных данных, при построении (совершенствовании) СОИБ организации БС РФ.

В настоящем документе определены требования по обеспечению безопасности персональных данных, выполнение которых способствует реализации в организациях БС РФ требований СТО БР ИББС-1.0. Выполнение установленных требований обеспечивает нейтрализацию актуальных для организаций БС РФ угроз безопасности персональных данных, содержащихся в рекомендациях в области стандартизации Банка России РС БР ИББС-2.4 «Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций БС РФ».

РС БР ИББС-2.3 используется для составления детализации и конкретизации вопросов частных показателей СТО БР ИББС-1.2 в части банковских технологических процессов, в рамках которых обрабатываются персональные данные. Перечень указанных детализирующих и конкретизирующих вопросов, а также подход к проведению оценок соответствия ИБ содержатся в СТО БР ИББС-1.2.

Рекомендации в области стандартизации Банка России РС БР ИББС-2.4 распространяются на организации БС РФ и содержат актуальные для большинства организаций БС РФ угрозы безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн).

Документом устанавливаются общие подходы и исходные данные к составлению отраслевой модели угроз, а также отраслевая модель угроз безопасности персональных данных, представленная в виде таблицы. Данная отраслевая частная модель угроз безопасности персональных данных при их обработке в инфор-

мационных системах персональных данных организаций БС РФ содержит актуальные для большинства организаций БС РФ угрозы безопасности персональных данных при их обработке в ИСПДн. Актуальные угрозы определены в результате проведения оценки рисков в соответствии с рекомендациями в области стандартизации Банка России РС БР ИББС-2.2.

Назначение и практику применения комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» иллюстрирует рис. 8.15.

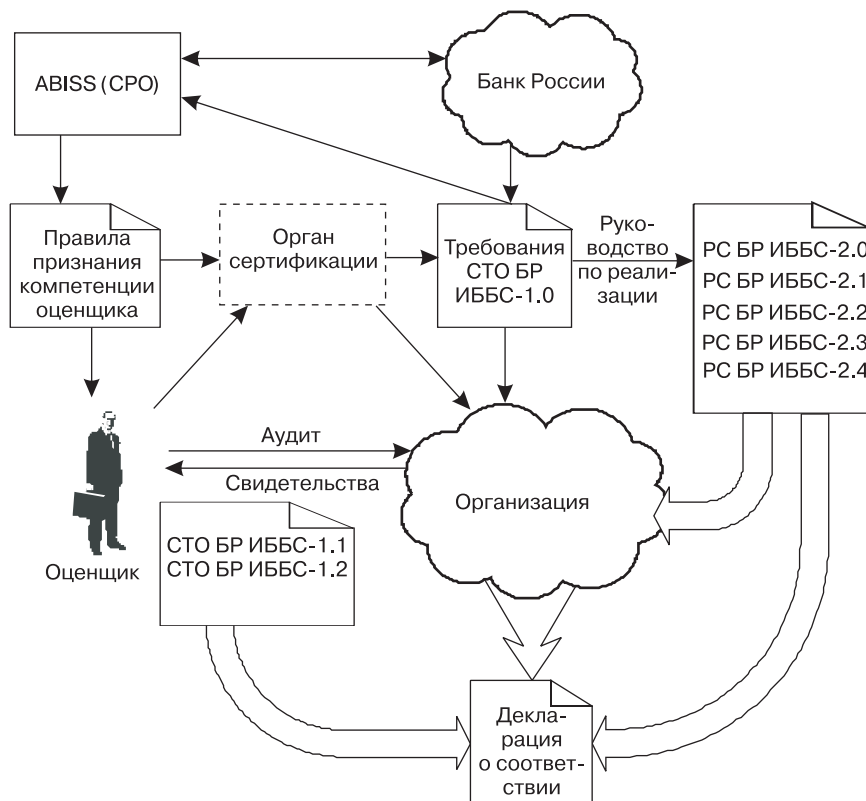


Рис. 8.15. Назначение и практика использования документов по стандартизации Банка России

Заявление о соответствии стандартам СТО БР ИББС предполагает, что:

- СОИБ банка (в идеале — всего банка, включая как головную организацию, так и все структурные и обособленные подразделения) отвечает требованиям базового стандарта СТО БР ИББС-1.0 (в актуальной его редакции);
- результат соответствия стандартам СТО БР ИББС оформлен в соответствии с требованиями СТО БР ИББС-1.2;

- процесс оценки соответствия СТО БР ИББС осуществлялся в соответствии с требованиями СТО БР ИББС — 1.1 для аудита ИБ и в соответствии с РС БР ИББС-2.1 для самооценки ИБ;
- при аудите ИБ аудитор (аудиторская группа) являлся сотрудником организации, являющейся полномочным членом ABISS (рекомендация Банка России).

Процедуры аудита ИБ, нашедшие отражение в СТО БР ИББС-1.1, базируются на международных рекомендациях по аудиту управленческих систем (систем менеджмента), включая требования ГОСТ Р ИСО 19011—2003.

Нижеследующая таблица иллюстрирует соответствие процесса аудита по требованиям стандарта Банка России и международного стандарта аудита СМИБ ISO/IEC 27007 в контексте требований универсального международного стандарта по аудиту систем менеджмента.

| № п/п | ГОСТ Р ИСО 19011 | СТО БР ИББС-1.1 | ISO/IEC 27007 |
|-------|---|---|--|
| 1 | <p>6.2. Организация проведения аудита включает следующее:</p> <ul style="list-style-type: none"> ■ назначение руководителя аудиторской группы (п. 6.2.1); ■ определение целей, области и критериев аудита (п. 6.2.2); ■ определение возможности проведения аудита (п. 6.2.3); ■ формирование аудиторской группы (п. 6.2.4); ■ установление первоначального контакта с проверяемой организацией (п. 6.2.5) | <p>7.2.2. Подготовка к проведению аудита ИБ:</p> <ul style="list-style-type: none"> ■ согласования и заключения договора на проведение аудита ИБ (п. 7.2.2); ■ назначение руководителя аудиторской группы (п. 7.2.2); ■ определение возможности проведения аудита ИБ (п. 7.2.3); ■ формирование аудиторской группы (п. 7.2.4), ■ установление руководителем аудиторской группы контакта с проверяемой организацией (п. 7.2.5) | <p>6.2. Организация проведения аудита:</p> <ul style="list-style-type: none"> ■ определение целей, области и критериев аудита (п. 6.2.1); ■ определение методов аудита (п. 6.2.2); ■ формирование аудиторской группы (п. 6.2.3); ■ установление первоначального контакта с проверяемой организацией (п. 6.2.4); ■ определение возможности проведения аудита (п. 6.2.5) |
| 2 | 6.3. Анализ документов | 7.2.6. Анализ документов | <i>Нет требований</i> |
| 3 | <p>6.4. Подготовка к проведению аудита на месте:</p> <ul style="list-style-type: none"> ■ подготовка плана аудита (п. 6.4.1); ■ распределение работ между членами аудиторской группы (п. 6.4.2); ■ подготовка рабочих документов (п. 6.4.3) | <p>7.2.7. Подготовка к проведению аудита на месте:</p> <ul style="list-style-type: none"> ■ подготовка и согласование плана аудита ИБ на месте. <p><i>(Данный этап отсутствует в перечне этапов аудита ИБ — п. 7.2.1)</i></p> | <p>6.3. Подготовка к проведению аудита:</p> <ul style="list-style-type: none"> ■ подготовка плана аудита (п. 6.3.1); ■ распределение работ между членами аудиторской группы (п. 6.3.2); ■ подготовка рабочих документов (п. 6.3.3) |

Окончание

| № п/п | ГОСТ Р ИСО 19011 | СТО БР ИББС-1.1 | ISO/IEC 27007 |
|-------|--|--|---|
| 4 | 6.5. Проведение аудита на месте: <ul style="list-style-type: none"> ■ проведение предварительного совещания (п. 6.5.1); ■ обмен информацией в ходе аудита (п. 6.5.2); ■ роль и обязанности сопровождающих лиц и наблюдателей (п. 6.5.3); ■ сбор и верификация информации (п. 6.5.4); ■ формирование выводов аудита (п. 6.5.5); ■ подготовка заключения по результатам аудита (п. 6.5.6); ■ проведение заключительного совещания (п. 6.5.7) | 7.2.8. Проведение аудита ИБ на месте: <ul style="list-style-type: none"> ■ проведение вступительного совещания (п. 7.2.9); ■ сбор дополнительных свидетельств аудита ИБ (п. 7.2.10 и 7.2.11); ■ оценка свидетельств аудита ИБ (п. 7.2.12); ■ подготовка заключения по результатам аудита ИБ (п. 7.2.13 и 7.2.14); ■ проведение заключительного совещания (п. 7.2.15) | 6.4. Проведение аудита: <ul style="list-style-type: none"> ■ проведение анализа (изучения) документов (п. 6.4.1); ■ проведение предварительного совещания (п. 6.4.2); ■ обмен информацией в ходе аудита (п. 6.4.3); ■ роль и обязанности сопровождающих лиц и наблюдателей (п. 6.4.4); ■ сбор и верификация информации (п. 6.4.5); ■ формирование выводов аудита (п. 6.4.6); ■ подготовка заключения по результатам аудита (п. 6.4.7); ■ проведение заключительного совещания (п. 6.4.8) |
| 5 | 6.6. Подготовка, утверждение и рассылка отчета (акта) по аудиту: <ul style="list-style-type: none"> ■ подготовка отчета (акта) по аудиту (п. 6.6.1); ■ утверждение и рассылка отчета (акта) по аудиту (п. 6.6.2) | 7.2.16. Подготовка, утверждение и рассылка отчета по аудиту ИБ | 6.5. Подготовка, утверждение и рассылка отчета (акта) по аудиту: <ul style="list-style-type: none"> ■ подготовка отчета (акта) по аудиту (п. 6.5.1); ■ утверждение и рассылка отчета (акта) по аудиту (п. 6.5.2) |
| 6 | 6.7. Завершение аудита | Завершение аудита ИБ | 6.6. Завершение аудита |
| 7 | 6.8. Действия по результатам аудита | Определяется заказчиком аудита | 6.7. Действия по результатам аудита |

По составу этапов аудита СМИБ и содержанию выполняемых на этих этапах работ ISO/IEC 27007 и СТО БР ИББС-1.1 практически аналогичны.

На 2010 год формальной системы оценки соответствия, которая бы обеспечивала поддержку норм аккредитации оценщиков, осуществляла бы контроль качества оценки соответствия и функции сертификации по требованиям стандартов Банка России, не учреждено.

Ее аналогом является Сообщество ABISS (см. http://www.cbr.ru/credit/Gubzi_docs/ и <http://www.abiss.ru/>).

Целью деятельности Сообщества ABISS является содействие развитию и широкому практическому применению единых стандартов (стандартов СТО БР ИББС), повышению уровня информационной безопасности организаций финансового сектора и содействию стабильности кредитно-финансовой системы Российской Федерации в целом.

Задачами Сообщества ABISS являются:

- пропагандировать и распространять стандарт (СТО БР ИББС-1.0);
- способствовать внедрению положений стандарта в кредитных организациях;
- обмениваться накопленным опытом
- консолидировать и анализировать обобщенный опыт внедрения для доработки стандарта и разработки новых стандартов;
- повышать уровень осведомленности организаций кредитно-финансовой системы Российской Федерации по вопросам информационной безопасности;
- способствовать повышению качества услуг, связанных с внедрением стандартов и оценкой соответствия требованиям стандартов, включая:
 - проведение разъяснительной работы по недопущению искаженного толкования и использования стандартов,
 - разработку квалификационных требований к организациям, выполняющим аудит (оценку) соответствия кредитно-финансовых институтов требованиям стандартов;
 - способствовать единому подходу.

СТАНДАРТЫ БЕЗОПАСНОСТИ ИНДУСТРИИ ПЛАТЕЖНЫХ КАРТ PCI DSS

Стандарт PCI DSS был разработан в 2004 г. как единый набор требований к безопасности для объектов, эксплуатирующихся в организациях и участвующих в операциях с использованием платежных карт. Он объединил в себе требования ряда программ по безопасности таких платежных систем, как Visa Int., MasterCard, American Express, Discover Card и JCB. Это достаточно логичный шаг. Многие операторы и эмитенты платежных карт поддерживают обслуживание в нескольких платежных системах.

Для развития и продвижения стандарта PCI DSS в 2006 г. был образован специальный Совет по безопасности — PCI Security Standards Council (<https://www.pcisecuritystandards.org>).

Основными функциями данного Совета по безопасности являются:

- разработка и публикация стандартов PCI и всей сопутствующей документации;
- определение требований к компаниям, планирующим получить аккредитацию (сертификат компетенции) для проведения аудитов по PCI DSS (Qualified Security Assessor — QSA) и сканирований (Approved Scanning Vendors — ASV), осуществление непосредственно самой сертификации;

- проведение обучающих тренингов для будущих QSA-аудиторов;
- осуществление контроля качества проведенных аудиторами работ.

В свою очередь международные платежные системы принимают отчетность по результатам аудитов и оценивают работу QSA.

Действие стандарта PCI DSS распространяется на все торгово-сервисные предприятия и поставщиков услуг, работающих с международными платежными системами, т.е. на всех тех, кто передает, обрабатывает и хранит данные держателей карт.

Также в зависимости от количества обрабатываемых транзакций каждой платежной системой компании присваивается определенный уровень с соответствующим набором требований, которые должны выполняться в обязательном порядке. Это может быть ежегодное прохождение аудита, ежеквартальные сканирования сети или ежегодное заполнение листа самооценки (Self Assessment Questionnaire — специальная анкета, разработанная PCI SSC для самооценки компаний).

Непрохождение компаниями обязательной ежегодной процедуры аудита может повлечь за собой штрафные санкции со стороны международных платежных систем. Невыполнение требований стандарта PCI DSS может также привести к значительным убыткам в случае возникновения утечки данных платежных карт, связанным с возмещением затрат на перевыпуск платежных карт всех банков, клиенты которых пострадали или могли пострадать в результате утечки данных.

Основными этапами по проведению аудита на соответствие требованиям PCI DSS, как правило, являются следующие:

- подготовка и планирование аудита PCI DSS;
- проведение проверок согласно утвержденным процедурам аудита PCI DSS;
- анализ результатов, формирование предварительного отчета о соответствии требованиям стандарта PCI DSS;
- представление сотрудникам компании предварительного отчета аудитора о соответствии требованиям стандарта PCI DSS;
- согласование с сотрудниками компании отчета и формирование окончательного отчета по результатам аудита PCI DSS, включая подготовку при необходимости плана устранения недостатков (формирование документа Action plan);
- уведомление администрации международной платежной системы о результатах аудита по требованиям PCI DSS в данной компании.

При вынесении аудитором вердикта о соответствии в администрацию международной платежной системы направляется результат проведения аудита и английская версия отчета.

При заключении аудитором о несоответствии в администрацию международной платежной системы направляется Action plan.

Аудит, согласно требованиям PCI DSS, производится по следующим 12 направлениям, сгруппированным в шесть тематических блоков:

I. Построение и поддержка безопасности сети:

- 1) наличие межсетевых экранов для защиты данных и актуальность их конфигурации;
- 2) отсутствие настроек безопасности и паролей по умолчанию оборудования и программного обеспечения.

II. Защита данных держателей карт:

- 3) обеспечение защиты хранящихся данных;
- 4) обеспечение шифрования данных владельцев карт и других важных данных при их передаче через общедоступные сети.

III. Поддержка программы управления уязвимостями:

- 5) использование и регулярное обновление антивирусного программного обеспечения;
- 6) разработка и поддержка безопасности систем и приложений.

IV. Реализация мер по строгому контролю доступа:

- 7) разграничение доступа к данным по принципу минимальной достаточности;
- 8) присвоение уникальных идентификаторов всем пользователям;
- 9) ограничение физического доступа к данным держателей карт.

V. Регулярный мониторинг и тестирование сетей:

- 10) отслеживание всех сеансов доступа к сетевым ресурсам и данным владельцев карт;
- 11) проведение периодического анализа процессов обеспечения безопасности и журналов средств информационной безопасности.

VI. Поддержка политики информационной безопасности:

- 12) наличие и исполнение политики информационной безопасности.

В отличие от стандартов СТО БР ИББС и ISO/IEC 27001 требованиями PCI DSS предусмотрены сканирование и тестирование на проникновение как при проведении оценки соответствия PCI DSS, так и далее на регулярной основе (сканирование раз в квартал, тестирование раз в год) с соответствующими записями в регистрационных журналах.

Сканирование по стандарту PCI DSS

Разработчики стандарта PCI DSS исходили из того, что регулярное сканирование сети должно позволить идентифицировать уязвимости и некорректные с точки зрения безопасности конфигурации элементов ИТ-инфраструктуры. При этом результаты сканирования должны обеспечить эффективное управление безопасностью и защиту от атак из Интернета. Необходимость регулярного сканирования сети отражена в требовании 11.2 стандарта PCI DSS, и все члены платежных систем, как отмечалось ранее, должны ежеквартально проходить процедуру сканирования сети. Порядок осуществления процедуры сканирования установлен в документе PCI Scanning Procedures.

Тест на проникновение по стандарту PCI DSS

Тестирование на проникновение по требованиям стандарта PCI DSS преследует цель определение того, насколько защищена корпоративная инфраструктура от действий потенциального злоумышленника. Эта необходимость отражена в обязательных требованиях подраздела 11.3 стандарта PCI DSS. Формулировка требований следующая: «По крайней мере ежегодно, а также после любых значительных улучшений или модификаций инфраструктуры или приложений (например, обновлении версии операционной системы, добавления подсети или web-сервера) должны проводиться внешние и внутренние тесты на проникновение...». Требованиями подраздела 11.3 стандарта PCI DSS предусмотрены два вида тестирования на проникновение: на уровне сети (п. 11.3.1) и на уровне приложений (п. 11.3.2). Не имитируются атаки типа «отказ в обслуживании».

Требования стандарта PCI DSS актуальны:

- для банков, располагающих своим (внутренним) процессинговым центром платежных систем;
- отдельных процессинговых центров;
- сервис-провайдеров;
- провайдеров электронного бизнеса (e-commerce);
- телекоммуникационных компаний;
- торгово-сервисных организаций;
- других организаций, деятельность которых связана с обработкой данных платежных карт и на которых распространяются требования стандарта PCI DSS.

Когда организация заявляет о соответствии стандарту PCI DSS, то это предполагает, что:

- в организации выполнены требования стандарта PCI DSS применительно к объекту, обрабатывающему данные пользователей платежных карт таких платежных систем, как Visa Int., MasterCard, American Express, Discover Card и JCB;
- результат соответствия стандарту PCI DSS оформлен в соответствии с требованиями руководящих документов Совета по безопасности платежной индустрии;
- процесс оценки соответствия PCI DSS осуществляется в соответствии с требованиями к процессу аудита, установленными в руководящих документах Совета по безопасности платежной индустрии;
- аудитор (аудиторская группа) являлись лицами, аккредитованными в соответствии с требованиями руководящих документов Совета по безопасности платежной индустрии.

Все основные процедурные и методические аспекты лежат в плоскости компетенции учредителей систем оценки соответствия и сертификации — Совета по безопасности платежной индустрии.

8.4. ОРГАНИЗАЦИОННАЯ ОСНОВА БЕЗОПАСНОСТИ И НАДЕЖНОСТИ НПС

Завершая краткое изложение проблемы обеспечения информационной безопасности в национальной платежной системе, приведенное в данной главе, необходимо указать на значимые факторы (видимо, они окажутся решающими) в практической работе по обеспечению информационной безопасности НПС.

Первым таким фактором является методологическая платформа и практика, наработанная Банком России — регулятором национальной банковской системы и НПС. Она хорошо систематизирована, развивается (содержит механизмы пересмотра и совершенствования) и вполне адекватна для операторов и других участников НПС.

На рисунке 8.16 представлена схема организационной основы выработки и реализации технологий обеспечения информационной безопасности для НПС (участники НПС, органы регулирования и безопасности). Она также иллюстрирует тот факт, что в практике платежных технологий присутствуют две значимые зоны, требующие особого внимания, которые определяют уровень доверия и безопасности в НПС — «клиент — система (участник НПС)» и «участник — участник НПС».

Эти зоны сопряжены со специфичными рисками. Надежность и безопасность протоколов доступа к финансовым услугам напрямую связаны с доверием к системе платежей. Все это актуально и для внутрисистемных операций, надежность и безопасность которых влияет на структуру рисков НПС и рисков пользователей системы.

Вторым фактором является платформа и практика мирового, и прежде всего европейского, пространства. В пользу этого фактора можно привести те обстоятельства, что значительная часть технологий, видимо, будет заимствована, а также очевидная необходимость унификации как минимум на уровне рабочих инструментов и содержания практических шагов (направлений деятельности и регулирования).

На рисунке 8.17 представлена схема управляющей структуры Европейского платежного совета (ЕПС) единого европейского платежного пространства (Single Euro Payments Area — SEPA). На членов ЕПС приходится до 95% платежей в зоне евро.

В составе рабочих групп Совета фактически отражены основные направления его работ, а также принципы взаимодействия причастных сторон и принятия решений.

Вопрос, следовательно, сводится к творческому осмыслению этих факторов в контексте их практической реализации в НПС.

Это сложная, интересная, важная и очень объемная задача.

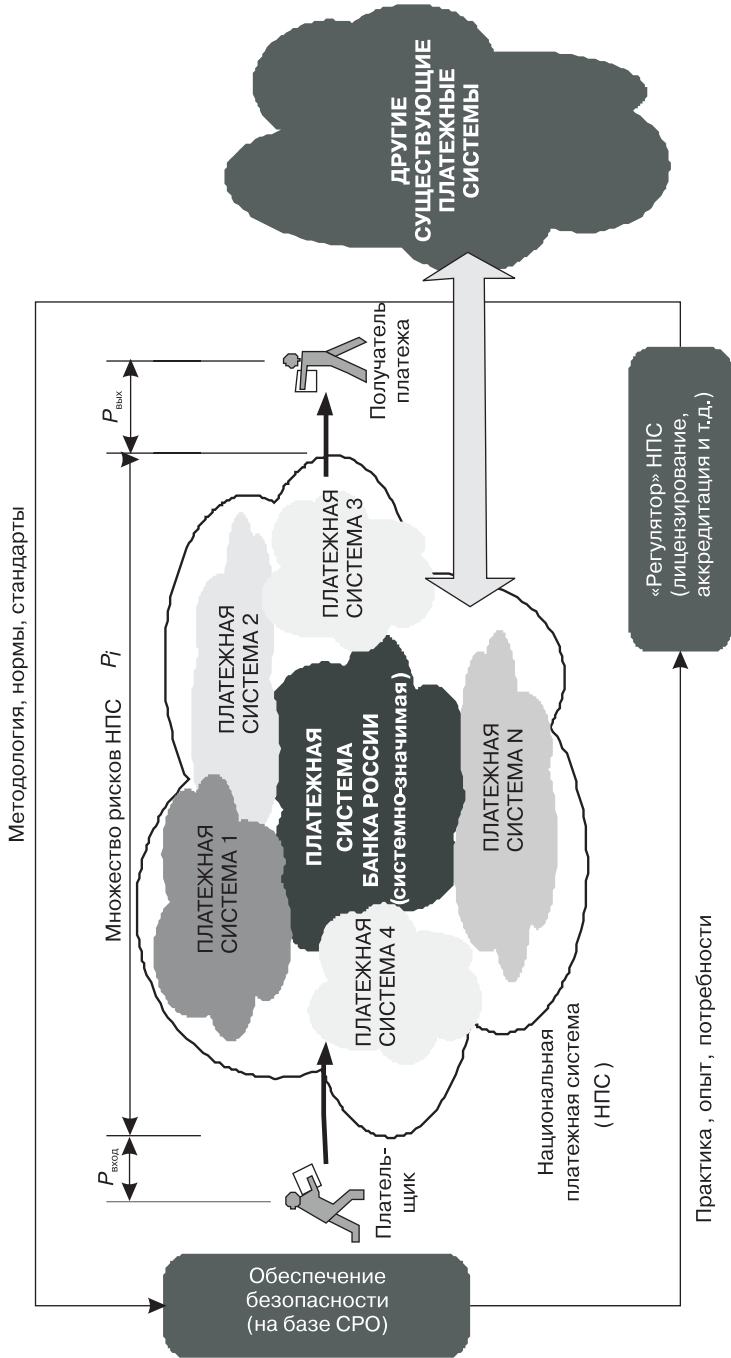


Рис. 8.16. Организационная основа обеспечения ИБ в НПС

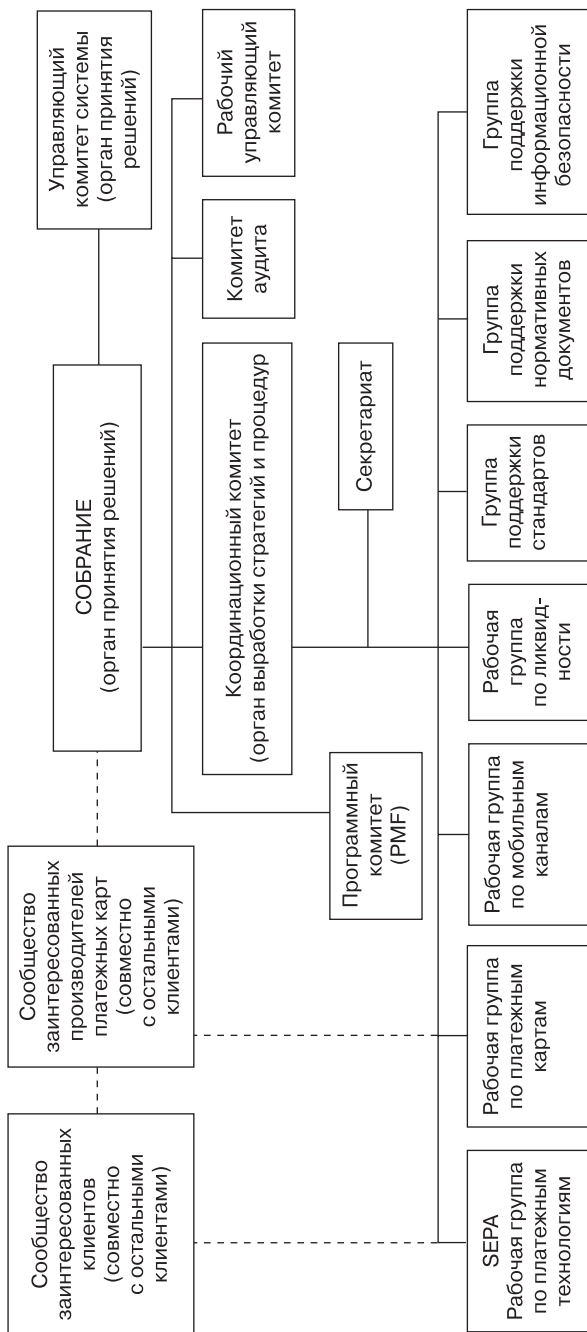


Рис. 8.17. Организационная основа Европейского платежного совета

ГЛАВА 9

ТЕХНОЛОГИИ АУТЕНТИФИКАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЛАТЕЖЕЙ

Предоставление государственных услуг в электронном виде подразумевает возможность достаточно простого, удобного для пользователя и безопасного способа оплаты этих услуг. Вместе с тем на примере развития банковских платежных систем (в частности, систем дистанционного банковского обслуживания, ДБО), видно, что данные системы все чаще подвергаются различного рода атакам. К сожалению, не слишком малая доля таких атак бывает успешной. Например, согласно данным, опубликованным в специальной литературе¹, на каждые 100 дол. оборота потери по банковским операциям с пластиковыми картами в последние десять лет в среднем составляют от 7 до 11 центов (для сравнения — потери банков, связанные с кредитованием клиентов, в среднем в 2 раза меньше). Это является сдерживающим фактором развития электронных платежных систем и существенно снижает уровень доверия пользователей.

Попробуем кратко проанализировать основные применяемые в настоящее время сервисы безопасности в электронных платежных системах с точки зрения выполнения требований информационной безопасности (ИБ).

Стандарт Банка России СТО БР ИББС-1.0—2010 (далее — Стандарт) в п. 7.1.8 рекомендует при принятии руководством банковской системы решения об использовании Интернета и подготовке регламентирующих документов учитывать следующие положения:

- Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) Интернета могут обеспечить только услуги, которые ими реализуются;
- существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством Интернета;

¹ Бизнес-энциклопедия «Платежные карты». М. : Центр исследований платежных систем и расчетов» (ЦИПСИР), 2008.

- существует вероятность атаки злоумышленников на оборудование, программное обеспечение и информационные ресурсы, подключенные (доступные) из сети Интернет;
- гарантии по обеспечению ИБ при использовании Интернета никаким органом (учреждением, организацией) не предоставляются.

Заметим, что в отличие от хорошо изученных корпоративных информационных систем (ИС), участниками электронного взаимодействия в которых является определенный круг лиц, в последние годы интенсивно развивается новый тип ИС — информационные системы общего пользования (ИСОП), «участниками электронного взаимодействия в которых является неопределенный круг лиц и в использовании которых этим лицам не может быть отказано» (п. 13 ст. 2 Федерального закона от 7 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее — Закон об электронной подписи)). В настоящее время размеры ИСОП, число их участников могут достигать гигантских размеров (один из самых очевидных примеров таких систем — Интернет). В отличие от Интернета, где изначально был реализован принцип анонимности пользователя, в большинстве ИСОП (системы электронной коммерции, государственных услуг для граждан и организаций и т.д.), за исключением случаев информирования (получения открытой информации), необходимо обеспечение надежных механизмов управления доступом пользователей системы. Решение данной задачи невозможно без применения средств автоматической идентификации — процедуры распознавания субъекта по его уникальному идентификатору, присвоенному данному субъекту ранее и занесенному в базу данных в момент регистрации субъекта в качестве легального пользователя системы. Если в системе обрабатывается и хранится информация ограниченного доступа (банковская тайна, персональные данные), то доступ пользователей должен быть минимально достаточен и строго персонифицирован, следовательно, необходимо использовать надежные средства удаленной аутентификации — комплекса процедур проверки подлинности входящего в систему объекта, предъявившего свой идентификатор. Поскольку банковские системы в отличие от ИСОП всегда были закрытыми (корпоративными), то предстоит большая организационная работа, необходимы изменения в нормативной базе и дополнительные технические средства для того, чтобы пользователи ИСОП могли присоединяться к банковским системам для оплаты, например, государственных услуг.

В большинстве случаев проверка состоит в процедуре обмена между входящим в систему объектом и ресурсом, отвечающим за принятие решения («да» или «нет»). Данная проверка, как правило, производится с применением криптографических преобразований, которые нужны, с одной стороны, для того, чтобы достоверно убедиться в том, что субъект является тем, за кого себя выдает, с другой — для защиты трафика обмена «субъект — система» от злоумышленника. Таким образом, идентификация и аутентификация как сервисы безопасности являются взаимосвязанными процессами распознавания и проверки подлинно-

сти пользователей. Именно от корректности решения этих двух задач (распознавания и проверки подлинности) зависит, можно ли разрешить доступ к ресурсам системы конкретному пользователю, т.е. будет ли он авторизован. Данному вопросу уделяется повышенное внимание и в руководящих документах. Так, стандарт в разделе 7.6 определяет следующие требования по обеспечению ИБ при использовании банковской системой ресурсов Интернета:

- решение об использовании Интернета должно документально приниматься руководством организации банковской системы для определенных целей, например, для ведения дистанционного банковского обслуживания (ДБО);
- для ограничения использования Интернета в неустановленных целях рекомендуется документально выделить ограниченное число пакетов, содержащих перечень сервисов и ресурсов Интернета, доступных пользователям (сотрудникам банка) в соответствии с их должностными обязанностями и ролями;
- в организациях банковской системы, осуществляющих ДБО клиентов, в связи с повышенными рисками нарушения ИБ при взаимодействии с Интернетом должны применяться средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии;
- рекомендуется выполнить выделение и организовать физическую изоляцию от внутренних сетей тех компьютеров, с помощью которых осуществляется взаимодействие с Интернетом в режиме онлайн;
- при осуществлении ДБО должны применяться защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы; все попытки таких подмен должны регистрироваться регламентированным образом;
- все операции клиентов в течение всего сеанса работы с системами ДБО должны выполняться только после выполнения процедур идентификации, аутентификации и авторизации, в случаях нарушения или разрыва соединения необходимо обеспечить повторное выполнение указанных процедур.

Поскольку последний из перечисленных пунктов в конкретных реализациях всегда вызывает много вопросов, остановимся на вопросах идентификации и аутентификации более подробно.

9.1. ВОПРОСЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

Аббревиатура AAA или 3A (authentication, authorization, accounting — аутентификация, авторизация, учет и аудит) ассоциируется с одним из ключевых средств обеспечения безопасности. Среди этих средств центральное место за-

нимают системы идентификации и аутентификации или, в терминологии ГОСТ Р 51241-98, устройства ввода идентификационных признаков, предназначенные для обеспечения защиты от несанкционированного доступа к компьютерам.

Вопросам идентификации и аутентификации как одним из самых важных для обеспечения ИБ уделяется внимание во многих статьях стандарта.

ААА И ВНУТРЕННИЕ УГРОЗЫ

Интерес к ААА вызван более глубоким осмыслением проблем безопасности и общим движением отрасли и технологий защиты от жестких и не всегда обоснованных запретов к контролируемому разделяемому доступу. Чтобы снизить потери от утечек данных, необходимо применять корректное решение задач аутентификации, управления доступом пользователей и аудита их действий. В таком случае говорят, что доступ персонифицирован. Заметим, что персонификация доступа легальных пользователей корпоративных систем при правильном (соответствующем) оформлении нормативно-распорядительной документации предприятия позволяет существенно снизить риски действий внутренних нарушителей — инсайдеров. Безусловно, это сказывается и на снижении рисков внешних атак, поскольку, как указано в п. 5.4 стандарта, «наибольшими возможностями для нарушения безопасности БС РФ обладает ее собственный персонал. В этом случае содержанием деятельности злоумышленника является прямое целевое использование предоставленного ему в порядке выполнения служебных обязанностей контроля над активами либо нерегламентированная деятельность для получения контроля над активами. При этом он будет стремиться к сокрытию следов своей деятельности. Внешний злоумышленник, как правило, имеет сообщника (сообщников) внутри организации БС РФ».

Термин «персонификация» в последние годы употребляется все чаще. Например, в Законе о НПС в ст. 10 вводится понятие персонифицированного средства платежа в случаях полной идентификации клиента — физического лица и размера остатка его электронных денежных средств.

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Важно различать понятия идентификации и аутентификации. При идентификации пользователь распознается системой по некоему установленному идентификационному признаку. Проверка того, что предъявленный идентификатор принадлежит именно его владельцу, осуществляется в процессе аутентификации.

Среди широко применяемых в последние три—пять лет терминов описания процесса идентификации (аутентификации) введено понятие индивидуальных характеристик, доказывающих подлинность субъектов или факторов. К факторам идентификации (аутентификации) относят:

- владение скрытой для посторонних информацией (запоминаемая либо хранящаяся конфиденциальная информация). Примерами могут служить

пароль, персональный идентификационный код (PIN), секретные ключи и т.п.;

- обладание материальным носителем информации (карта с магнитной полосой, электронные ключи классов touch memo и eToken, смарт-карта и т.д.);
- биометрические характеристики субъекта (отпечатки пальцев, голос, геометрия лица, особенности сетчатки и радужной оболочки глаз и т.п.).

РОЛЬ И ВИДЫ АУТЕНТИФИКАЦИИ

В зависимости от используемых в технологиях идентификации и аутентификации факторов различают однофакторную или двухфакторную аутентификацию. Понятие трехфакторной аутентификации в последнее время много обсуждается, однако на практике используется достаточно редко ввиду прозрачности ее целесообразности. Чаще всего для реального противодействия мошенничеству используется второй доверенный канал как средство подтверждения волеизъявления (электронной подписи), в котором также используются средства строгой (двухфакторной) аутентификации. Рассмотрим наиболее развитые методы аутентификации с точки зрения применяемых в них технологий.

ТЕХНОЛОГИИ АУТЕНТИФИКАЦИИ

Для того чтобы понять, что такое AAA и, в частности, аутентификация, обратимся к простому и всем понятному примеру сотового телефона. Для начала работы в телефон необходимо вложить SIM-карту. Когда телефон включается, на дисплее появляется надпись: «Введите PIN-код». После правильного ввода PIN-кода (как правило, это четыре цифры) телефон начинает работать. Налицо так называемая двухфакторная аутентификация. Пользователь должен иметь персональный носитель (SIM-карту) и знать личный PIN-код. Они связаны между собой, причем эта связь закладывается администратором оператора сотовой связи при предпродажной подготовке контрактов с определенным тарифом и самих SIM-карт. Телефонный аппарат в данном случае по аналогии с корпоративными информационными системами играет роль компьютера. Аналогом SIM-карты может являться микропроцессорная смарт-карта, к которой привязан личный PIN-код. Итак, рассмотрим основные методы аутентификации по принципу нарастающей сложности, начиная с самого простого и общеизвестного метода — аутентификации по паролю.

АУТЕНТИФИКАЦИЯ ПО МНОГОРАЗОВЫМ ПАРОЛЯМ

Простейшая схема аутентификации по многоразовому паролю выглядит следующим образом: учетные записи пользователей операционных систем включают в себя службу аутентификации, которая может хранить простейший идентификатор (login) и пароль (password) пользователя в своей базе данных. При

попытке логического входа в сеть пользователь набирает свой пароль, который поступает в службу аутентификации. По итогам сравнения пары login/password с эталонным значением из базы данных учетных записей пользователь может успешно пройти процедуру простейшей аутентификации и авторизоваться в информационной системе. В рамках эволюционного развития протоколов применения многоразовых паролей в операционных системах Windows были реализованы различные по степени защищенности протоколы, такие как LAN Manager (LM), NT LAN Manager (NTLM), NT LAN Manager версии 2 (NTLM v2) и Kerberos, наиболее распространенный и защищенный на сегодня протокол аутентификации в локальных сетях.

ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ ДЛЯ УДАЛЕННОГО ДОСТУПА

Поддержка протокола RADIUS реализована на многих современных платформах, что позволяет использовать его в межплатформенных решениях.

В качестве примера сервера и посредника RADIUS можно привести реализованную в Windows Server 2008 службу NPS (Network Policy Server), которая позиционируется как механизм централизованной аутентификации и авторизации пользователей, использующих различные способы подключений к сети. Служба NPS интегрирована с другими сетевыми службами Windows Server 2008, такими как служба маршрутизации и удаленного доступа и служба каталога Active Directory.

АУТЕНТИФИКАЦИЯ НА ОСНОВЕ ОДНОРАЗОВЫХ ПАРОЛЕЙ

Для организации удаленного доступа пользователей к защищенным информационным ресурсам были разработаны достаточно надежные схемы с применением одноразовых паролей (OTP — One Time Password). Суть концепции одноразовых паролей состоит в использовании различных паролей при каждом новом запросе на предоставление доступа. Одноразовый пароль действителен только для одного входа в систему. Динамический механизм задания пароля является одним из лучших способов защитить процесс парольной аутентификации от внешних угроз. Известно четыре метода аутентификации с применением технологии OTP:

- 1) использование механизма временных меток на основе системы единого времени;
- 2) применение общего пароля для легального пользователя и проверяющего списка случайных паролей и надежного механизма их синхронизации;
- 3) использование общего пароля для пользователя и проверяющего генератора псевдослучайных чисел с одним и тем же начальным значением;
- 4) применение фиксированного числа случайных (псевдослучайных) последовательностей, скопированных на носители в виде скретч-карт.

Наиболее распространены аппаратные реализации генераторов одноразовых паролей, именуемые OTP-токенами. Они имеют небольшой размер и выпускаются в различных форм-факторах:

- карманного калькулятора;
- брелока;
- простейшей смарт-карты;
- устройства, комбинированного с USB-ключом.

В целом технология OTP основана на использовании двухфакторных схем аутентификации и может быть классифицирована как усиленная технология аутентификации (рис. 9.1).

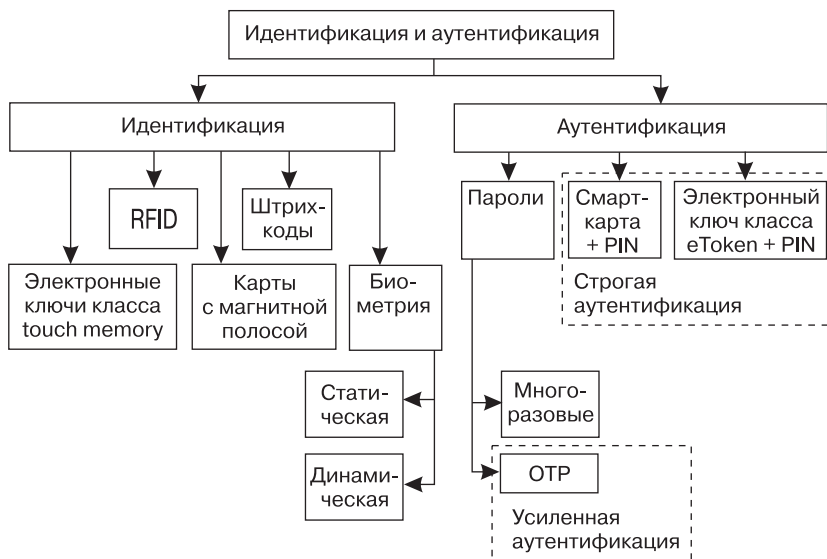


Рис. 9.1. Классификация средств идентификации и аутентификации с точки зрения применяемых технологий

Аутентификация по цифровым сертификатам и закрытому ключу

Простейшие механизмы аутентификации на основе сертификатов обычно используют протокол с запросом и ответом. Согласно этому протоколу, сервер аутентификации направляет пользователю последовательность символов, называемую запросом, а программное обеспечение клиентского компьютера для генерирования ответа вырабатывает с помощью закрытого ключа пользователя цифровую подпись под запросом от сервера аутентификации. Общий процесс подтверждения подлинности пользователя состоит из следующих стадий:

- получение сервером открытого ключа удостоверяющего центра (CA, Certificate Authority), выдавшего сертификат пользователю;
- получение по некоторому незащищенному каналу от этого пользователя его сертификата открытого ключа (включающее получение идентификато-

ра пользователя, проверку даты и времени относительно срока действия, указанного в сертификате, на основе локальных доверенных часов, проверку действительности открытого ключа CA, проверку подписи под сертификатом пользователя с помощью открытого ключа CA, проверку сертификата на предмет отзыва);

- если все проверки успешны, открытый ключ в сертификате считается подлинным открытым ключом заявленного пользователя;
- проверка на наличие у пользователя закрытого ключа, соответствующего данному сертификату, с помощью алгоритма «запрос — ответ».

В качестве примера алгоритмов, работающих по такой схеме, можно назвать протоколы SSL/TLS. Аутентификация с открытым ключом используется как защищенный механизм аутентификации в таких протоколах, как SSL/TLS, а также может использоваться как один из методов аутентификации в рамках протоколов Kerberos с расширением PKINIT и EAP-TLS.

ИСПОЛЬЗОВАНИЕ МИКРОПРОЦЕССОРНЫХ СМАРТ-КАРТ

Несмотря на то что криптография с открытым ключом, согласно спецификации X.509, может обеспечивать строгую аутентификацию пользователя, сам по себе незащищенный закрытый ключ подобен паспорту без фотографии. Закрытый ключ, хранящийся на жестком диске компьютера владельца, уязвим по отношению к прямым и сетевым атакам. Достаточно подготовленный злоумышленник может похитить закрытый ключ пользователя и с его помощью представляться системе этим пользователем. Защита ключа с помощью пароля помогает, но недостаточно эффективно — пароли уязвимы по отношению ко многим атакам. Несомненно, требуется более безопасное хранилище.

Аутентификацию на основе микропроцессорных карт (другое часто используемое название — смарт-карты) сложнее всего обойти, так как используется уникальный физический объект, которым должен обладать человек, чтобы войти в систему. В отличие от паролей владелец быстро узнает о краже и может сразу принять необходимые меры для предотвращения ее негативных последствий. Кроме того, данные защищены при помощи двухфакторной аутентификации: злоумышленнику необходимо не только украсть смарт-карту (фактор обладания), но и узнать пароль к нему (фактор знания). Микропроцессорные карты могут повысить надежность служб Public Key Infrastructure (PKI): смарт-карта может использоваться для безопасного хранения закрытых ключей пользователя, а также для безопасного выполнения криптографических преобразований в рамках протокола аутентификации. Безусловно, данные устройства аутентификации не обеспечивают абсолютную безопасность, но надежность их защиты намного превосходит возможности обычного настольного компьютера.

Для хранения и использования закрытого ключа разработчики используют различные подходы. Наиболее простой из них — использование устройства аутентификации в качестве защищенного носителя аутентификационной информации:

при необходимости карта экспортирует закрытый ключ, и криптографические операции осуществляются на рабочей станции. Этот подход является не самым совершенным с точки зрения безопасности, зато относительно легко реализуемым и предъявляющим невысокие требования к устройству аутентификации. В качестве примера реализации такого подхода можно привести устройство `guToken`.

Два следующих подхода более безопасны, поскольку предполагают выполнение устройством аутентификации криптографических операций. При первом — пользователь генерирует ключи на рабочей станции и сохраняет их в памяти устройства. При втором — пользователь генерирует ключи при помощи устройства. В обоих случаях, после того как закрытый ключ сохранен, его нельзя извлечь из устройства и получить любым другим способом. Примером такого решения является смарт-карта класса `eToken`.

В случае генерации ключевой пары вне устройства пользователь может сделать резервную копию закрытого ключа. Если устройство выйдет из строя, будет потеряно, повреждено или уничтожено, пользователь сможет сохранить тот же закрытый ключ в памяти нового устройства. Это необходимо, если пользователю требуется расшифровать какие-либо данные, сообщения и т.д., зашифрованные с помощью соответствующего закрытого ключа. Однако при этом закрытый ключ пользователя подвергается риску быть похищенным, т.е. скомпрометированным.

При генерации ключевой пары с помощью устройства закрытый ключ не является в открытом виде и нет риска, что злоумышленник украдет его резервную копию. Единственный способ использования закрытого ключа — это обладание устройством аутентификации. Являясь наиболее безопасным, это решение выдвигает высокие требования к возможностям самого устройства: оно должно обладать функциональностью генерации ключей и осуществления криптографических преобразований. Решение также предполагает, что закрытый ключ не может быть восстановлен в случае выхода устройства из строя и т.п.

ВЫБОР НОСИТЕЛЕЙ КЛЮЧЕВОЙ ИНФОРМАЦИИ

Исходя из вышеизложенного можно рассмотреть вопросы выбора устройств аутентификации (микропроцессорных карт), которые обычно называют персональными идентификаторами (поскольку они содержат идентификаторы не только на поверхности смарт-карты, но и внутри чипа) или носителями ключевой информации. Кроме последнего упомянутого названия в последние годы эти устройства аутентификации еще называют персональными идентификаторами с неизвлекаемыми ключами, поскольку, согласно международным, в частности европейским, требованиям (например, *Guide on the Use of Electronic Signatures*. European Committee of Standardization. *Cen Workshop Agreement CWA 14365*, 2003), устройства, применяющиеся для так называемой квалифицированной электронной подписи (согласно Закону об электронной подписи), должны быть спроектированы как SSCD (*Secure Signature Creation Device* — устройства, способные безопасно генерировать ключевые пары, при этом закрытые ключи

обязаны никогда не покидать защищенную память устройства типа Write Only). Наконец, эти устройства еще называют программно-аппаратными средствами хранения ключевой информации. Мировой рынок смарт-карт достаточно велик, однако с целью снижения себестоимости для использования в банках обычно применяются одни из самых дешевых микропроцессорных карт, в заданное время выполняющих сегодня необходимый объем вычислений и работающих с устройствами чтения (ридерами) по протоколу T0. Для работы с банковскими приложениями вычислительной мощности таких карт было достаточно. Однако для перехода на устройства класса SSCD на рынке БС РФ ожидается появление смарт-карт с повышенными требованиями к функционалу и производительности чипа (особенно в части выполнения криптографических операций) и соответственно более дорогих в цене.

В Российской Федерации, к сожалению, на момент написания данного материала никаких официальных требований к аутентификации и ключевым носителям не зафиксировано. Однако движение в сторону появления таких документов началось, особенно после появления постановления Правительства РФ от 28 ноября 2011 г. № 977 «О федеральной государственной информационной системе „Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме“», которое предписывает в весьма сжатые сроки (до 15 апреля 2012 г.) ввести в эксплуатацию единую систему идентификации и аутентификации в Российской Федерации. В силу важности данного вопроса и развития системы юридически значимых электронных документов требования к уровням аутентификации при удаленном доступе к различным информационным системам, скорее всего, появятся в ближайшем будущем. Кроме ключей ЭЦП и шифрования, которые генерируются внутри чипа смарт-карты, в защищенную память ключевого носителя помещают ключи VPN, ключи шифрования и другой ключевой (критичный к разглашению) материал.

При выборе программно-аппаратных средств для хранения ключевой информации, идентификации и аутентификации пользователей — владельцев смарт-карт, реализующих криптографические алгоритмы и протоколы, согласно Стандарту, указанные средства должны иметь сертификат соответствия требованиям ФСБ России к СКЗИ класса КС1 или КС2 в соответствии с утвержденной для данной информационной системы моделью угроз.

9.2. ПЕРСПЕКТИВНЫЕ РЕШЕНИЯ. МОБИЛЬНЫЙ БАНКИНГ

В последние годы наметился интерес к взаимному сближению двух направлений обслуживания клиентов через разные по своей природе каналы связи. С одной стороны, банки вынуждены искать новые формы борьбы с развивающимся

все более умным и изощренным мошенничеством в системах ДБО. С другой стороны, операторам сотовой связи приходится создавать новые сервисы для своих абонентов, исчисляющихся десятками и сотнями миллионов.

Идеальным сервисом для операторов сотовой связи могли бы стать возможность предоставления комплекса дистанционных услуг, включая доступ на портал государственных услуг, а также массовые сервисы безопасной оплаты услуг сторонних (не имеющих отношения к сотовой связи) организаций (парковка, транспорт, отели, аптеки, театры, билеты, оплата покупок в магазинах и т.д.).

Как сделать эти платежи безопасными? Опять обратимся к опыту банков, которые первыми начали использовать в своих приложениях виртуальное киберпространство, т.е. «недоверенную» анонимную среду Интернета.

Вначале данные кредитной карты просто вводились в HTML-форму и передавались по протоколу HTTPS, и клиенты банков регулярно страдали от атак на карточные системы. Была предпринята попытка создания некоего островка «пространства доверия». В частности, был разработан протокол SET (SecureElectronicTransaction — протокол защищенных электронных транзакций). В его разработке кроме Visa и MasterCard принимали участие такие известные компании, как IBM, Microsoft, Netscape, RSA, Terisa и VeriSign.

Суть протокола SET состоит в том, что для всех основных участников электронных транзакций сертификаты подписи формата X.509 выпускаются одним удостоверяющим центром, а для проверки неотказуемости заказа и платежеспособности покупателя и, кроме того, наличия товара (услуги) и правильности понимания заказа продавец использовал «дуальную» электронную цифровую подпись (ЭЦП). Сертификаты X.509, по замыслу разработчиков, должны были обеспечивать надежную идентификацию трех сторон электронной сделки: покупателя, интернет-магазина и платежного шлюза. Целью применения «дуальной» подписи является связывание двух сообщений, предназначенных двум разным получателям. SET использовал алгоритм, позволяющий скрывать данные кредитной карты покупателя, заменяя их подписанным банком сертификатом. Тем самым он обеспечивал сохранность (обезличенность) данных кредитной карты, так как при хранении сертификата его попадание в руки злоумышленника не позволяло этому последнему провести какую-либо мошенническую транзакцию по карте. Несмотря на целый ряд технологических инноваций и высокий уровень безопасности, SET не получил широкого распространения в Интернете. Сказались как высокая сложность, так и уязвимость дополнительного программного обеспечения (ПО), устанавливаемого на компьютере покупателя. Урезанные версии SET, не требовавшие такого ПО, были реализованы несколькими платежными шлюзами Интернета, в том числе и в России. Однако они не несли в себе всех преимуществ полного варианта, и к настоящему моменту протокол SET в целом прекратил свое развитие. Поддержка платежных систем Visa, MasterCard и примкнувшей к ним JCB досталась более простому в использовании протоколу 3DSecure/SecureCode, также разработанному специалистами Visa.

Протокол 3D Secure является XML-протоколом с дополнительным уровнем безопасности для онлайн-оплат по кредитным и дебетовым картам. Суть протокола, называемого Verified by Visa (сокращенно — VbV) в терминологии платежной системы Visa, SecureCode — в терминологии MasterCard и J/Secure — в терминологии JCB International, состоит в дополнительной аутентификации владельца карты перед совершением платежа для предотвращения или существенного снижения уровня мошенничеств. Название 3-D протокол получил вследствие того, что в процессе подтверждения подлинности участвуют три домена, третья доверенная сторона — общий домен.

В отличие от банков идентификация клиентов в сетях GSM (Global System for Mobile Communications) строилась на основе модели строгой двухфакторной аутентификации с помощью специальных чипов (SIM-карт). В основу безопасности сетей GSM положены достаточно стойкие алгоритмы и стройная архитектура, которые при надежном исполнении и развитии вполне способны гарантировать надежную аутентификацию пользователя, обеспечить защиту от клонирования и прочих методов мошенничества. Собственно говоря, именно эти ее качества предопределили конкурентные преимущества для компаний, занимающихся разворачиванием сетей GSM по всему миру. Однако сети GSM изначально создавались для обеспечения надежного и гарантированного канала «речевой» связи, а не для банковских приложений или мобильных платежей. Соответственно в SIM-картах нет и не было поддержки ЭЦП и PKI приложений.

Коммерческий успех того или иного предложения основан на эффективности применяемых решений. Решения должны быть простыми, привычными, доступными, надежными и быть всегда «под рукой», т.е. работать в любую минуту и на всех каналах сервиса. При этом субъекты и объекты в диалоге должны быть надежно идентифицированы, а пользователь должен быть уверен в своей защищенности от атак на безопасность, осуществляемых, как правило, по принципу «злоумышленник посередине» (phishing, relay attack и т.п.).

При работе с электронными приложениями пользователь нуждается не только в строгой пользовательской аутентификации, но и в строгой отчетности, особенно в работе с бесконтактными платежами и операционными приложениями (операционное подписание и операционное архивирование).

Безопасность проводимых операций может быть обеспечена при выполнении следующих условий:

- процесс идентификации и аутентификации (подтверждения подлинности идентификации) пользователя выполняется отдельно от фактической сделки (канала запроса);
- пароль доступа никогда не передается по каналам связи;
- аутентификатор пользователя не может быть использован другим человеком;
- вор, завладевший средством доступа, может им воспользоваться, но не сможет выдать себя за владельца сертификата жертвы.

Сочетание перечисленных факторов возможно, если в системе оказания дистанционных услуг присутствуют не только «островки доверительных отношений», но и «канал доверенной связи». Этот второй канал запроса к «островам доверия» может быть организован по каналу GSM с помощью специальной SIM-карты — Mobil-ID + ЭЦП. Данный способ позволяет легко и просто организовать персональное адресное взаимодействие в виртуальном пространстве и сделает это естественным, безопасным и надежным способом.

Суть перспективного технологического предложения — попробовать соединить в одном мобильном устройстве несоединимые раньше вещи: GSM и PKI. Кроме обычных функций SIM-карта Mobil-ID + ЭЦП должна содержать функционал, на основании которого провайдеры интернет-услуг смогут при необходимости по каналу запроса надежно идентифицировать пользователя как законного владельца данной SIM-карты. Владелец смарт-карты в свою очередь сможет подтвердить (собственноручно подписать) с ее помощью свое волеизъявление, используя для этого легитимный инструментарий электронной цифровой подписи.

SIM-карта Mobil-ID + ЭЦП в отличие от обычной должна иметь дополнительное средство строгой аутентификации на основе криптографии с открытым ключом. Аппаратно это средство может существовать интегрально либо размещаться отдельно, например в виде второй SIM-карты, связанной прокси с основной SIM-картой, или отдельного устройства microSD. С помощью данного средства будет обеспечиваться связь владельца (абонента сети GSM) с инфраструктурой открытых ключей PKI.

Равно как и для оператора сотовой связи, для которого пара — секретный ключ Ki — персональный идентификатор IMSI (International Mobile Subscriber Identity) используется повсеместно в связке с регистром положения домашних абонентов (HLR¹) для строгой идентификации SIM-карт. В виртуальном «анонимном» пространстве мобильный сертификат становится электронным удостоверением личности, который в любой момент может быть предъявлен владельцем. Мобильным сертификатом можно пользоваться повсеместно и многократно, его, как и мобильный телефон, пользователь всегда носит с собой.

Основная область применения SIM-карты Mobil-ID + ЭЦП — использование мобильного телефона для подтверждения операций, требующих исполнения строгих процедур проверки подлинности данных и субъектов информационного взаимодействия. Услуги WirelessPKI для сотового оператора должен предоставлять специальный провайдер услуг, именуемый Mobile Signature Service Provider (MSSP).

На практике двухканальная многофакторная мобильная аутентификация на основе SIM-карты Mobil-ID + ЭЦП позволит не только идентифицировать владельца в системе оказания электронных услуг, но и использовать электронные подписи в течение всего сеанса связи или даже по завершении телефонного звонка. Владельцу больше не придется запоминать все свои пароли и имена пользователя. Он сможет вообще отказаться от кодовых банковских карточек

¹ HLR — Home Location Register, Регистр положения домашних абонентов.

и PIN-калькуляторов. Если для различных сервисов сейчас пользователь вынужден использовать различные идентификационные данные (пароли и имена пользователя), то такая SIM-карта позволит авторизоваться во все службы и сервисы с одним-единственным персональным кодом. Функционально владелец новой SIM-карты сможет делать те же электронные операции, что и владельцы обычных смарт-карт, — заходить в интернет-банк, на порталы услуг, подписывать различные договоры и пр. При этом MSSP обеспечивает двухканальную поддержку строгой аутентификации по сочетаниям многих факторов, включая ГОСТ Р 34.10—2001, ГОСТ Р 34.11—94 (криптография с открытым ключом), ГОСТ 28147—89.

Сертификат ключа подписи можно сравнить с имеющимся образцом подписи — доступ к нему открыт и адресат всегда может проверить подлинность этой подписи. Если IMSI, сертификат и цифровая подпись совпадают, можно быть уверенным в том, что электронный документ был подписан именно тем человеком, чьи данные записаны в сертификате. Секретный ключ «помечает» подписанный документ уникальным образом, так что позднее всегда можно доказать, что подпись была сделана именно с помощью этого средства.

С помощью SIM-карты Mobil-ID + ЭЦП можно осуществлять шифрование данных, в первую очередь для безопасной транспортировки файлов по каналам связи. Если пользователь утратил ее, расшифрование файлов становится невозможным. Неоспоримое преимущество Mobil-ID + ЭЦП заключается в том, что владельцу не придется отдельно использовать какой-либо считыватель для смарт-карт, он сможет воспользоваться услугой доступа с любого, даже очень «сомнительного» («недоверенного») компьютера. Мобильный телефон в данном случае выполняет функции считывателя смарт-карт, самой карты и доверенного канала. Криптозащита основывается на разделяемой между Mobil-ID + ЭЦП и MSSP, а также SIM-картой и Центром коммутации сотовой связи (HLR) секретной информации.

Поддержку электронной подписи при таком подходе можно интегрировать практически в любое программное приложение.

Владельцам SIM-карт и операторам сотовой связи Mobil-ID + ЭЦП обеспечит уникальные свойства и отличительные качества:

- высокую степень безопасности и высокую производительность системы аутентификации;
- отсутствие процедурных ограничений по ведению бизнеса, включая соблюдение авторских прав и безопасности загружаемых данных;
- возможность для обезличивания персональных данных — без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных невозможно;
- интегрированный механизм обеспечения безопасности (доверенная среда с прозрачным шифрованием данных);
- надежные ко взлому алгоритмы и аппаратные средства многофакторной аутентификации, основанные на принципах суверенитета (национальной криптографии);

- доступ к любым услугам, включая услуги «электронного правительства»;
- доверенный мониторинг — имеется возможность наблюдать за всеми действиями и передавать результаты пользователю, который может убедиться в том, что все действия провайдера выполняются в соответствии с документированными запросами и с регламентом (подписанным соглашением).

Данная SIM-карта обеспечивает уникальные коммерческие качества провайдерам услуг:

- Mobile Signature Service Provider, который может работать виртуально на любых коммуникационных сетях, предоставляет коммерческим операторам взаимодействующих информационных систем дополнительный доверенный сервис в виде приложений (WPKI);
- администратор не имеет доступа к паролям пользователей;
- MSSP может предоставлять по документированному запросу документированные ответы (доказательства), которым смогут доверять все подписчики того или иного сервиса.

Дополнительно владельцам таких SIM-карт со стороны провайдеров услуг могут быть предоставлены:

- «облака» национальной аутентификации;
- объединяющие транснациональные решения (транспортные, таможенные, межбанковские, нотариальные и др.);
- поддержка доверенных «облаков» в «облаке» корпоративных приложений;
- мультисервисная национальная аутентификация в трансграничном домене услуг.

Безусловно, в данной главе книги рассмотрены далеко не все проблемы, связанные с решением проблем применения идентификации и аутентификации при проведении расчетов и платежей через сети общего пользования. Например, одним из открытых вопросов пока остается проблема формирования требований к AAA при неотвратимом взаимодействии ИСОП и закрытых корпоративных систем, принадлежащих банковской системе РФ.

Согласно ст. 2 Закона об электронной подписи участниками информационного взаимодействия могут быть государственные органы, органы местного самоуправления, организации и граждане. Попробуем сформулировать требования к идентификации и аутентификации для этих групп участников взаимодействия.

Если запрос на услуги не персонифицирован (например, в простейшем случае не требует реакции ответственного лица), то идентификация не нужна. Соответственно не требуется и аутентификация того, кто делает запрос.

Если запрос на государственную услугу персонифицирован, то требуется идентификация пославшего запрос. Если ответ подразумевает подпись ответственного лица, то вдобавок к обязательной идентификации требуется аутентичность запроса и ответа. Если подпись усиленная (с использованием неквалифицированного или квалифицированного сертификата), то требуется строгая аутентификация (табл. 9.1).

Таблица 9.1

**Требования к идентификации и аутентификации
для участников информационного взаимодействия**

| Участники информационного взаимодействия | Идентификация | Аутентификация |
|--|-----------------------------------|-----------------------------------|
| Государственные органы | Да | Строгая |
| Органы местного самоуправления | Да | Строгая |
| Организации | Да | Да (нет) в зависимости от запроса |
| Граждане | Да (нет) в зависимости от запроса | Да (нет) в зависимости от запроса |

Соответственно на основе анализа текста Закона об электронной подписи и приведенных рассуждений мы можем сформулировать и требования к способам аутентификации. В случаях, когда ответ ответственного лица на запрос государственной услуги имеет правовые последствия (типичным примером является услуга подтверждения или перехода прав собственности на недвижимость), необходимо применять усиленную электронную подпись и квалифицированный сертификат. При этом требуется применение строгой двухфакторной аутентификации. Результаты для наглядности представлены в виде табл. 9.2.

Таблица 9.2

Требования к аутентификации в зависимости от вида электронной подписи

| Виды подписи | Аутентификация |
|--|----------------|
| Простая | Да |
| Усиленная (неквалифицированный сертификат) | Строгая |
| Усиленная (квалифицированный сертификат) | Строгая |

* * *

В зависимости от назначения системы, степени конфиденциальности циркулирующей в ней информации и роли пользователей задачи автоматической идентификации и аутентификации претендентов на право авторизации в качестве одновременно пользователя ИСОП и, например, ДБО всегда требуют внимательного изучения. С одной стороны, это обусловлено тем, что в нормативных актах отсутствуют рекомендации по выбору технологических решений для решения данной задачи. С другой стороны, существующее многообразие технологий, продвигаемых производителями с той или иной степенью успешности, может породить ошибки проектировщиков ИСОП с точки зрения обеспечения надежности функционирования и реальной защиты выбранных решений.

Выражаем надежду, что предложенные требования к идентификации и аутентификации позволят существенно снизить риски мошенничеств при строительстве ИСОП и систем платежей с использованием Интернета.

ГЛАВА 10

ЗАКОН О НПС: СТРУКТУРА И КОММЕНТАРИИ

Закон об НПС, или Закон «О национальной платежной системе» определил законодательное поле для всех субъектов рынка. Впервые в российской истории, признав наличие электронных средств для осуществления расчетов, Закон устанавливает единые для всех участников НПС правила проведения расчетов (момент наступления окончательности платежа, обеспеченность расчетов, круг лиц, принимающих участие в расчетах, и роль каждого из них и др.).

Принятие данного документа потребовало основательной переработки многих иных документов и законов, что повлекло одновременное принятие и Закона «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона „О национальной платежной системе“» от 27 июня 2011 г. № 162-ФЗ (перечень законодательных актов, затронутых Законом № 162-ФЗ см. в конце данной главы).

В данной главе книги будут рассмотрены структура Закона об НПС, последовательность вступления в силу положений Закона, будут обсуждены особенности регулирования платежных услуг, деятельности субъектов национальной платежной системы с точки зрения нового закона, надзора и наблюдения в НП, даны некоторые комментарии¹.

10.1. ЧТО ПРЕДСТАВЛЯЕТ СОБОЙ НПС С ТОЧКИ ЗРЕНИЯ ЗАКОНА

Приведем еще раз определение НПС, данное Законом об НПС (ст. 3): «Национальная платежная система (НПС) — совокупность операторов по переводу денежных средств (включая операторов электронных денежных средств), банковских платежных агентов (субагентов), платежных агентов, организаций Федеральной почтовой связи, операторов услуг платежной инфраструктуры».

¹ Закон № 162-ФЗ, на наш взгляд, в особых комментариях не нуждается, поэтому ограничимся тем, что приведем список законодательных актов, которые он затрагивает (см. приложение в конце данной главы).

Уже из данного определения можно сделать вывод, что Закон регулирует отношения, возникающие между широким кругом участников, задействованных в осуществлении платежей (в том числе электронных), проводимых по инициативе (с согласия) плательщика в пользу получателя денежных средств.

Напомним, что Закон о деятельности по приему платежей физических лиц, осуществляемой платежными агентами регулирует отношения, возникающие только по инициативе продавца товаров (услуг), и не охватывает большинства операций, существующих сегодня.

Закон о НПС дает возможность, сохраняя стабильность системы расчетов, на законных основаниях существенно расширить круг участников расчетов, что в свою очередь приводит к снижению цены обработки одного платежа и расширению доступности платежной инфраструктуры для плательщиков (рис. 10.1).

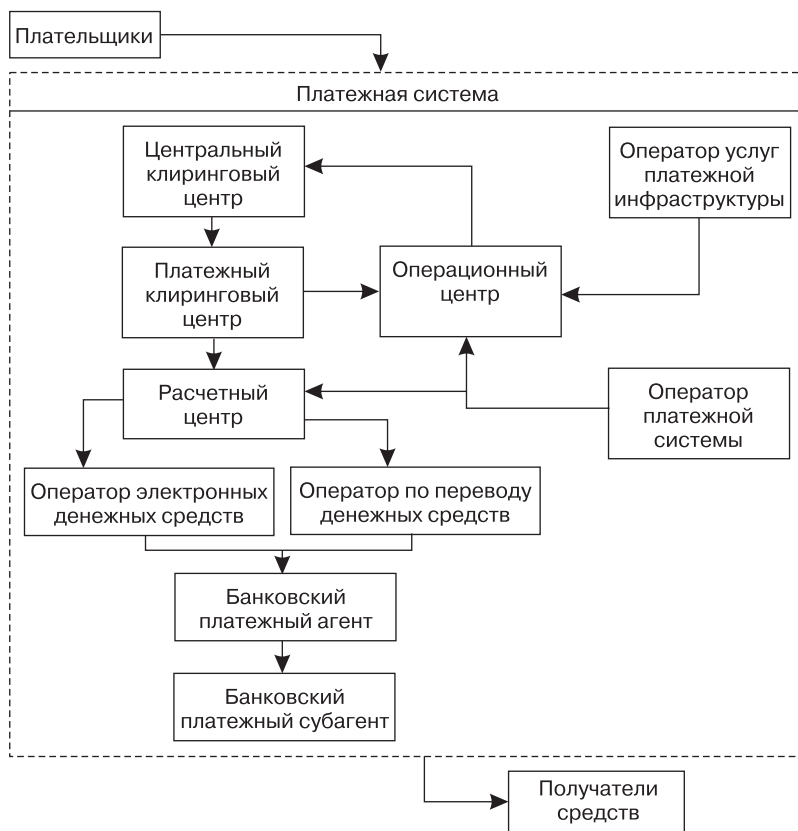


Рис. 10.1. Структурная схема национальной платежной системы в соответствии с Законом о НПС

УЧАСТНИКИ ПЛАТЕЖНОЙ СИСТЕМЫ

Согласно Закону, в состав платежной системы в общем случае могут входить:

- 1) оператор по переводу денежных средств;
- 2) оператор электронных денежных средств;
- 3) банковский платежный агент;
- 4) банковский платежный субагент;
- 5) оператор платежной системы;
- 6) оператор услуг платежной инфраструктуры;
- 7) операционный центр;
- 8) платежный клиринговый центр;
- 9) центральный клиринговый центр;
- 10) расчетный центр.

Приведенный состав участников является максимальным и может меняться в сторону уменьшения в зависимости от операций, осуществляемых конкретной платежной системой. Несмотря на то, что к каждому из участников Закон предъявляет свои требования, возможно совмещение некоторых участников платежной системы в рамках одного юридического лица (при условии его соответствия предъявляемым законодательством требованиям в совокупности). Также допускается иметь неограниченное количество участников платежной системы, выполняющих одинаковые функции.

Подробнее об организационной форме, особенностях лицензирования участников НПС и их функциональных обязанностях — табл. 10.1.

Таблица 10.1

Описание участников платежной системы

| Наименование участника и ссылка на статью Закона № 161-ФЗ, содержащую полное описание | Организационная форма и особенности лицензирования | Функциональные обязанности |
|---|--|---|
| Оператор по переводу денежных средств (ст. 11, 14) | 1) Банк России; 2) кредитные организации, имеющие право на осуществление перевода денежных средств; 3) Внешэкономбанк | Осуществляет перевод денежных средств между участниками платежной системы |
| Оператор электронных денежных средств (ст. 12, 13, 14) | Кредитная организация (в том числе небанковская кредитная организация), имеющая право на осуществление переводов денежных средств без открытия банковских счетов | Осуществляет перевод электронных денежных средств без открытия банковского счета |

Продолжение

| Наименование участника и ссылка на статью Закона № 161-ФЗ, содержащую полное описание | Организационная форма и особенности лицензирования | Функциональные обязанности |
|---|--|--|
| Банковский платежный агент (ст. 14) | 1) юридическое лицо (за исключением кредитной организации); 2) индивидуальный предприниматель | Осуществляют прием-выдачу наличных денежных средств и (или) распоряжений на осуществление переводов, а также осуществляют иную деятельность, которая возложена на кредитные организации в рамках Закона № 161-ФЗ |
| Банковский платежный субагент (ст. 14) | Юридическое лицо (за исключением кредитной организации) или индивидуальный предприниматель, которые привлекаются банковским платежным агентом | Осуществляют прием-выдачу средств наличных денежных средств и (или) распоряжений на осуществление переводов, а также осуществляют иную деятельность, которая возложена на кредитные организации в рамках Закона № 161-ФЗ, с рядом ограничений |
| Оператор платежной системы (ст. 15) | 1) кредитная организация; 2) организация, не являющаяся кредитной организацией; 3) Банк России; 4) Внешэкономбанк | Определяет правила платежной системы |
| Оператор услуг платежной инфраструктуры (ст. 16) | 1) кредитная организация; 2) организация, не являющаяся кредитной организацией; 3) Банк России; 4) Внешэкономбанк | Не является самостоятельным участником и представляет совокупность следующих центров: операционного, платежно-клирингового и расчетного |
| Операционный центр (ст. 17) | 1) кредитная организация; 2) организация, не являющаяся кредитной организацией; 3) Банк России; 4) Внешэкономбанк | Оказывает операционные услуги: перевод денежных средств, в том числе с использованием электронных средств платежа, а также обмен электронными сообщениями |
| Платежный клиринговый центр (ст. 18) | 1) кредитная организация; 2) организация, не являющаяся кредитной организацией; 3) Банк России; 4) Внешэкономбанк | Обеспечивает прием к исполнению распоряжений участников платежной системы об осуществлении перевода денежных средств и выполнение иных действий |

Окончание

| Наименование участника и ссылка на статью Закона № 161-ФЗ, содержащую полное описание | Организационная форма и особенности лицензирования | Функциональные обязанности |
|---|---|--|
| Центральный клиринговый центр (ст. 18) | 1) кредитная организация; 2) Банк России; 3) Внешэкономбанк. Обычное юридическое лицо выступать центральным клиринговым центром не может | Выступает плательщиком и получателем средств по переводам денежных средств участников платежной систем |
| Расчетный центр (ст. 19) | 1) кредитная организация; 2) Банк России; 3) Внешэкономбанк | Обеспечивает исполнение распоряжений участников платежной системы посредством списания и зачисления денежных средств по банковским счетам участников платежной системы, а также направление подтверждений, касающихся исполнения распоряжений участников платежной системы |

ОБЩАЯ СТРУКТУРА ЗАКОНА ОБ НПС И ПОРЯДОК ВСТУПЛЕНИЯ В СИЛУ ЕГО ПОЛОЖЕНИЙ

Как это часто бывает с принимаемыми законами (особенно имеющими инновационный характер), введение в действие его отдельных положений отсрочено. Некоторые положения Закона № 161-ФЗ вступили в силу в момент его подписания, некоторые — через полгода, а отдельные положения должны вступить через год и даже полтора. В целях удобства информация сведена в одну таблицу (табл. 10.2).

Таблица 10.2

Порядок вступления в силу положений Закона об НПС, привязанный к его структуре

| Глава | Статья | Дата вступления в силу | | | |
|--------------------------|--|------------------------|------------------|-----------|---------------|
| | | сразу | через шесть мес. | через год | через 18 мес. |
| Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ | Статья 1. Предмет регулирования настоящего Федерального закона | | | X | |
| | Статья 2. Нормативно-правовое регулирование отношений в национальной платежной системе | | | X | |

Продолжение

| Глава | Статья | Дата вступления в силу | | | |
|---|--|------------------------|---|---|------------------|
| | | сразу | через шесть мес. | через год | через 18 мес. |
| | Статья 3. Основные понятия, используемые в настоящем Федеральном законе | О | Пункты 12–16 (перевод денежных средств; трансграничный перевод денежных средств; безотзывность перевода денежных средств; безусловность перевода денежных средств; окончательность перевода денежных средств) | Пункты 1, 6–11, 20–25 (определения: национальная платежная система; оператор платежной системы; оператор услуг платежной инфраструктуры; операционный центр; платежный клиринговый центр; центральный клиринговый центр; расчетный центр; платежная система; значимая платежная система; правила платежной системы; участники платежной системы; обмен электронными сообщениями; платежные клиринговые позиции) | |
| Глава 2. ПОРЯДОК ОКАЗАНИЯ ПЛАТЕЖНЫХ УСЛУГ, В ТОМ ЧИСЛЕ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ, И ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА | Статья 4. Порядок оказания платежных услуг | Х | | | |
| | Статья 5. Порядок осуществления перевода денежных средств | | Х | | |
| | Статья 6. Особенности осуществления перевода денежных средств по требованию получателя средств | | Х | | |

Продолжение

| Глава | Статья | Дата вступления в силу | | | |
|---|---|------------------------|---------------------|--------------|------------------|
| | | сразу | через шесть мес. | через год | через 18 мес. |
| | Статья 7. Особенности осуществления перевода электронных денежных средств | X | | | |
| | Статья 8. Распоряжение клиента, порядок его приема к исполнению и исполнения | | X | | |
| | Статья 9. Порядок использования электронных средств платежа | O | | | |
| | Статья 10. Порядок использования электронных средств платежа при осуществлении перевода электронных денежных средств | X | | | |
| Глава 3. СУБЪЕКТЫ НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ И ТРЕБОВАНИЯ К ИХ ДЕЯТЕЛЬНОСТИ | Статья 11. Оператор по переводу денежных средств и требования к его деятельности | X | | | |
| | Статья 12. Оператор электронных денежных средств и требования к его деятельности | X | | | |
| | Статья 13. Требования к деятельности оператора электронных денежных средств при увеличении остатков электронных денежных средств физических лиц — абонентов оператора связи | X | | | |

Продолжение

| Глава | Статья | Дата вступления в силу | | | |
|---|---|------------------------|---------------------|---|------------------|
| | | сразу | через шесть мес. | через год | через 18 мес. |
| | Статья 14. Требования к деятельности оператора по переводу денежных средств при привлечении банковского платежного агента (субагента) | Х | | | |
| | Статья 15. Оператор платежной системы и требования к его деятельности | | | Х | |
| | Статья 16. Оператор услуг платежной инфраструктуры и требования к его деятельности | | | Х | |
| | Статья 17. Требования к деятельности операционного центра | О | | Части 1–7 (все, кроме взаимодействия с иностранными операционными центрами) | |
| | Статья 18. Требования к деятельности платежного клирингового центра | | | Х | |
| | Статья 19. Требования к деятельности расчетного центра | | | Х | |
| | Статья 20. Правила платежной системы | | | Х | |
| Глава 4. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЮ ПЛАТЕЖНЫХ СИСТЕМ | Статья 21. Участники платежной системы | | | Х | |
| | Статья 22. Признание платежной системы значимой | | | Х | |

Продолжение

| Глава | Статья | Дата вступления в силу | | | |
|-------|--|------------------------|---------------------|--------------|------------------|
| | | сразу | через шесть мес. | через год | через 18 мес. |
| | Статья 23. Порядок проверки Банком России соответствия правил значимой платежной системы установленным требованиям | | | X | |
| | Статья 24. Требования к значимой платежной системе | | | X | |
| | Статья 25. Осуществление платежного клиринга и расчета в платежной системе | | | X | |
| | Статья 26. Обеспечение банковской тайны в платежной системе | X | | | |
| | Статья 27. Обеспечение защиты информации в платежной системе | | | X | |
| | Статья 28. Система управления рисками в платежной системе | | | X | |
| | Статья 29. Обеспечение исполнения обязательств участников платежной системы | | | X | |
| | Статья 30. Счет гарантийного фонда платежной системы | | | X | |
| | Статья 31. Цели надзора и наблюдения в национальной платежной системе | | | X | |

Продолжение

| Глава | Статья | Дата вступления в силу | | | |
|---|--|------------------------|---------------------|--------------|------------------|
| | | сразу | через шесть мес. | через год | через 18 мес. |
| Глава 5. НАД- ЗОР И НА- БЛЮДЕНИЕ В НАЦИО- НАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ | Статья 32. Осущест- вление надзора в на- циональной платеж- ной системе | | | X | |
| | Статья 33. Порядок проведения инспек- ционных проверок поднадзорных орга- низаций | | | X | |
| | Статья 34. Действия и меры принуждения, применяемые Бан- ком России в случае нарушения поднад- зорной организацией требований настоя- щего Федерального закона или принятых в соответствии с ним нормативных актов Банка России | | | X | |
| | Статья 35. Содержа- ние и приоритеты наблюдения в наци- ональной платежной системе | | | X | |
| | Статья 36. Взаимо- действие Банка Рос- сии с федеральными органами исполни- тельной власти при осуществлении над- зора и наблюдения в национальной пла- тежной системе | | | X | |
| | Статья 37. Междуна- родное сотрудниче- ство Банка России по вопросам надзора и наблюдения в на- циональной платеж- ной системе | | | X | |

Окончание

| Глава | Статья | Дата вступления в силу | | | |
|-----------------------------------|---|------------------------|---------------------|--------------|------------------|
| | | сразу | через шесть мес. | через год | через 18 мес. |
| Глава 6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ | Статья 38. Заключительные положения | Х | | | |
| | Статья 39. Порядок вступления в силу настоящего Федерального закона | Х | | | |

Примечания: Х — статья вступает в силу целиком; О — статья вступает в силу частично (те положения, которые вступают позднее, перечислены в графах «Через 6 мес.», «Через год» и «Через 18 мес.»)

ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДОВ

Схемы перевода денежных средств (в том числе электронных) согласно Закону об НПС выглядят следующим образом.

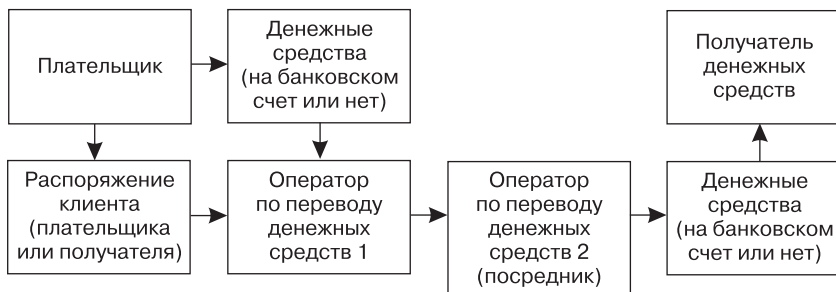


Схема 10.1. Перевод денежных средств

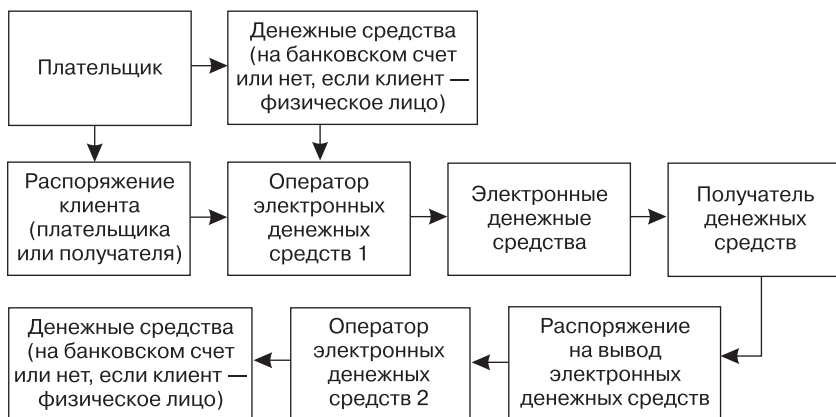


Схема 10.2. Перевод электронных денежных средств

Как видно из приведенных схем, основным отличием переводов обычных денежных средств от электронных является то, что при переводе электронных средств необходимо сначала зарезервировать обычные денежные средства. Данное положение Закона делает невозможным выпуск необеспеченных электронных денежных средств (иные отличия — табл. 10.3).

Таблица 10.3

Различные свойства

| Категория | Свойство | |
|---|---|--|
| | Перевод денежных средств | Перевод электронных средств |
| Оператор может предоставлять средства клиенту | Да | Нет |
| Оператор вправе начислять проценты и выплачивать иное вознаграждение клиенту на остаток средств | Да | Нет |
| Время осуществления перевода | Допустимо в течение трех дней | Сразу |
| Подтверждение исполнения перевода | Допустимо в течение трех дней | Сразу |
| Момент наступления безотзывности и окончательности перевода | Допустимо в течение трех дней | Сразу |
| Момент исполнения денежного обязательства плательщика перед получателем | С момента получения средств получателем | Сразу |
| Обязанность открытия банковского счета у оператора для юридических лиц | Нет | Да |
| Наличие права оператора не осуществлять перевод средств (не заключать договор) | Нет | Да |
| Максимально допустимый объем средств у клиента | Неограничен | 100 тыс. руб. при условии идентификации клиента и 15 тыс. руб. без идентификации |

НАДЗОР И НАБЛЮДЕНИЕ ЗА ПЛАТЕЖНОЙ СИСТЕМОЙ

Основными целями надзора и наблюдения в национальной платежной системе являются обеспечение стабильности НПС и ее развитие.

Контроль и надзор за соблюдением операторами по переводу денежных средств, являющимися кредитными организациями, операторами платежных

систем, операторами услуг платежной инфраструктуры требований законодательства в НПС осуществляет Банк России.

При осуществлении надзора Банк России:

- 1) анализирует документы и информацию (в том числе данные отчетности), которые касаются деятельности поднадзорных организаций и участников платежных систем, а также организации и функционирования платежных систем;
- 2) проводит инспекционные проверки поднадзорных организаций;
- 3) осуществляет действия и применяет меры принуждения.

Также Банк России определяет формы и сроки представления отчетности, в том числе в виде отчетности поднадзорной организации и сводной отчетности по платежной системе, методику составления указанной отчетности.

Банк России проводит плановые инспекционные проверки поднадзорных организаций не чаще одного раза в два года в соответствии с утвержденным Банком России планом проверок. При нарушении бесперебойности функционирования значимой платежной системы Банк России проводит внеплановые инспекционные проверки. Инспекционные проверки могут проводиться по отдельным вопросам деятельности поднадзорных организаций либо являться комплексными.

При осуществлении надзора и наблюдения в национальной платежной системе Банк России взаимодействует с федеральными органами исполнительной власти, в том числе с ФСФР России, в том числе по вопросам участия в платежных системах профессиональных участников рынка ценных бумаг, юридических лиц — участников организованных торгов и (или) участников клиринга, а также по вопросам взаимодействия операторов услуг платежной инфраструктуры с клиринговыми организациями, центральными контрагентами и (или) депозиториями.

Банк России может запросить центральный банк и иной орган надзора и наблюдения в национальной платежной системе иностранного государства о предоставлении информации или документов, которые получены в ходе исполнения функций надзора и наблюдения, а также может предоставить центральному банку и иному органу надзора и наблюдения в национальной платежной системе иностранного государства указанные информацию или документы, которые не содержат сведений о переводах денежных средств, при условии обеспечения указанным органом надзора и наблюдения в национальной платежной системе режима сохранности информации, соответствующего установленным законодательством Российской Федерации требованиям обеспечения сохранности информации, предъявляемым к Банку России. В отношении информации и документов, которые получены от центральных банков и иных органов надзора и наблюдения в национальных платежных системах иностранных государств, Банк России обязан соблюдать требования по раскрытию информации в соответствии с заключенными соглашениями (меморандумами) о сотрудничестве.

СИСТЕМА РЕГУЛИРОВАНИЯ РИСКОВ ПЛАТЕЖНОЙ СИСТЕМЫ

Принципиальным новшеством для российских платежных систем стала необходимость выстраивания системы регулирования рисков, что закреплено в ст. 28 Закона № 161-ФЗ.

Систему рисков как свод правил создает оператор или коллегиальный орган во главе с оператором платежной системы в каждой платежной системе самостоятельно.

Оператор платежной системы определяет одну из следующих используемых в платежной системе организационных моделей управления рисками в платежной системе:

- 1) самостоятельное управление рисками в платежной системе оператором платежной системы;
- 2) распределение функций по оценке и управлению рисками между оператором платежной системы, операторами услуг платежной инфраструктуры и участниками платежной системы;
- 3) передача функций по оценке и управлению рисками оператором платежной системы, не являющимся кредитной организацией, расчетному центру.

Система управления рисками должна предусматривать следующие мероприятия:

- 1) определение организационной структуры управления рисками, обеспечивающей контроль за выполнением участниками платежной системы требований к управлению рисками, установленных правилами платежной системы;
- 2) определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений;
- 3) доведение до органов управления оператора платежной системы соответствующей информации о рисках;
- 4) определение показателей бесперебойности функционирования платежной системы в соответствии с требованиями нормативных актов Банка России;
- 5) определение порядка обеспечения бесперебойности функционирования платежной системы в соответствии с требованиями нормативных актов Банка России;
- 6) определение методик анализа рисков в платежной системе, включая профили рисков, в соответствии с требованиями нормативных актов Банка России;
- 7) определение порядка обмена информацией, необходимой для управления рисками;
- 8) определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев;
- 9) определение порядка изменения операционных и технологических средств и процедур;
- 10) определение порядка оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией;

11) определение порядка обеспечения защиты информации в платежной системе.

Способы управления рисками в платежной системе определяются оператором платежной системы с учетом особенностей организации платежной системы, модели управления рисками, процедур платежного клиринга и расчета, количества переводов денежных средств и их сумм, времени окончательного расчета.

Система управления рисками может предусматривать следующие способы управления рисками:

- 1) установление предельных размеров (лимитов) обязательств участников платежной системы с учетом уровня риска;
- 2) создание гарантийного фонда платежной системы;
- 3) управление очередностью исполнения распоряжений участников платежной системы;
- 4) осуществление расчета в платежной системе до конца рабочего дня;
- 5) осуществление расчета в пределах предоставленных участниками платежной системы денежных средств;
- 6) обеспечение возможности предоставления кредита;
- 7) использование безотзывных банковской гарантии или аккредитива;
- 8) другие способы управления рисками, предусмотренные правилами платежной системы.

Таким образом, финансовые риски, возлагаемые на каждого из участника платежной системы, становятся контролируруемыми, и при должном контроле риск дефолта платежной системы сведен к минимуму.

10.2. КОММЕНТАРИИ К СТАТЬЯМ ЗАКОНА ОБ НПС

ОСНОВНЫЕ ПОНЯТИЯ (СТ. 3)

Статью 3 Закона, в которой даются основные понятия, используемые в данном законе, и в том числе определения участников НПС (см. табл. 10.1), необходимо читать с поправкой на то, что определения, данные в ней, не являются исчерпывающими. Более того — их конкретизация в последующих статьях Закона может существенно корректировать данные в ст. 3 определения. Например, в п. 7 ст. 3 дается определение оператора услуг платежной инфраструктуры как операционного, платежного клирингового и расчетного центра. Понятиям операционного, платежного клирингового и расчетного центра в последующих пунктах статьи (8, 9, 11) тоже даются определения, также имеющие общий характер. И далее в ст. 16, полностью посвященной оператору услуг платежной инфраструктуры и требованиям к его деятельности, конкретизируется круг организаций — потенциальных и реальных операторов, причем наряду с общим делением организаций, имеющих право быть операторами, на кредитные организации и некредитные

организации называются две конкретные организации — Банк России и Внешэкономбанк.

И это не единственный пример — какие-то понятия исчерпывающе описаны в Законе в рамках одной статьи, некоторые — в двух или трех (см. табл. 10.1).

ПОРЯДОК УСЛУГ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА (СТ. 7, 9, 10, 12, 13)

Отметим следующую особенность отдельных статей: порядок оказания платежных услуг, связанных с использованием электронных средств платежа (ст. 7, 9, 10, 12, 13), не содержит никаких положений, связанных с переводом обычных денежных средств, поэтому представителям организаций, не занимающихся электронными платежами, можно не изучать данные статьи, пропуская их в полном объеме.

ТРЕБОВАНИЯ К ДЕЯТЕЛЬНОСТИ ОПЕРАТОРА ПРИ ПРИВЛЕЧЕНИИ БАНКОВСКОГО ПЛАТЕЖНОГО АГЕНТА (СТ. 14)

Начнем с того, что данная статья появилась в Законе об НПС в связи с тем, что теперь банкам как участникам национальной платежной системы разрешено иметь банковских платежных агентов и субагентов. По сути статья шире, чем обсуждаемый нами Закон, и относится, скорее, к Закону о банках и банковской деятельности. На взгляд автора, вместо ее включения в текст Закона об НПС было бы правильнее сделать отсылку к Закону о банках, но законодатели выбрали вариант с включением статьи в текст.

Статья 14 содержит два принципиальных новшества, которые способны серьезно изменить рынок:

1) предусмотрена возможность выдачи наличных денежных средств банковскими платежными агентами и субагентами. Правда, пока законодатель не разрешает использовать для выдачи полученную агентом выручку — ее надо сдавать в банк на специальный счет в полном объеме, а потом заново получить средства для выдачи наличных денежных средств. Однако в будущем данное положение открывает возможность выдачи кредитов и депозитов с помощью тех же терминалов приема наличных денежных средств;

2) предусмотрена возможность банку работать через субагентов. Раньше это было запрещено, что ставило банки в неравное положение с обычными платежными агентами, работающими по Закону № 103-ФЗ. Отметим, что пока использование данного преимущества затруднено, поскольку Банком России еще не полностью обновлена соответствующая нормативная база, но это вопрос времени.

Положения Закона начиная со ст. 18 пока не вступили в силу, не имеют правоприменительной практики и комментировать их пока не имеет смысла. Прокомментируем один важный нормативный акт Банка России — Инструкцию № 135-И¹.

¹ Ранее действовала Инструкция Банка России от 14 января 2004 г. № 109-И.

ОПЕРАТОРЫ ПЛАТЕЖНЫХ СИСТЕМ И ТРЕБОВАНИЯ К ИХ ДЕЯТЕЛЬНОСТИ (СТ. 15)

Оператор платежной системы по сути является организатором и «руководящим звеном» этой системы.

Оператором платежной системы может стать:

- кредитная организация;
- организация, не являющаяся кредитной организацией и созданная в соответствии с законодательством Российской Федерации;
- Банк России;
- Внешэкономбанк.

Оператор платежной системы обязан:

- определять правила платежной системы, организовывать и осуществлять контроль за их соблюдением участниками платежной системы, операторами услуг платежной инфраструктуры;
- осуществлять привлечение операторов услуг платежной инфраструктуры исходя из характера и объема операций в платежной системе, обеспечивать контроль за оказанием услуг платежной инфраструктуры участникам платежной системы, а также вести перечень операторов услуг платежной инфраструктуры;
- организовывать систему управления рисками в платежной системе, осуществлять оценку и управление рисками;
- обеспечивать возможность досудебного и (или) третейского рассмотрения споров с участниками платежной системы и операторами услуг платежной инфраструктуры в соответствии с правилами платежной системы.

Если оператор платежной системы не является кредитной организацией, он обязан привлечь в качестве расчетного центра кредитную организацию, которая не менее одного года осуществляет перевод денежных средств по открытым в этой кредитной организации банковским счетам. Кроме того, к таким организациям, намеревающимся стать операторами платежных систем, выставляются определенные требования, связанные с величиной чистых активов и некоторыми характеристиками руководителей высшего уровня.

Организация, намеревающаяся стать оператором платежной системы, направляет в Банк России регистрационное заявление в сопровождении пакета документов, перечень которых установлен отдельно для кредитных и прочих организаций (у последних список необходимых документов вдвое длиннее).

В течение 30 дней со дня получения регистрационного заявления Банк России принимает решение о регистрации претендента в качестве оператора платежной системы либо решение об отказе в такой регистрации.

Отказ в регистрации организации в качестве оператора платежной системы со стороны ЦБ РФ должен быть мотивированным. Перечень оснований для отказа является закрытым и также дифференцирован для кредитных и некредитных организаций.

Одна и та же организация может быть зарегистрирована как оператор нескольких платежных систем.

Законом предусмотрен закрытый перечень оснований, по которым Банк России вправе принимать решение об исключении сведений об организации из реестра операторов платежных систем. Более того, имеется специальная оговорка о том, что по иным основаниям исключение организаций из реестра не допускается.

Операторы различных платежных систем могут заключить договор о взаимодействии своих платежных систем (при условии отражения порядка такого взаимодействия в правилах платежных систем).

Кредитным организациям, являющимся операторами по переводу денежных средств (т.е. практически всем действующим кредитным организациям, обладающим лицензиями на осуществление банковских операций), следует обратить внимание на п. 39 ст. 15, согласно которому при определенном стечении обстоятельств может возникнуть необходимость зарегистрировать новую платежную систему в принудительном порядке:

«Оператор по переводу денежных средств, за исключением Банка России, у которого открыты банковские счета не менее трех других операторов по переводу денежных средств и между этими счетами осуществляются переводы денежных средств в течение трех месяцев подряд в размере, превышающем значение, установленное Банком России, обязан обеспечить в соответствии с требованиями настоящей статьи направление в Банк России заявления о регистрации оператора платежной системы в течение 30 дней после дня начала соответствия указанному требованию. По истечении четырех месяцев после дня начала соответствия указанному требованию осуществление перевода денежных средств между банковскими счетами операторов по переводу денежных средств, открытыми у такого оператора по переводу денежных средств, допускается только в рамках платежной системы».

Речь идет о корреспондентских счетах ЛОРО, которые кредитные организации открывают друг у друга для осуществления собственных и клиентских расчетов. Количество таких счетов в зависимости от величины банка и степени его активности на межбанковском рынке может колебаться от нуля до нескольких сотен, а объем оборотов по ним — и вовсе величина неограниченная.

Таким образом, если объем взаимных расчетов между четырьмя и более банками превысит установленное (на данный момент — пока неизвестное) значение, они должны объявить себя платежной системой, зарегистрироваться в установленном порядке и дальше продолжать деятельность в соответствии с Законом об НПС.

Очевидно, таким способом регулятор пытается не допустить появления на рынке и функционирования «скрытых» платежных систем и незарегистрированных операторов таких платежных систем.

ОПЕРАТОРЫ УСЛУГ ПЛАТЕЖНОЙ ИНФРАСТРУКТУРЫ (СТ. 16)

К операторам услуг платежной инфраструктуры (далее — оператор УПИ) относятся:

- операционный центр;

- платежный клиринговый центр;
- расчетный центр.

О возможности и даже необходимости участия в расчетах указанных организаций Банк России заявлял еще 16 лет назад. Как указывалось в Стратегии развития платежной системы России, утвержденной Советом директоров Банка России (Протокол № 15 от 1 апреля 1996 г.), регулятор *«не намерен монополизировать систему расчетов в России, будучи уверенным в том, что в рыночной экономике есть место для негосударственных расчетных и клиринговых палат, в первую очередь для организации расчетов на финансовых и товарных рынках и осуществления расчетов с большими встречными обязательствами кредитных учреждений внутри замкнутой группы участников»*.

Под *замкнутой группой участников*, очевидно, подразумевался аналог современной платежной системы в терминах Закона: совокупность организаций, взаимодействующих по правилам платежной системы в целях осуществления перевода денежных средств, включающая оператора платежной системы, операторов услуг платежной инфраструктуры и участников платежной системы, из которых как минимум три организации являются операторами по переводу денежных средств.

Следует отметить, что расчетный центр и платежный клиринговый центр должны быть созданы в соответствии с законодательством РФ, т.е. фактически должны быть расположены на территории РФ и являться резидентами с точки зрения законодательства о валютном регулировании и валютном контроле.

Что же касается операционного центра, то в отношении этого участника расчетов требование о резидентстве отсутствует — таким образом, обеспечивается взаимодействие с международными платежными системами (в частности, с VISA и MasterCard, на которые приходится до 90% российского рынка банковских карт) с минимальными издержками.

Согласно п. 1 ст. 16 Закона об НПС, оператором УПИ может являться:

- кредитная организация;
- организация, не являющаяся кредитной организацией;
- Банк России;
- Внешэкономбанк.

Оператор УПИ (кроме организаций, не являющихся кредитными организациями) может совмещать оказание операционных услуг, услуг платежного клиринга и расчетных услуг, в том числе в рамках одной организации. Кроме того, он может совмещать указанную деятельность с деятельностью оператора по переводу денежных средств (далее — оператор по ПДС), оператора платежной системы (далее — оператор ПС) и иной деятельностью, не противоречащей законодательству Российской Федерации.

Организации, не являющиеся кредитными, могут совмещать оказание операционных услуг и услуг платежного клиринга. Они также могут совмещать указанную деятельность с деятельностью оператора ПС и иной деятельностью, не противоречащей законодательству Российской Федерации.

Банк России осуществляет деятельность оператора УПИ на основании Закона об НПС в соответствии с нормативными актами Банка России и заключаемыми договорами.

Остальные операторы УПИ осуществляют свою деятельность в соответствии с правилами платежной системы и договорами, заключенными с участниками платежной системы и другими операторами УПИ.

Правилами платежной системы должны определяться требования к операторам УПИ, с которыми могут заключаться договоры в соответствии с Законом.

В частности, в отношении операторов УПИ должны быть определены требования к их финансовому состоянию, технологическому обеспечению и другим факторам, обеспечивающим бесперебойность функционирования платежной системы.

Указанные требования должны:

- быть объективными (реальными, лишенными предвзятости);
- быть доступными для публичного ознакомления;
- обеспечивать равноправный доступ операторов УПИ в платежную систему.

Операторы УПИ обязаны предоставлять оператору ПС информацию о своей деятельности (в части оказания услуг платежной инфраструктуры) в соответствии с правилами платежной системы.

После 30 июня 2014 г. (по истечении трех лет со дня официального опубликования Закона об НПС) при осуществлении переводов денежных средств в рамках платежной системы операторами по ПДС, находящимися на территории Российской Федерации, должны привлекаться операторы УПИ, которые соответствуют требованиям Закона об НПС и находятся на территории Российской Федерации. Исключение из этого требования сделано лишь для операционных центров (но в этом случае оператор ПС несет ответственность за надлежащее оказание операционных услуг участникам платежной системы).

Здесь, кстати, следует отметить некоторое несоответствие между отдельными статьями Закона об НПС. В соответствии с п. 7 ст. 38 рассматриваемого документа *«Положения части 11 статьи 16 и пункта 3 части 12 статьи 21 настоящего Федерального закона в части привлечения операционного центра и (или) платежного клирингового центра применяются по истечении трех лет после дня опубликования настоящего Федерального закона»*. При этом, однако, в указанных частях и пунктах речь идет только о привлечении оператором платежной системы операционного центра, находящегося за пределами Российской Федерации, и нет даже намека на возможность участия в российских платежных системах платежных клиринговых центров, являющихся нерезидентами.

ОПЕРАЦИОННЫЙ ЦЕНТР (СТ. 17)

Операционный центр (далее — ОЦ) обеспечивает в рамках платежной системы для ее участников и их клиентов доступ к услугам по переводу денежных средств, в том числе с использованием электронных средств платежа, а также обмен электронными сообщениями.

ОЦ осуществляет свою деятельность в соответствии с правилами платежной системы и на основании договоров с оператором ПС, участниками платежной системы, платежным клиринговым центром и расчетным центром, если заключение таких договоров предусмотрено правилами платежной системы.

ОЦ может быть создан как в соответствии с законодательством Российской Федерации, так и в соответствии с законодательством других государств. Таким образом, первоначальные намерения части разработчиков Закона, связанные с запретом передачи данных о внутрироссийских транзакциях за рубеж, так и остались на данный момент нереализованными (соответствующие поправки в законопроект были внесены ко второму чтению).

Кроме того, из окончательной редакции Закона исчезли ограничения, связанные с правом ОЦ передавать информацию по переводам денежных средств, осуществляемых на территории Российской Федерации, на территорию иностранного государства или предоставлять доступ к ней с территории иностранного государства. В первоначальном варианте такая возможность допускалась в двух случаях:

1) в случае резервного хранения указанной информации с правом ее передачи на территорию Российской Федерации или доступа с территории Российской Федерации, в том числе в целях восстановления информации или подтверждения осуществленных переводов денежных средств, без права операционного центра иностранного государства, осуществляющего резервное хранение информации, по ее передаче на территорию третьих государств;

2) в случае передачи информации по переводу денежных средств с использованием платежной карты в части суммы, валюты перевода, а также данных, идентифицирующих платежную карту (за исключением фамилии, имени, отчества клиента), и техническое устройство, применяемое при осуществлении указанного перевода денежных средств.

Следует напомнить, что вопрос возможного ограничения деятельности международных платежных систем в России неоднократно поднимался в течение как минимум двух лет до обнародования законопроекта и был, собственно, одной из основных причин его появления. О необходимости снижения зависимости от международных платежных систем в декабре 2009 г. заявлял президент Дмитрий Медведев. Закон об НПС Минфин России несколько раз переписывал, во внесенном в Госдуму варианте об особых требованиях к иностранным компаниям уже не говорилось ни слова. В декабре 2010 г. законопроект прошел первое чтение, несмотря на серьезную критику со стороны депутатов. В новой версии законопроекта, подготовленной ко второму чтению в марте, снова появились положения о безопасности информации по операциям российских граждан, что вызвало обеспокоенность VISA и MasterCard. Тогда представители компаний заявляли, что строительство всей инфраструктуры в России потребует крупных финансовых затрат, что приведет к удорожанию услуг для потребителей. Депутаты в свою очередь указывали, что серьезным поводом для беспокойства

является ситуация, когда 90% рынка принадлежит иностранным компаниям, которые не контролируются российскими регуляторами.

В результате был достигнут относительный компромисс — из трех видов операторов УПИ два должны быть «чисто российскими», т.е. поднадзорными Банку России и отечественным правоохранительным органам, а ответственность за деятельность иностранных ОЦ будет нести российский оператор платежной системы.

Поскольку зарубежные ОЦ не попадают в сферу контроля и регулирования Банка России, ответственность за оказание ими услуг надлежащего качества несет оператор ПС, привлечший такой ОЦ.

В платежной системе может быть один или несколько ОЦ.

Технология оказания услуг операционным центром

При обеспечении доступа клиентам — участникам платежной системы к услугам по переводу денежных средств ОЦ обязан обеспечивать клиентам возможность передачи платежных распоряжений участнику платежной системы с использованием согласованных договором технических средств и способов.

Обмен электронными сообщениями включает в себя:

- получение операционным центром электронных сообщений, содержащих распоряжения участников платежной системы;
- передачу указанных сообщений в платежный клиринговый центр, расчетный центр;
- передачу извещений (подтверждений) о приеме и об исполнении распоряжений участников платежной системы.

ОЦ обеспечивает обмен электронными сообщениями:

- между участниками платежной системы;
- участниками платежной системы и их клиентами, платежным клиринговым центром, расчетным центром;
- платежным клиринговым центром и расчетным центром.

ОЦ может осуществлять иные действия, связанные с использованием информационно-коммуникационных технологий, необходимые для функционирования платежной системы и предусмотренные правилами платежной системы.

Ответственность операционного центра

ОЦ несет ответственность за реальный ущерб, причиненный участникам платежной системы, платежному клиринговому центру и расчетному центру вследствие неоказания (ненадлежащего оказания) операционных услуг.

Правилами платежной системы и договором об оказании операционных услуг ответственность ОЦ за реальный ущерб может быть ограничена размером неустойки, за исключением случаев умышленного неоказания (ненадлежащего оказания) операционных услуг.

В случае если правилами платежной системы и договором об оказании операционных услуг предусмотрена обязанность ОЦ обеспечить гарантированный уровень бесперебойности оказания операционных услуг в течение определенного времени, могут быть установлены ответственность ОЦ за реальный ущерб и неустойка.

Оператор ПС в случаях и порядке, предусмотренных правилами платежной системы, вправе привлекать ОЦ, находящийся за пределами Российской Федерации, для оказания операционных услуг участникам платежной системы. В данном случае, как уже было сказано, оператор ПС несет ответственность за надлежащее оказание операционных услуг участникам платежной системы.

Банк России имеет право ограничить (приостановить) своим предписанием оказание операционных услуг ОЦ (в том числе при привлечении ОЦ, находящегося за пределами Российской Федерации) в случае, если нарушение требований Закона об НПС или принятых в соответствии с ним нормативных актов Банка России поднадзорной ему организацией (в данном случае — оператором ПС) влияют на бесперебойность функционирования платежной системы либо на услуги, оказываемые участникам платежной системы и их клиентам.

ПЛАТЕЖНЫЙ КЛИРИНГОВЫЙ ЦЕНТР (СТ. 18)

Платежный клиринговый центр (далее — ПКЦ) обеспечивает в рамках платежной системы оказание услуг платежного клиринга, в том числе:

- прием к исполнению распоряжений участников платежной системы об осуществлении перевода денежных средств;
- определение платежных клиринговых позиций участников платежей — сумм денежных средств, подлежащих списанию и зачислению расчетным центром по банковским счетам участников платежной системы;
- передачу расчетному центру от имени участников платежной системы подлежащих исполнению распоряжений участников платежной системы;
- выполнение иных действий, предусмотренных Законом об НПС.

Функции ПКЦ в отличие от функций операционного центра может выполнять только организация, созданная в соответствии с законодательством Российской Федерации.

ПКЦ осуществляет свою деятельность в соответствии с правилами платежной системы и на основании договоров об оказании услуг платежного клиринга¹, заключаемых с участниками платежной системы, ОЦ и расчетным центром, если заключение таких договоров предусмотрено правилами платежной системы.

В платежных системах, в рамках которых осуществляются переводы денежных средств по сделкам, совершенным на организованных торгах, услуги платежного клиринга могут оказываться в рамках клиринговой услуги клиринговой организацией, осуществляющей свою деятельность в соответствии с Законом о клиринге.

¹ Образцы таких договоров уже представлены в некоторых информационно-правовых системах.

В целом Закон о клиринге не распространяется на отношения, возникающие при осуществлении клиринга в соответствии с Законом об НПС (п. 2 ст. 1 Закона о клиринге). Тем не менее из него можно почерпнуть некоторую полезную информацию при составлении типовых договоров об оказании услуг платежного клиринга и разработке технологических решений этого процесса.

В частности, само определение **клиринга** как *«определения подлежащих исполнению обязательств, возникших из договоров, в том числе в результате осуществления неттинга обязательств, и подготовки документов (информации), являющихся основанием прекращения и (или) исполнения таких обязательств»* вполне соответствует как духу, так и букве Закона об НПС, тем более что в самом Законе определение клиринга отсутствует.

В платежной системе может быть один или несколько ПКЦ.

Договор об оказании услуг платежного клиринга, заключаемый с участниками платежной системы, является договором присоединения (договором, условия которого определены одной стороной в формулярах или иных стандартных формах и могут быть приняты другой стороной не иначе как путем присоединения к предложенному договору в целом).

В соответствии с договором об оказании услуг платежного клиринга, заключаемым с расчетным центром, ПКЦ обязуется передавать расчетному центру от имени участников платежной системы подлежащие исполнению распоряжения участников платежной системы.

ТЕХНОЛОГИЯ ОСУЩЕСТВЛЕНИЯ ПЛАТЕЖНОГО КЛИРИНГА (СТ. 25)

Платежный клиринг в платежной системе осуществляется ПКЦ посредством:

а) выполнения процедур приема к исполнению распоряжений участников платежной системы, включая:

- проверке соответствия распоряжений участников платежной системы установленным требованиям,
- определению достаточности денежных средств для исполнения распоряжений участников платежной системы,
- определению платежных клиринговых позиций;

б) передачи расчетному центру для исполнения принятых распоряжений участников платежной системы;

в) направления участникам платежной системы извещений (подтверждений), касающихся приема к исполнению распоряжений участников платежной системы, а также передачи извещений (подтверждений), касающихся исполнения распоряжений участников платежной системы.

Процедуры приема к исполнению распоряжений участников платежной системы выполняются ПКЦ в соответствии с правилами платежной системы.

Определение платежной клиринговой позиции участника платежной системы может осуществляться на валовой основе и (или) на нетто-основе.

Платежная клиринговая позиция **на валовой основе** определяется в размере суммы индивидуального распоряжения участника платежной системы или общей суммы распоряжений участников платежной системы, по которым участник платежной системы является плательщиком или получателем средств.

После определения платежной клиринговой позиции на валовой основе распоряжения участников платежной системы передаются ПКЦ расчетному центру для исполнения.

Платежная клиринговая позиция **на нетто-основе** определяется в размере разницы между общей суммой подлежащих исполнению распоряжений участников платежной системы, по которым участник платежной системы является плательщиком, и общей суммой распоряжений участников платежной системы, по которым участник платежной системы является получателем средств.

После определения платежной клиринговой позиции на нетто-основе ПКЦ передает расчетному центру для исполнения распоряжения ПКЦ на сумму определенных платежных клиринговых позиций на нетто-основе участников платежной системы и (или) принятые распоряжения участников платежной системы.

Ответственность платежного клирингового центра

ПКЦ несет ответственность за убытки, причиненные участникам платежной системы и расчетному центру вследствие неоказания (ненадлежащего оказания) услуг платежного клиринга.

Правилами платежной системы и договором об оказании услуг платежного клиринга ответственность ПКЦ за убытки может быть ограничена размером неустойки, за исключением случаев умышленного неоказания (ненадлежащего оказания) услуг платежного клиринга.

В случаях если нарушения ПКЦ требований Закона об НПС или принятых в соответствии с ним нормативных актов Банка России влияют на бесперебойность функционирования платежной системы либо на услуги, оказываемые участникам платежной системы и их клиентам, Банк России может применить одну из следующих норм принуждения:

- направить предписание об устранении нарушения с указанием срока для его устранения;
- ограничить (приостановить) предписанием оказание услуг платежного клиринга.

Центральный платежный клиринговый контрагент

ПКЦ, выступающий в соответствии с Законом об НПС плательщиком и получателем средств по переводам денежных средств участников платежной системы, называется **центральным платежным клиринговым контрагентом** (далее — ЦПКК).

На практике это означает, что ЦПКК совмещает функции ПКЦ и расчетного центра, т.е. не только определяет размеры взаимных обязательств участников

платежной системы (платежные клиринговые позиции), но и осуществляет расчеты между ними. При этом не исключается возможность участия в платежной системе других ПКЦ и других расчетных центров.

ЦПКК может выступать кредитная организация, Банк России или Внешэкономбанк в порядке, предусмотренном правилами платежной системы и договорами об оказании услуг платежного клиринга.

ЦПКК обязан:

- обладать денежными средствами, достаточными для исполнения своих обязательств, либо обеспечивать исполнение своих обязательств, в том числе за счет гарантийного фонда, в размере наибольшего обязательства, по которому ЦПКК становится плательщиком, за период, определяемый правилами платежной системы;
- ежедневно осуществлять контроль за рисками неисполнения (ненадлежащего исполнения) участниками платежной системы своих обязательств по переводу денежных средств;
- применять в отношении участников платежной системы, анализ финансового состояния которых свидетельствует о повышенном риске, ограничительные меры, включая установление максимального размера платежной клиринговой позиции, и предъявлять требования о повышенном размере обеспечения исполнения обязательств участников платежной системы по переводу денежных средств.

Исходя из перечня функций и требований к ЦПКК можно сделать вывод о том, что в каждой платежной системе может быть только один ЦПКК. В то же время платежная система может и вовсе не иметь ЦПКК — его функции в этом случае делят между собой ПКЦ и расчетный центр (расчетные центры).

РАСЧЕТНЫЙ ЦЕНТР (СТ. 19)

Расчетный центр (далее — РЦ) — организация, созданная в соответствии с законодательством Российской Федерации, обеспечивающая в рамках платежной системы расчетные услуги.

К расчетным услугам, согласно Закону об НПС, относятся следующие виды деятельности:

- исполнение распоряжений участников платежной системы посредством списания и зачисления денежных средств по банковским счетам участников платежной системы;
- направление подтверждений, касающихся исполнения распоряжений участников платежной системы.

РЦ может выступать кредитная организация, Банк России или Внешэкономбанк.

В платежной системе может быть один или несколько РЦ.

РЦ осуществляет свою деятельность в соответствии с правилами платежной системы и на основании:

- договоров банковского счета, заключаемых с участниками платежной системы и (или) ЦПКК (при его наличии);
- договоров, заключаемых с ОЦ и ПКЦ, если заключение таких договоров предусмотрено правилами платежной системы.

РЦ исполняет поступившие от ПКЦ распоряжения участников платежной системы посредством списания и зачисления денежных средств по банковским счетам участников платежной системы и (или) банковскому счету ЦПКК (при его наличии).

Если услуги платежного клиринга оказываются клиринговой организацией, осуществляющей свою деятельность в соответствии с Законом о клиринге, то РЦ платежной системы может исполнять распоряжения участников платежной системы, поступившие от такой клиринговой организации.

Технология осуществления расчетных услуг

Расчет в платежной системе осуществляется РЦ посредством списания и зачисления денежных средств по банковским счетам участников платежной системы и (или) ЦПКК на основании поступивших от ПКЦ распоряжений в размере сумм определенных платежных клиринговых позиций.

Ответственность расчетного центра

Ответственность РЦ действующей редакцией Закона об НПС не предусмотрена. Таким образом, если не будут внесены изменения в Закон, она будет определяться общегражданским законодательством, правилами платежной системы и условиями заключенных договоров.

ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЮ ПЛАТЕЖНЫХ СИСТЕМ

Стоит напомнить, что перечисленные ниже требования (за исключением обеспечения банковской тайны в платежных системах) вступают в силу с 1 июля 2012 г. С этой даты все действующие и вновь образуемые платежные системы должны соответствовать требованиям к их организации и функционированию, установленным ст. 20—30 Закона об НПС.

В число указанных требований входят:

- требования к составу, форме, доступности, порядку применения и некоторым другим аспектам правил платежной системы (ст. 20);
- требования к участникам платежной системы (ст. 21);
- порядок признания платежной системы значимой, требования к значимой платежной системе и особенности функционирования таких платежных систем (ст. 22—24);
- требования по обеспечению банковской тайны и защиты информации в платежных системах (ст. 26—27);

- правила управления рисками в платежных системах (ст. 28);
- порядок обеспечения исполнения обязательств участников платежных систем (включая порядок формирования и использования гарантийного фонда) (ст. 29—30).

ПРАВИЛА ПЛАТЕЖНОЙ СИСТЕМЫ (СТ. 20)

Закон об НПС определяет **правила платежной системы** как документ (документы), содержащий (содержащие) условия:

- участия в платежной системе;
- осуществления переводов денежных средств;
- оказания услуг платежной инфраструктуры;
- иные условия, определяемые оператором платежной системы в соответствии с Законом об НПС.

Перечень информации, которая должна быть включена в правила платежной системы, установлен п. 1 ст. 20 Закона об НПС и включает 22 позиции. Список этот не закрыт: согласно п. 2 той же ст. 20, правилами могут быть предусмотрены «другие положения, необходимые для обеспечения функционирования платежной системы».

Многие из позиций (например, «система управления рисками в платежной системе, включая используемую модель управления рисками, перечень мероприятий и способов управления рисками» или «порядок взаимодействия в рамках платежной системы в спорных и чрезвычайных ситуациях»), разработанные должным образом, представляют собой полноценные внутренние процедуры (положения), разработка и согласование которых могут занять не один месяц. В связи с этим операторам платежных систем, ответственным за разработку правил, следует позаботиться об этом заранее.

Помимо перечня обязательной информации законодатели предусмотрели для правил платежных систем список ограничений, которые устанавливать запрещается (в частности, нельзя устанавливать требования к участникам платежной системы о неучастии в других платежных системах — так называемые условия об исключительном участии).

Правила расчетной системы прилагаются к регистрационному заявлению организации, намеревающейся стать оператором платежной системы.

В случае изменения правил платежной системы оператор платежной системы обязан представить в Банк России информацию об этом (включая сами изменения) не позднее десяти дней со дня их внесения.

Правила платежной системы могут быть составлены в виде единого документа или нескольких взаимосвязанных документов.

Оператор платежной системы обязан предоставлять организациям, намеревающимся участвовать в платежной системе, правила платежной системы для предварительного ознакомления без взимания платы (за исключением расходов на изготовление копий правил).

Правила платежной системы, включая тарифы, являются публично доступными. Оператор ПС вправе не раскрывать информацию о требованиях к защите информации и информацию, доступ к которой ограничен в соответствии с федеральным законом.

Участники платежной системы присоединяются к правилам платежной системы только путем принятия их в целом.

Законодателем предусмотрено право оператора платежной системы в одностороннем порядке вносить изменения в правила платежной системы при условии:

1) обеспечения участникам платежной системы возможности предварительного ознакомления с предлагаемыми изменениями и направления своего мнения оператору платежной системы в установленный им срок, который не может быть менее одного месяца;

2) установления срока внесения изменений не менее одного месяца со дня окончания указанного выше срока.

У некоторых экспертов такая формулировка уже вызвала тревогу. «Поскольку о последующих действиях и связанных с ними правах участников более ничего не сказано, можно сделать вывод, что оператор получил реальное право диктовать участникам системы свои условия, избавляться от неудобных и решать иные организационные задачи», — пишет доцент филиала СГЮА (СГАП) И. Иванов в статье «Виртуальные деньги теперь в законе» (ЭЖ-Юрист. 2011. № 37).

Правила платежной системы Банка России определяются нормативными актами Банка России на основании Закона об НПС.

Особенности правил платежных систем, в рамках которых осуществляются переводы денежных средств по сделкам, совершенным на организованных торгах, устанавливаются Банком России по согласованию с уполномоченным федеральным органом исполнительной власти.

УЧАСТНИКИ ПЛАТЕЖНОЙ СИСТЕМЫ (СТ. 21)

Участниками платежной системы могут стать следующие организации (при условии их присоединения к правилам платежной системы в порядке, установленном правилами платежной системы):

1) операторы по переводу денежных средств (включая операторов электронных денежных средств);

2) профессиональные участники рынка ценных бумаг, а также юридические лица, являющиеся участниками организованных торгов и (или) участниками клиринга в соответствии с Законом о клиринге;

3) страховые организации, осуществляющие обязательное страхование гражданской ответственности в соответствии с законодательством Российской Федерации;

4) органы Федерального казначейства;

5) организации Федеральной почтовой связи.

В случае заключения между операторами платежных систем договора о взаимодействии платежных систем участниками платежной системы могут являться ЦПКК и (или) РЦ другой платежной системы, действующие по поручению оператора такой платежной системы. При этом платежный клиринг и расчет в целях перевода денежных средств между участниками одной платежной системы осуществляются соответственно платежным клиринговым центром и расчетным центром этой платежной системы, если иное не предусмотрено договором о взаимодействии между платежными системами.

Платежный клиринг и расчет в целях перевода денежных средств между участниками различных платежных систем осуществляются в порядке, предусмотренном договором о взаимодействии между платежными системами.

Участниками платежной системы могут являться международные финансовые организации, иностранные центральные (национальные) банки, иностранные банки.

Правилами платежной системы должно быть предусмотрено:

- прямое участие в платежной системе;
- косвенное участие в платежной системе.

Правилами платежной системы также могут быть предусмотрены различные виды прямого и косвенного участия в платежной системе.

Прямое участие в платежной системе требует открытия в РЦ банковского счета организации, становящейся прямым участником, в целях осуществления расчета с другими участниками платежной системы.

Прямыми участниками платежной системы могут являться:

- операторы по переводу денежных средств, включая операторов электронных денежных средств;
- профессиональные участники рынка ценных бумаг;
- юридические лица, являющиеся участниками организованных торгов и (или) участниками клиринга в соответствии с Законом о клиринге (при осуществлении ими переводов денежных средств по сделкам, совершенным на организованных торгах);
- страховые организации, осуществляющие обязательное страхование гражданской ответственности в соответствии с законодательством Российской Федерации (при осуществлении ими расчетов по обязательным видам страхования гражданской ответственности);
- органы Федерального казначейства.

Косвенное участие в платежной системе требует открытия косвенному участнику (организации, имеющей право быть участником платежной системы) банковского счета прямым участником платежной системы, являющимся оператором по переводу денежных средств, в целях осуществления расчета с другими участниками платежной системы.

Отношения между прямыми и косвенными участниками платежной системы регулируются правилами платежной системы и заключенными договорами банковского счета.

Для каждого вида участия в платежной системе ее правилами устанавливаются отдельные критерии участия, которые должны включать доступные для публичного ознакомления требования, обеспечивающие равноправный доступ участников платежной системы одного вида в платежную систему. Указанные требования могут касаться финансового состояния, технологического обеспечения и других факторов, влияющих на бесперебойность функционирования платежной системы.

ЗНАЧИМАЯ ПЛАТЕЖНАЯ СИСТЕМА (СТ. 22–24)

Платежная система может быть признана **системно значимой** или **социально значимой**.

Для признания платежной системы значимой достаточно соответствия одному из критериев, разработанных Банком России для системно значимых и социально значимых платежных систем.

Информация о признании платежной системы значимой включается в реестр операторов платежных систем. С этого момента на оператора такой платежной системы возлагаются дополнительные требования и функции, предусмотренные ст. 22 и 24 Закона об НПС.

Для Банка России Законом установлен специальный порядок проверки соответствия правил значимой платежной системы установленным требованиям (ст. 23 Закона об НПС).

Для исключения значимой кредитной организаций из числа «избранных» необходимо, чтобы она в течение шести календарных месяцев не соответствовала ни одному из критериев значимости, установленных Банком России.

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ПЛАТЕЖНОЙ СИСТЕМЕ (СТ. 27)

Все участники платежной системы — операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы УПИ обязаны обеспечивать защиту информации:

- о средствах и методах обеспечения информационной безопасности;
- о персональных данных;
- об иной информации, подлежащей обязательной защите в соответствии с российским законодательством.

Требования к защите указанной информации устанавливает Правительство РФ. В свою очередь контроль и надзор за выполнением этих требований осуществляются:

- федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (Федеральной службой безопасности РФ);
- федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты ин-

формации (Федеральной службой по техническому и экспортному контролю РФ).

Контроль и надзор за обеспечением защиты информации в платежной системе осуществляются указанными федеральными органами в пределах их полномочий и без права ознакомления с защищаемой информацией.

УПРАВЛЕНИЕ РИСКАМИ В ПЛАТЕЖНОЙ СИСТЕМЕ (СТ. 28)

Под **системой управления рисками** в платежной системе понимается комплекс мероприятий и способов снижения вероятности возникновения неблагоприятных последствий для бесперебойности функционирования платежной системы с учетом размера причиняемого ущерба.

Оператор платежной системы определяет одну из трех организационных моделей управления рисками в платежной системе, которая будет использоваться в платежной системе:

- 1) самостоятельное управление рисками в платежной системе оператором платежной системы;
- 2) распределение функций по оценке и управлению рисками между оператором платежной системы, операторами услуг платежной инфраструктуры и участниками платежной системы;
- 3) передача функций по оценке и управлению рисками оператором платежной системы, не являющимся кредитной организацией, расчетному центру.

Законодатель определил перечень обязательных мероприятий, включаемых в систему управления рисками, а также возможные способы управления рисками.

ОБЕСПЕЧЕНИЕ ИСПОЛНЕНИЯ ОБЯЗАТЕЛЬСТВ УЧАСТНИКОВ ПЛАТЕЖНОЙ СИСТЕМЫ (СТ. 29, 30)

Правилами платежной системы должен быть установлен порядок обеспечения исполнения обязательств участников платежной системы.

Одним из способов обеспечения исполнения таких обязательств является создание гарантийного фонда, который используется для удовлетворения требований по обязательствам в случае их неисполнения (ненадлежащего исполнения) участником платежной системы.

Гарантийный фонд платежной системы учитывается на отдельном банковском счете, открываемом оператору платежной системы, ЦПКК или участникам платежной системы в соответствии со ст. 20 Закона об НПС.

На денежные средства, находящиеся на счете гарантийного фонда платежной системы, не может быть наложен арест по долгам оператора платежной системы, ЦПКК или участника платежной системы. Также не могут быть приостановлены операции по указанному счету, в том числе по основаниям, предусмотренным законодательством Российской Федерации о налогах и сборах.

КОММЕНТАРИЙ К ИНСТРУКЦИИ БАНКА РОССИИ № 135-И

В числе уже вышедших нормативных актов Банка России, имеющих прямое отношение к Закону об НПС, Инструкция № 135-И, которая изменила порядок лицензирования НКО. В числе прочего Инструкцией предусмотрен новый тип лицензии, который фактически позволяет НКО работать как платежной системе. Таким образом, у действующих (и будущих) российских платежных систем по приему наличных платежей есть выбор, в каком статусе работать на рынке — либо в статусе платежной системы согласно Закону № 161-ФЗ, либо получить лицензию НКО Банка России. Последний вариант имеет несколько преимуществ. Во-первых, у НКО есть только один регулятор — Банк России. Банковская система работает уже более 20 лет, система взаимоотношений ЦБ РФ с поднадзорными кредитными организациями давно сложилась и устоялась, тогда как Закон № 161-ФЗ у регуляторов больше соблазнов толковать «в свою пользу». Во-вторых, НКО имеет право открывать клиентам — юридическим лицам счета. Это дает возможность аккумулировать средства клиентов, а кроме того, не отдавать клиентскую базу на сторону, в банк-оператор. Последнее обстоятельство — дополнительная гарантия, что клиента не «уведут». Из минусов работы платежной системы в форме НКО (табл. 10.3) — большие требования к размеру уставного капитала — 18 млн руб. (для платежных систем в рамках Закона об НПС — порядка 10 млн руб.).

Таблица 10.3

Сравнение преимуществ и недостатков различных вариантов работы платежной системы

| Категория | ООО без лицензий (ПА/БПА) | ООО с лицензией ПС | НКО с расчетной лицензией (8.3.1) | НКО с лицензией под ПС (8.3.4) |
|--|---------------------------|--------------------|-----------------------------------|--------------------------------|
| Отсутствие больших затрат на содержание | + | + | – | – |
| Возможность хранить остатки дилеров | + | – | + | + |
| Возможность хранить остатки субдилеров и иных клиентов | – | – | + | – |
| Возможность заводить субдилеров | – | + | + | + |
| Возможность работать с электронными деньгами | – | + | + | + |

Окончание

| Категория | ООО без лицензий (ПА/БПА) | ООО с лицензией ПС | НКО с расчетной лицензией (8.3.1) | НКО с лицензией под ПС (8.3.4) |
|---|---------------------------------|--------------------------|--|--------------------------------------|
| Возможность инкассировать терминалы (кассы) в части выручки от платежей | – | – | + | + |
| Возможность проводить иные инкассации | – | – | + | – |
| Возможность проводить любые расчетные операции | – | – | + | – |
| Зависимость от банков-партнеров | + | + | – | – |
| Прозрачность для взаимодействия с банками | – | + | + | + |
| Защищенность клиентской базы | + | – | + | + |
| Возможность проводить валютные (конверсионные) операции | – | – | + | – |

Краткие выводы

Сформулируем некоторые выводы:

1) Законом № 161-ФЗ охвачены экономические отношения, стихийно сложившиеся на рынке, причем не запретительными мерами, а регулируемыми нормами;

2) впервые официально признано существование в экономическом обороте электронных денег¹;

3) вводятся элементы саморегулирования с внешним контролем платежных систем, рекомендациям по риск-менеджменту, что должно оздоровить рынок, позволить избежать платежным системам банкротства²;

¹ На взгляд автора, электронные деньги все-таки являются не собственно денежными средствами, а всего лишь вариантом безналичных расчетов.

² Отметим, что еще не до конца ясно, как именно будет реализован большой потенциал Закона по риск-менеджменту, ведь даже крупные банки испытывают сложности с внедрением эффективной системы управления рисками.

4) в Законе есть предпосылки к выводу из тени «черного нала»¹;

5) процесс работы над Законом выявил определенные противоречия между государственными институтами, регулирующими финансовый рынок (в частности — между Минфином России и Банком России), которые не удалось преодолеть в полной мере, что, по всей видимости, во многом и предопределило противоречивость отдельных положений Закона.

Отметим в заключение, что, несмотря на некоторые недоработки (связанные, очевидно, с новизной регулируемого предмета и сложностью увязки положений Закона об НПС с уже сложившимся законодательным полем), данный Закон оказался востребован участниками российского рынка.

Приложение к главе 10

Перечень законодательных актов, в который вносятся изменения Законом № 162-ФЗ

1. Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» (в ред. Федерального закона от 3 февраля 1996 г. № 17-ФЗ).

2. Закон РФ от 21 марта 1991 г. № 943-1 «О налоговых органах Российской Федерации».

3. Закон РФ от 7 февраля 1992 г. № 2300-1 «О защите прав потребителей».

4. Федеральный закон от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг».

5. Налоговый кодекс Российской Федерации.

6. Бюджетный кодекс Российской Федерации.

7. Федеральный закон от 25 февраля 1999 г. № 40-ФЗ «О несостоятельности (банкротстве) кредитных организаций».

8. Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

9. Кодекс Российской Федерации об административных правонарушениях.

10. Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».

11. Федеральный закон от 22 мая 2003 г. № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт».

12. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

13. Федеральный закон от 10 декабря 2003 г. № 173-ФЗ «О валютном регулировании и валютном контроле».

14. Федеральный закон от 23 декабря 2003 г. № 177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации».

¹ Все больше свидетельств того, что эти предпосылки не сработали так эффективно, как этого хотелось законодателям.

15. Федеральный закон от 26 июля 2006 г. № 135-ФЗ «О защите конкуренции».

16. Федеральный закон от 2 октября 2007 г. № 229-ФЗ «Об исполнительном производстве».

17. Федеральный закон от 3 июня 2009 г. № 103-ФЗ «О деятельности по приему платежей физических лиц, осуществляемой платежными агентами».

18. Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

19. Федеральный закон от 27 ноября 2010 г. № 311-ФЗ «О таможенном регулировании в Российской Федерации».

ГЛАВА 11

РАЗВИТИЕ НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ В ДОЛГОСРОЧНОЙ ПЕРСПЕКТИВЕ

В данной главе мы рассмотрим дизайн и место в будущем обществе национальной платежной системы (далее — «перспективная НПС»¹). Сразу уточним, что под НПС в данной главе будет пониматься платежная система исключительно в узком смысле — как находящаяся под управлением государства подсистема, часть национальной технологической инфраструктуры, обеспечивающая предоставление на всей территории страны инфраструктурных платежно-расчетных сервисов для использования частными платежными системами в целях создания платежно-расчетных сервисов для конечных потребителей. Сами же частные платежные системы и конечные потребители платежно-расчетных сервисов в понятие НПС включаться не будут.

Понимая, что безошибочно угадать даже контуры общества будущего, а тем более разглядеть детали таких его составляющих, как НПС, невозможно, автор не претендует на точность и конечность заключений. Данная глава — скорее, попытка инициировать обсуждение вопроса предложением спорного ответа.

11.1. ТЕНДЕНЦИИ РАЗВИТИЯ И СОВРЕМЕННОЕ СОСТОЯНИЕ НПС

Анализируя динамику развития технологий платежей и расчетов, можно отметить, что в течение последних нескольких лет в большинстве развитых и развивающихся стран наблюдается исключительно высокий уровень активности в этой области. Это объясняется тем, что к настоящему времени накоплен огромный инновационный технологический потенциал, опережающий существующий уровень развития экономики и платежно-расчетных технологий, и тем самым созданы условия для «технологического скачка».

¹ Понятия, используемые автором в данной главе, и их трактовка приведены в конце. Поскольку понятийный аппарат в рассматриваемой предметной области окончательно не сложился, предложенные определения могут расходиться с определениями других авторов бизнес-энциклопедии.

Повышенное внимание к развитию именно НПС обусловлено тем, что НПС, являясь ключевым компонентом экономики любой страны, во многом определяет ее развитие и место, которое нация займет в мире. Кроме того, поскольку НПС является компонентом фундамента экономики, проектирование и внедрение НПС должно опережать развитие других составляющих экономики. Относительно небольшие, но правильные инвестиции в развитие НПС, сделанные сегодня, дадут огромный эффект в будущем. И наоборот, бездействие или неправильное развитие могут стоить очень дорого.

Обращает на себя внимание то, что, несмотря на либерально-рыночный характер экономики стран, наиболее успешно развивающих свои НПС, управление созданием НПС осуществляется далеко не рыночными методами и роль государства и наднациональных органов является определяющей.

Примером комплексного, эффективного, хорошо организованного и жестко управляемого государством (государствами) процесса проектирования НПС является Европейский союз, страны которого совместно работают над созданием инфраструктуры наднациональной европейской платежной системы¹.

В России сегодня не существует полнофункциональной НПС в понимании, предлагаемом в данной главе, т.е. покрывающей все потребности общества в инфраструктурных платежно-расчетных сервисах. В настоящее время в России есть два компонента (с точки зрения архитектуры перспективной НПС) — национальная система наличных денег и национальная система валовых расчетов (в виде расчетной системы Банка России). Два других существенных компонента — национальная система розничных платежей и национальная инвойсинговая система отсутствуют.

Поскольку рынок услуг не терпит пустоты, незаполненные ниши закрываются конкурирующими друг с другом, слабоинтегрированными российскими и зарубежными частными платежными системами. Данные системы, рассматриваемые вместе, неправильно называть системой, поскольку отсутствуют такие важные признаки системы, как взаимосвязанность элементов, единое законодательное регулирование, единые стандарты и правила.

11.2. ДИЗАЙН И ФУНКЦИОНАЛЬНОСТЬ НПС

Проанализируем факторы, определяющие дизайн и функциональность НПС, и сформулируем порождаемые этими факторами требования к НПС. На наш взгляд, при проектировании НПС в первую очередь необходимо учитывать такие факторы, как:

- мировая экономика — все страны и наднациональные структуры, с которыми взаимодействует Россия;

¹ Подробные материалы по этой теме представлены на сайте Европейской комиссии: <http://ec.europa.eu/>

- национальная экономика — экономика страны в широком смысле, включая особенности общественного устройства и государственного строя;
- потребители конечных сервисов — потребители сервисов, создаваемых частными платежными системами на основе инфраструктурных сервисов НПС, с учетом их требований и цены, которую они готовы заплатить;
- провайдеры конечных сервисов — частные платежные системы, создающие платежно-расчетные сервисы для конечных потребителей на основе инфраструктурных сервисов НПС;
- технологические возможности — полная совокупность технических и технологических возможностей, которые могут быть использованы в НПС.

В рамках первого фактора (мировая экономика) как одного из основополагающих выделим межстрановую конкуренцию в области эффективности экономики. Являясь существенным компонентом экономической инфраструктуры, НПС существенно влияет на эффективность экономики, которая не может быть более эффективной, чем это позволяет НПС. Отсюда вытекает основное требование к НПС: она не должна ограничивать возможности построения эффективной экономики, способной конкурировать с экономиками других стран.

Из данного общего требования вытекают частные — относительно функциональной полноты, технологичности, операционной эффективности и т.п., более подробно рассмотренные далее.

Глобализация мировой экономики делает необходимым взаимодействие НПС разных стран и создание глобальных наднациональных платежных систем, откуда вытекает требование интегрируемости НПС — поддержки ею механизмов, необходимых для интеграции НПС с аналогичными системами других стран и наднациональными платежными системами.

Из общих принципов национальной безопасности вытекает требование суверенности НПС — ни одно другое государство не должно иметь возможности как-либо воздействовать на внутренние операции НПС.

Рассматривая фактор «национальная экономика», предположим, что в будущем:

- останутся актуальными такие понятия, как «государство», «наличные» и «безналичные национальные деньги», «платежи», «расчеты», «товары и услуги», их продажа¹;
- платежно-расчетные сервисы, так же как и любые другие сервисы и услуги, будут предоставляться на платной основе;
- регулирование денежного обращения будет осуществляться централизованно на уровне государства и (или) надгосударственных образований специализированными структурами, условно называемыми центральными банками.

НПС должна удовлетворять требованию функциональной полноты — обеспечивать в полном объеме потребности национальной экономики в инфраструктурных платежно-расчетных сервисах, поскольку в случае функциональной

¹ Если данное предположение неверно, то обсуждать НПС не имеет смысла.

неполноты национальной системы инфраструктурные платежно-расчетные сервисы, отсутствующие в НПС, были бы реализованы за ее пределами, т.е. не удовлетворяли бы полному комплексу требований, предъявляемых к НПС.

Поскольку операционная эффективность экономики определяется ее составляющими, НПС должна удовлетворять требованию операционной эффективности и обеспечивать минимальную трудоемкость обработки платежно-расчетных операций.

В силу особенной роли, которую система денежного обращения играет для современного общества и подверженности этой системы различного рода рискам НПС должна удовлетворять таким требованиям, как управление и контроль со стороны государства; законность, прозрачность и контролируемость операций; исключительность (эксклюзивность) в том смысле, что все потребительские платежно-расчетные сервисы должны основываться на инфраструктурных сервисах НПС.

Так как возможность обработки операций в режиме реального времени порождает риски недостаточности ликвидности отдельных участников расчетов, НПС, очевидно, должна удовлетворять такому требованию, как наличие эффективной подсистемы управления ликвидностью.

Учитывая, что требования максимальной доступности, удобства и эффективности могут находиться в противоречии с требованием безопасности, в перспективной НПС должен быть найден разумный баланс выполнения этих требований, основанный на принципе соразмерности мер защиты рискам.

Важно также учитывать «среду исполнения», в которой будет функционировать НПС. Предположительно такой средой будет так называемое информационное общество — модель общественного устройства, которая, как ожидается, возникнет в результате реализации потенциала информационных и других современных и будущих технологий.

Из особенностей операционной модели информационного общества, наиболее существенных с точки зрения проектирования НПС, можно выделить следующие:

- дистанционные взаимодействия участников операционных процессов;
- совершение сделок преимущественно в электронном виде;
- исполнение операций в реальном времени;
- непрерывная доступность сервисов и услуг;
- глобализация — совместимость и доступность сервисов в мировом масштабе;
- низкая стоимость транзакций за счет преимущественно автоматической обработки;
- специализация сервис-провайдеров¹.

¹ Имеется в виду дальнейшее движение в направлении разделения труда в связи с большей эффективностью специализированных провайдеров по отношению к универсальным.

Рассматривая такой фактор, как потребитель конечных сервисов, примем, что в основе его поведения (неважно — физическое это лицо или юридическое) останутся те же целевые функции, что действовали в течение всей истории человечества и обеспечили его развитие, а именно стремление:

- минимизировать любые трудозатраты, как физические, так и умственные (т.е. лень);
- обеспечить комфортное существование и условия ведения бизнеса;
- сохранить достигнутое, а лучше повысить качество жизни (бизнеса);
- обеспечить свою безопасность во всех ее формах и продлить время жизни.

При рассмотрении такого фактора, как провайдер конечных сервисов, примем, что в основе его поведения останется первичная цель любого бизнеса — максимизация прибыли. В этом предположении поведение провайдера будет определяться стремлением:

- повысить доходность операций за счет увеличения числа предоставляемых сервисов и их стоимости;
- повысить конкурентоспособность за счет повышения качества, разнообразия и востребованности сервисов и снижения их стоимости;
- понизить расходы за счет снижения стоимости проведения и обработки операций;
- максимально продлить время жизни компании за счет минимизации рисков.

Из описанных моделей провайдера и потребителя конечных платежно-расчетных сервисов следует, что инфраструктурные сервисы НПС должны быть таковы, чтобы частные платежные системы могли на их основе создать платежно-расчетные сервисы для конечных потребителей, удовлетворяющие таким требованиям, как:

- операционная эффективность с точки зрения как потребителя, так и провайдера сервисов;
- многоканальность и поддержка каналов дистанционного доступа;
- возможность выбора канала, средства доступа, режима использования и источников средств;
- непрерывная доступность;
- возможность доступа к сервисам из любой точки;
- низкие риски использования;
- низкая стоимость использования;
- высокая скорость проведения и обработки операций (при необходимости в реальном времени);
- контролируемость и прозрачность;
- наличие механизмов обратной связи;
- удобство и простота использования.

Требование проведения операций в реальном времени заслуживает более детального рассмотрения. Автору представляется разумным предположение, что

безналичные расчеты в силу технологических причин вряд ли всегда могут проводиться в реальном времени¹. Если это предположение верно, то для выполнения требования обработки операции оплаты в реальном времени необходимо, чтобы продавец имел возможность предоставить товар или услугу после получения подтверждения оплаты, а не после поступления суммы оплаты на счет.

Отсюда вытекает требование поддержки режима «двухфазной оплаты», при котором операция оплаты товара или услуги распадается на две операции — «подтверждение оплаты» и «расчеты по обязательствам», между которыми вклиниваются такие события, как предоставление товара или услуги и клиринг (расчет сумм, подлежащих переводу между счетами для погашения обязательств). Отметим, что описанный режим «двухфазной оплаты» в настоящее время широко применяется платежными системами на основе платежных карт.

В отношении фактора «технологические возможности» выделим технические и технологические достижения, наиболее сильно влияющие на дизайн НПС:

- возможность реализации эффективных алгоритмов управления транзакциями и ликвидностью в реальном времени благодаря росту мощности компьютеров;
- возможность доступа потребителей из любой точки планеты благодаря наличию мобильной связи с глобальным покрытием;
- возможность заключения юридически значимых сделок в электронном виде для закрытых и открытых систем благодаря криптографии на асимметричных ключах, инфраструктуре открытых ключей и законодательства об ЭЦП;
- наличие глобальной информационно-коммуникационно-транзакционной среды (Интернет).

В не слишком далеком будущем можно ожидать появления персональных средств доступа — универсальных многоканальных, многофункциональных коммуникационных устройств, которые обеспечат владельцу широкий спектр возможностей, необходимых для доступа к платежно-расчетным сервисам, в том числе таких, как идентификация, аутентификация, многофакторная защита транзакций, защищенное хранение закрытых или симметричных ключей, подписание транзакций юридически значимым аналогом собственноручной подписи, генерация разовых паролей, кодов аутентификации сообщений, интерфейсы для безконтактного взаимодействия по различным протоколам (например, NFC)

¹ В принципе, в идеальном мире можно было бы говорить о выполнении в режиме реального времени в рамках одной распределенной транзакции всех действий, включая расчеты и движения по счетам всех участников операции. Это позволило бы исключить этап клиринга и значительно упростить управление рисками (в частности, ликвидностью). Однако такой режим вряд ли реализуем на практике даже в перспективной НПС в силу того, что: 1) предъявляет исключительно высокие требования к режиму работы всех участников, в частности банков, АБС которых обычно не работают в режиме постоянной доступности и не спроектированы под обработку запросов в режиме реального времени (в отличие от процессинговых центров); 2) делает невозможными любые технологии, в которых возникают этапы «локальной автономной обработки».

с терминальными устройствами, персональными компьютерами и другими персональными устройствами доступа (peer-to-peer), развитый пользовательский интерфейс с возможностью представления информации и формирования распоряжений на проведение операций, передача распоряжений по различным каналам и т.п.

Результатом всех вышеперечисленных достижений будет принципиальная возможность электронификации (перевода в электронную форму) многих процессов, сегодня осуществляющихся в материальном виде, и, как следствие, возможность дистанционного взаимодействия участников процессов. Кроме того, появится возможность реализации новых процессов и видов электронных взаимодействий, недоступных сегодня из-за отсутствия технических возможностей.

Поскольку возможность электронного дистанционного взаимодействия, очевидно, удовлетворяет сразу нескольким требованиям к НПС, можно предположить, что эта возможность будет использована в полной мере и основной технологической особенностью перспективной НПС будет практически полная миграция в область электронных дистанционных взаимодействий между участниками.

Сведя вышесказанное вместе, получаем перечень требований, которым должны удовлетворять потребительские сервисы, создаваемые частными платёжными системами на базе инфраструктурных сервисов НПС:

- функциональная полнота. Должны быть обеспечены все существующие и прогнозируемые платёжно-расчётные потребности всех категорий пользователей;
- поддержка различных инструментов. Должна быть обеспечена возможность использования различных форм денег, в том числе должны поддерживаться различные валюты, электронные, цифровые и иные «деньги» российских и международных частных платёжных систем;
- операционная эффективность. Должна быть обеспечена минимальная стоимость проведения и обработки платёжно-расчётных операций;
- единая система идентификации пользователей, маршрутизации и доставки электронных сообщений с использованием сервисов национальной системы электронных взаимодействий;
- сквозная автоматическая обработка. Должна быть обеспечена возможность автоматической обработки всех операций в пределах НПС, а также сквозной автоматической обработки с участием систем автоматизации пользователей;
- максимальная электронификации. Должна быть обеспечена возможность проведения в электронной форме всех операций, кроме тех, для которых это явно запрещено законодательством;
- скорость. Должна быть возможна обработка операций в режиме реального времени;
- поддержка различных режимов проведения операций. Должна быть обеспечена поддержка всех необходимых пользователям режимов инициации и проведения операций;

- суверенность. НПС должна быть независима от других стран, ни одно государство не должно иметь возможности воздействовать на внутренние операции НПС;
- законность и юридическая значимость — действия, совершаемые в виде обмена электронными сообщениями, должны быть юридически значимыми;
- дистанционный доступ и многоканальность. Должна быть обеспечена возможность проведения операций по различным дистанционным каналам с возможностью выбора пользователем подходящих ему каналов;
- возможность использования универсального персонального многоканального многофункционального коммуникационного устройства для выполнения функций идентификации, аутентификации, формирования и подтверждения сообщений;
- доступность. Сервисы должны быть непрерывно доступны из любой точки всем категориям пользователей;
- нейтральность. Сервисы должны быть равным образом доступны всем пользователям независимо от категории, резидентности и т.п.;
- гибкость. Пользователь должен иметь возможность выбора способа и режима проведения операции, в том числе канала, персонального средства и терминала доступа, источника средств;
- безопасность. Должна быть обеспечена защита операций и средств пользователей;
- интегрируемость. Должна быть обеспечена возможность интеграции с НПС других стран и наднациональными платежными системами;
- управление рисками. В состав НПС должна входить эффективная подсистема управления рисками.

11.3. АРХИТЕКТУРА НПС

Для определения функциональной архитектуры НПС составим перечень основных действий, совершаемых экономическими субъектами, в целях или в связи с оплатой товаров и услуг, переводами денежных средств и т.п. Это позволит определить структуру потребностей общества в платежно-расчетных сервисах и исходя из них — состав основных функциональных компонент НПС.

Рассмотрим упрощенную модель жизненного цикла экономического субъекта (рис. 11.1). В разное время субъект может выступать как производитель, продающий свои продукты другим субъектам, либо как потребитель, приобретающий продукты.

Анализируя предложенную модель, можно составить перечень платежно-расчетных сервисов, необходимых для нормального функционирования экономики:

- возможность оплаты товара или услуги путем предоставления покупателем и получения продавцом юридически значимого подтверждения обязанности рассчитаться за предоставленный товар или услугу;

- возможность выставления продавцом и получения покупателем требования (инвойса) на оплату товара или услуги;
- возможность расчетов за предоставленный товар или услугу путем перевода денежных средств от покупателя продавцу в соответствии с обязательствами, взятыми на себя покупателем при оплате товара или услуги или другими обязательствами.

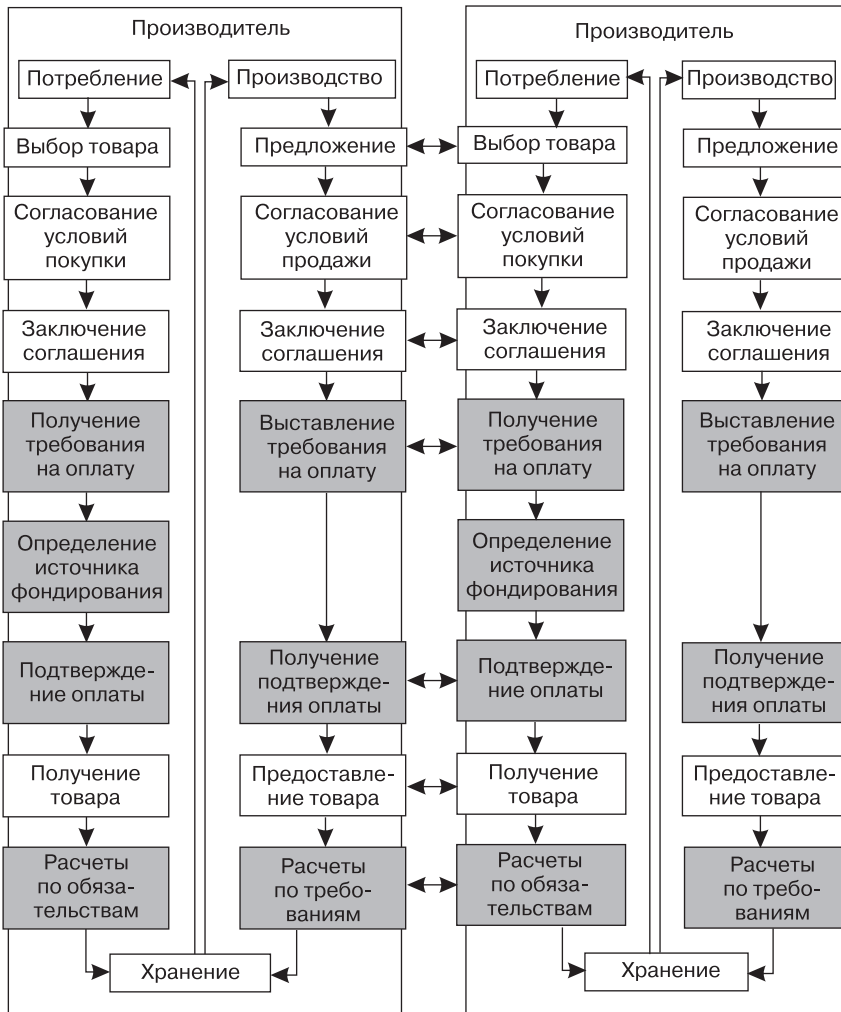


Рис. 11.1. Жизненный цикл экономического субъекта (серым цветом выделены действия, связанные с платежами или расчетами)

Помимо перечисленного в силу значительных технологических особенностей обращения наличных денежных средств в отдельный необходимый обществу сервис можно выделить возможность использования наличных денежных средств.

Из рассмотренных потребностей экономики в платежно-расчетных сервисах вытекает состав функциональных компонент НПС:

- национальная система валовых расчетов;
- национальная система розничных платежей;
- национальная инвойсинговая система;
- национальная система наличных денег.

Поскольку рассмотренные платежно-расчетные сервисы (за исключением наличного денежного обращения) основаны на дистанционном взаимодействии субъектов путем обмена электронными сообщениями, возникает необходимость в стандартных механизмах маршрутизации и доставки сообщений. Создавать такие механизмы специально для НПС нецелесообразно.

Как отмечалось ранее, взаимодействия субъектов в информационном обществе будут в значительной степени происходить дистанционно в электронном виде (путем обмена электронными сообщениями). Это означает, что в инфраструктуре информационного общества обязательно будут присутствовать развитые механизмы и инструментарий, обеспечивающие возможность юридически значимого обмена субъектов электронными сообщениями.

Совокупность таких механизмов и инструментов можно условно рассматривать как систему электронных взаимодействий (СЭВ) — одну из систем инфраструктуры информационного общества, предоставляющую другим функциональным компонентам инфраструктуры сервисы обмена электронными сообщениями (ЭС).

Ввиду того, что НПС является частью инфраструктуры информационного общества, ее проектирование должно производиться с учетом наличия других подсистем этой инфраструктуры, а частности, для того чтобы избежать дублирования сходной функциональности в разных подсистемах. Таким образом, логично потребовать, чтобы НПС использовала для обмена сообщениями сервисы, предоставляемые СЭВ.

С учетом сказанного оптимальной представляется логическая архитектура НПС, показанная на рис. 11.2.

11.4. О СРЕДСТВАХ ДИСТАНЦИОННОГО ДОСТУПА К СЕРВИСАМ

Важнейшим элементом системы дистанционного доступа к сервисам является персональное средство доступа (ПСД). Это оборудование, используемое физическими лицами — потребителями сервисов (в том числе платежно-расчетных) для

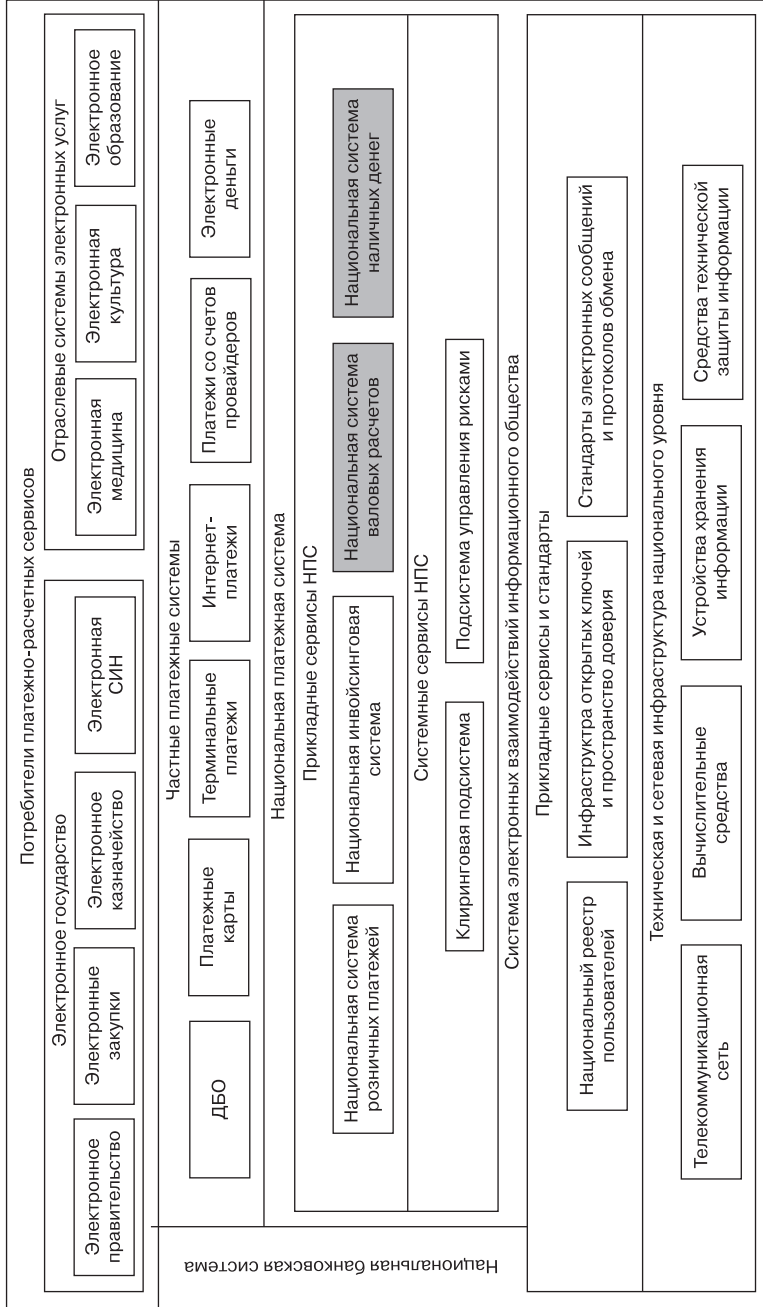


Рис. 11.2. Логическая архитектура НПС (темным фоном выделены уже существующие компоненты)

доступа к ним по различным каналам. Именно от функциональных возможностей ПСД во многом зависит, будут ли выполнены требования к НПС, описанные ранее.

Достаточно очевидным общим требованием к ПСД является требование исчерпывающей функциональности, т.е. способности обеспечить полный спектр функций, необходимых для доступа к сервисам без использования каких-либо еще средств или устройств помимо ПСД. Его владелец должен иметь возможность получить доступ ко всем необходимым сервисам. Исходя из требования исчерпывающей функциональности можно сформулировать и остальные требования. Например, ПСД должно одновременно являться и средством коммуникации общего характера.

ПСД должно обеспечивать возможность выполнения полного спектра функций, связанных с обеспечением безопасности, в том числе таких, как:

- возможность защиты доступа к функциям ПСД локальными средствами (локальный пароль, биометрия);
- возможность оперативной дистанционной блокировки ПСД;
- возможность уведомления пользователя о существенных для него событиях;
- идентификация пользователя с помощью различных механизмов в зависимости от каналов, проводимых операций, потребностей и возможностей пользователя и провайдера сервисов (НИК, сертификат открытого ключа и др.);
- аутентификация пользователя с помощью различных механизмов в зависимости от каналов, проводимых операций, потребностей и возможностей пользователя и провайдера сервисов (постоянные и разовые пароли, запрос-ответ);
- подтверждение сообщений с помощью различных механизмов в зависимости от каналов, проводимых операций, потребностей и возможностей пользователя и провайдера сервисов (постоянный и разовые пароли, вычисление кода подтверждения сообщения (MAC), аналог собственноручной подписи, в частности ЭЦП на сертифицированных и несертифицированных крипто средствах);
- защищенное хранение информации и данных, в том числе ключевой и финансовой информации, цифровых денег (недублируемых требований денежного характера)
- и поддержка протоколов передачи цифровых денег.

ПСД должно обеспечивать пользователю постоянную глобальную доступность сервисов — возможность доступа к сервисам в различных режимах в любое время из любой точки мира, для чего в том числе обеспечивать следующие возможности:

- возможность законного использования в разных юрисдикциях с учетом возможных страновых ограничений (например, на экспорт средств криптографии);
- доступ к различным локальным и глобальным телекоммуникационным сетям, доступным на территории нахождения пользователя, и поддержка всех основных коммуникационных протоколов;

- возможность выбора пользователем режима доступа при наличии нескольких вариантов;
- связь по различным протоколам с локальными терминалами в точках обслуживания (POS-терминалы, банкоматы, устройства контроля доступа, устройства оплаты доступа к сервисам), точках доступа в глобальные сети (домашний компьютер или компьютер общего пользования);
- связь с другими ПСД в режимах непосредственного взаимодействия ПСД—ПСД и взаимодействия через локальные или глобальные телекоммуникационные сети.

ПСД должно обеспечивать пользователю возможность выбора режима использования в зависимости от проводимых операций, потребностей и возможностей пользователя и провайдера сервисов, в том числе:

- поддержка различных каналов доступа к сервисам с возможностью выбора пользователем предпочтительного для него канала;
- выбор пользователем средств и режимов идентификации, аутентификации и подтверждения сообщений;
- выбор пользователем способа использования ПСД, например управление голосом в некоторых ситуациях;
- возможность выбора пользователем режима взаимодействия с терминалами доступа и настройки режимов выполнения операций, например, пользователь должен иметь возможность установить, что списание цифровых денег при доступе в средство транспорта требует (не требует) авторизации с его стороны.

ПСД должно обеспечивать возможность практически неограниченного развития функциональности и, в частности, не должно создавать ограничений с точки зрения провайдеров сервисов в случаях, когда последним необходима специальная функциональность ПСД, для чего в том числе должно обеспечивать следующие возможности:

- поддержка различных режимов взаимодействия с пользователем, в том числе визуальный интерфейс, голосовое взаимодействие, взаимодействие через клавиатуру;
- возможность получения и передачи сервис-провайдеру биометрической информации пользователя;
- поддержка различных режимов информационного обмена (пакетный и интерактивный);
- поддержка симметричного режима взаимодействия (взаимодействие может инициироваться как пользователем, так и провайдером сервисов, например путем вызова ПСД или отправки сообщения);
- возможность реализации различных алгоритмов обработки входящих запросов и сообщений;
- возможность независимой установки разными сервис-провайдерами своих приложений с обеспечением безопасного независимого исполнения;

- оптимальные процессы управления приложениями и статической информацией со стороны поставщиков, в том числе возможность удаленного управления.

ПСД должно быть доступным для использования различными категориями пользователей, в том числе пользователей с разным уровнем технической грамотности, разным уровнем дохода, пользователей с ограниченными возможностями. Для этого (в числе прочего) должны выполняться такие требования, как простота использования, ценовая доступность для массовых пользователей.

ПСД должно быть практичным, его использование не должно создавать для пользователя излишних трудозатрат, неудобств или ограничений, в том числе ПСД должно удовлетворять таким требованиям, как удобный пользовательский интерфейс, портативность, ударостойкость, энергонезависимое хранение.

Если сопоставить вышеперечисленные требования с возможностями современных мобильных телефонов или аналогичных устройств, можно увидеть, что практически все требования либо уже выполняются, либо с большой вероятностью будут выполнены в ближайшем будущем. Являясь по сути универсальным персональным коммуникационным устройством, мобильный телефон обеспечивает:

- многоканальность и доступ к основным телекоммуникационным сетям;
- интерактивный и пакетный режимы взаимодействия;
- симметричное взаимодействие;
- защищенное хранение данных;
- возможность взаимодействия с другими устройствами по локальным и глобальным сетям и в режиме прямого взаимодействия;
- развитый пользовательский интерфейс (экран высокого разрешения, цифровой и буквенный ввод, аудиоввод и вывод, распознавание голоса);
- вычислительные ресурсы и память;
- поддержку среды исполнения и различных программных средств (стандартная операционная система, полнофункциональные приложения, защищенные приложения, загрузка приложений OTA);
- различные способы идентификации, аутентификации и подтверждения сообщений.

На основании сказанного можно сделать вывод, что мобильный телефон является естественной платформой для создания на его основе универсального многофункционального ПСД, которое объединит «в одном корпусе» всю функциональность, реализуемую в настоящее время с помощью различных устройств и средств, что сделает использование последних излишним.

В частности, если подобный сценарий реализуется, можно ожидать, что ПСД на базе мобильного телефона в не очень отдаленном будущем заменит распространенные, но морально устаревшие средства (например — карты с магнитной полосой и с чипом). Данное соображение необходимо учитывать при инициации масштабных и дорогостоящих проектов, предполагающих реализацию каких-либо инновационных технологий, поскольку есть риск, что выбранный носитель устареет до завершения реализации проекта.

11.5. НАЦИОНАЛЬНАЯ СИСТЕМА ЭЛЕКТРОННЫХ ВЗАИМОДЕЙСТВИЙ

Национальная система электронных взаимодействий (см. рис. 11.2 (нижняя часть схемы) и рис. 11.3) является одним из элементов национальной технологической инфраструктуры.

СЭВ обеспечивает маршрутизацию и передачу юридически значимых электронных сообщений в интересах любых функциональных компонент инфраструктуры информационного общества, а также любых других систем, использующих в своей работе обмен электронными сообщениями. В этих целях СЭВ также обеспечивает сервисы, необходимые для формирования национального пространства доверия, в том числе сервисы управления РКІ.

Являясь провайдером сервисов по транспорту электронных сообщений для различных областей, СЭВ должна быть нейтральной по отношению к предметной области. Как следствие, в ее основе должны находиться национальные стандарты на формат и протокол маршрутизации и доставки электронных сообщений, не зависящие от предметной области и содержания сообщений.

Для доступа к сервисам СЭВ пользователь заключает соглашение с одним или несколькими сервис-провайдерами (см. рис. 11.3, стрелка 1).

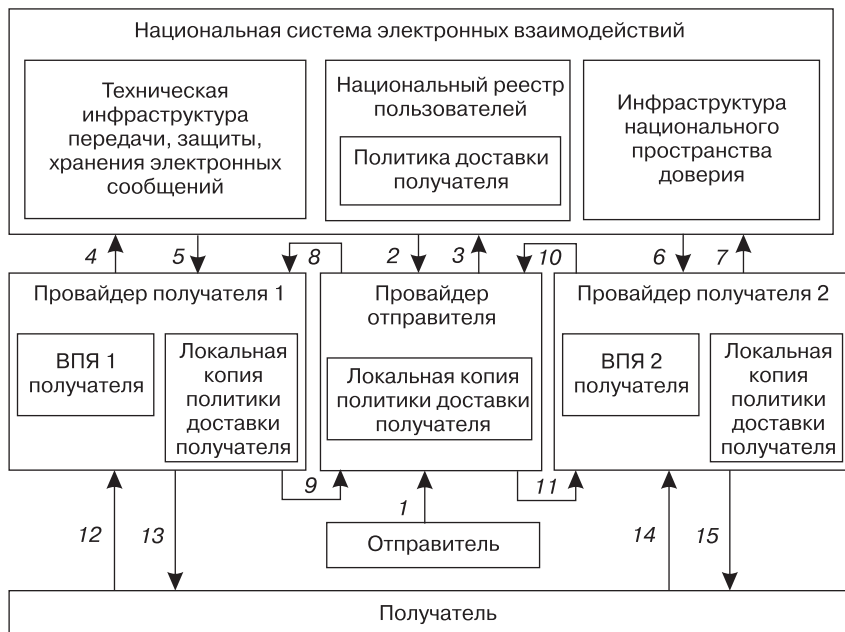


Рис. 11.3. Маршрутизация и доставка ЭС

Для доставки пользователю ЭС используются виртуальные почтовые ящики (ВПЯ) пользователя, открываемые последним у обслуживающих его сервис-провайдеров. Пользователь может открыть неограниченное число ВПЯ у одного или разных сервис-провайдеров. Доставка ЭС до любого из активных ВПЯ пользователя признается юридически значимой доставкой ЭС до пользователя.

Маршрутизация ЭС производится на основе политики доставки (ПД) — совокупности правил маршрутизации, определяющих, в какой виртуальный ящик пользователя должно быть доставлено электронное сообщение. Политика доставки хранится в профиле пользователя в базе данных Национального реестра пользователей (НРП). Ответственность за поддержание политики доставки в актуальном состоянии несет пользователь.

Провайдер, обслуживающий пользователя, обязан хранить актуальную копию политики доставки пользователя. Основным механизмом актуализации является подписка провайдера на уведомления НРП об изменениях политики доставки.

Первичная маршрутизация ЭС производится провайдером отправителя с использованием локальной копии политики доставки получателя¹. Если локальная копия политики доставки отсутствует, она запрашивается в НРП. Вместе с ЭС передаются дата и время последнего изменения политики доставки.

Провайдер получателя, получив ЭС, проверяет дату и время политики доставки, использованной отправителем, наличие и состояние ВПЯ получателя. В случае если политика доставки, использованная провайдером отправителя, неактуальна, либо ЭС не может быть принято по другим причинам, провайдер получателя возвращает отказ в приеме ЭС.

Получив отказ в связи с неактуальностью политики доставки, провайдер отправителя запрашивает в НРП актуальную версию политики доставки отправителя, после чего передает ЭС.

Ключевым элементом системы маршрутизации ЭС и идентификации пользователей является национальный реестр пользователей СЭВ — централизованная база данных, ведущаяся на национальном уровне, содержащая учетные записи пользователей всех систем, использующих сервисы СЭВ.

Пользователи систем, использующих сервисы СЭВ, независимо от их категории (физические лица, индивидуальные предприниматели, все виды юридических лиц, включая государственные и муниципальные организации и ведомства, резиденты и нерезиденты РФ) в обязательном порядке регистрируются в НРП.

Регистрация пользователей в НРП производится уполномоченными участниками, которые отвечают за идентификацию пользователя, контроль и ввод данных. Порядок регистрации пользователей в НРП показан на рис. 11.4. Допускается только однократная регистрация пользователя в НРП.

При регистрации пользователю назначается национальный идентификационный код (НИК), однозначно определяющий пользователя во множестве

¹ Передача ресурсоемкой функции обработки политики доставки на провайдера отправителя создает механизм масштабирования и позволяет избежать эффекта «узкого горла», который имел бы место, если бы данная нагрузка легла на НО СЭВ.

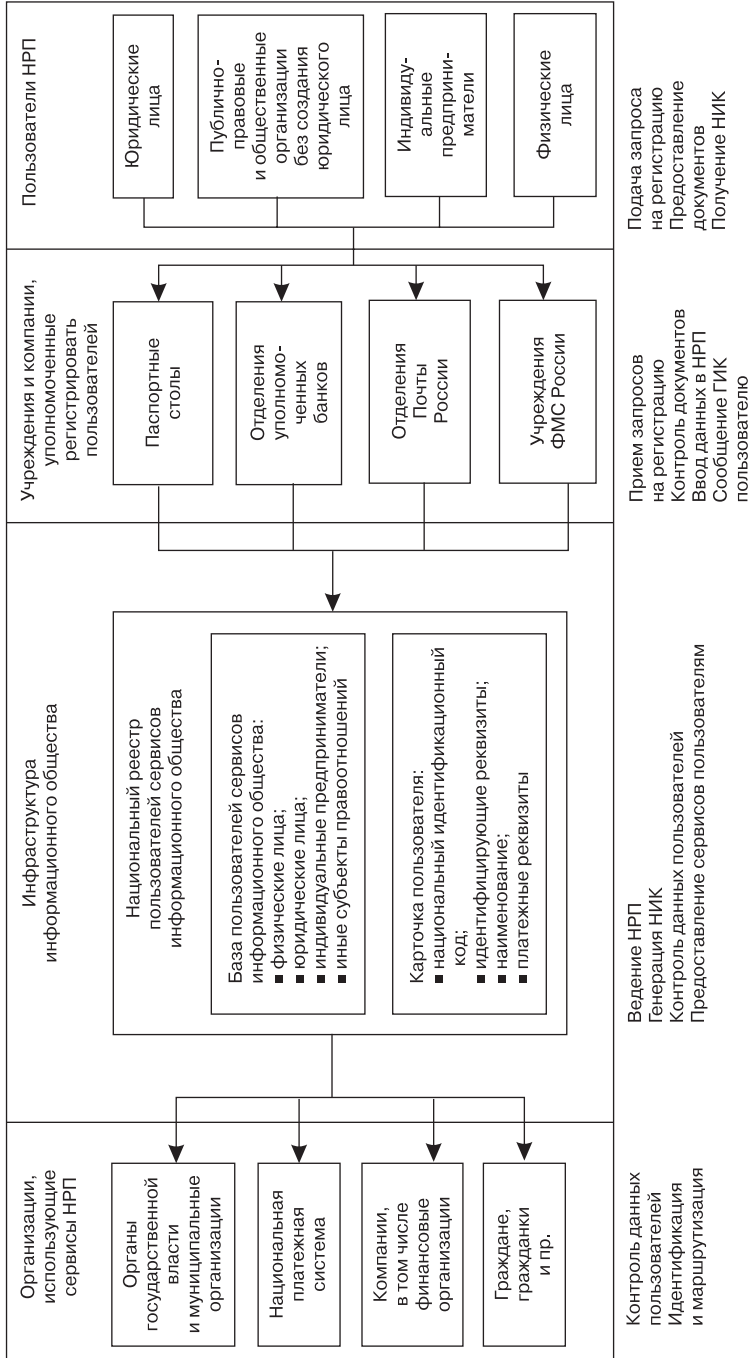


Рис. 11.4. Регистрация пользователей СЭВ в национальном реестре пользователей

пользователей СЭВ. НИК используется во всех процессах СЭВ как идентификатор пользователя, которому может быть назначен только один НИК, постоянный в течение жизненного цикла пользователя.

Формат НИК должен быть ориентирован как на использование человеком при доступе по различным каналам (например, телефон с тоновым набором или речевой канал с распознаванием речи), так и на автоматическую обработку. Наиболее целесообразно использование в качестве НИК последовательности цифр с контрольными разрядами.

При регистрации пользователя в НРП создается профиль пользователя, в котором хранится набор данных достаточный для исполнения бизнес-процессов (наименование пользователя, адреса для маршрутизации, открытые ключи, расчетные реквизиты).

Основные параметры профиля, однозначно идентифицирующие пользователя, вводятся на основании документов, предоставленных пользователем уполномоченному участнику. Некоторые данные профиля (например, адресную информацию) пользователь может изменять самостоятельно.

11.6. НАЦИОНАЛЬНАЯ ИНВОЙСИНГОВАЯ СИСТЕМА (НИС)

Ярким примером нетехнологичности современной НПС России является существующая система выставления и обработки счетов на оплату — инвойсинг¹. В России в отличие от многих других стран инвойсинг по-прежнему в основном использует бумажные документы, т.е. является материальным.

Выделяясь из остальной среды, которая в значительной степени уже электронифицирована, материальный инвойсинг вынуждает на каком-то этапе переводить в бумажную форму процессы, в основном происходящие электронно, и не позволяет до конца реализовать потенциал электронной обработки.

По сути материальный инвойсинг является технологическим атавизмом, снижающим операционную эффективность общества и тормозящим развитие в других областях. Недостатки материального инвойсинга в силу их системного характера не могут быть устранены путем совершенствования.

Вышесказанное означает, что внедрение национальной инвойсинговой системы и переход к электронному инвойсингу не только возможны технологически, но и весьма актуальны, так как существующая практика материального инвойсинга в ряде случаев является заметным препятствием на пути повышения эффективности экономики.

Далее кратко описаны принципы построения и основные требования к НИС: область действия электронного инвойсинга показана на рис. 11.5.

¹ Термины и сокращения, не определенные по месту использования, применяются в соответствии с определениями, приведенными в конце данной главы.

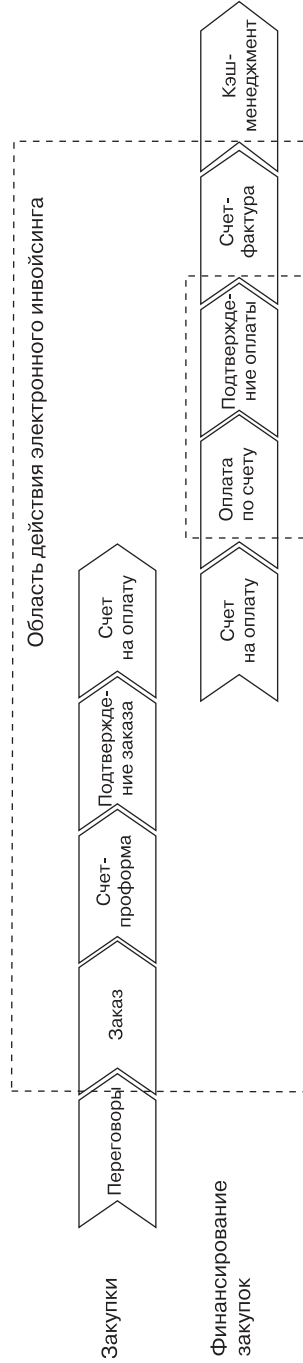


Рис. 11.5. Область действия электронного инвойсинга

НИС должна основываться на принципе «расширенной функциональной эквивалентности» — переводе процессов формирования и обработки материальных инвойсов в электронную форму с одновременным расширением функциональности с тем, чтобы максимально использовать возникающие дополнительные возможности.

Так, в НИС должны быть воспроизведены все существующие процессы и артефакты материального инвойсинга, за исключением случаев, когда существующие процессы имеют смысл только для материальных объектов либо в электронной форме процессы могут быть спроектированы более оптимально. В случаях, когда это позволяют возможности электронного инвойсинга, могут быть реализованы новые процессы.

К инвойсинговой системе применяются все требования к НПС, описанные ранее в данной главе (подразделе «Дизайн и функциональность НПС»), а также некоторые специальные требования, которые рассмотрены далее.

Пользователь любой категории и резидентности должен иметь возможность выступать в любой роли. В частности, как сторона, выставяющая счет (эмитент), или как сторона, его оплачивающая (плательщик). Например, физическое лицо должно иметь возможность выставить ЭИ юридическому лицу или публично-правовому образованию.

НИС должна реализовывать принцип открытости, предполагающий необязательность парных договорных отношений между пользователями — эмитент может выставить ЭИ плательщику без предварительного заключения соглашения об обмене ЭИ. Данный принцип не запрещает двусторонние договорные отношения и не означает, что плательщик обязан обработать ЭИ — отношения данного рода находятся за рамками НИС.

Являясь частью национальной технологической инфраструктуры, НИС должна быть основана на национальных стандартах в области инвойсинга, обязательных для применения всеми участниками и пользователями НИС на всей территории страны. На национальном уровне должны быть определены и централизованно управляться как технологические стандарты — таксономия и форматы сообщений, основные технологические процессы и процедуры, интерфейсы и правила обработки ЭИ.

Чтобы в полной мере реализовать потенциал электронификации процессов, НИС должна на технологическом уровне (изменение законодательства — отдельный вопрос) обеспечить возможность перевода в электронную форму обработки всех видов документов, возникающих в жизненном цикле различных сделок. В частности, как показывает опыт других стран, НИС должна проектироваться с учетом задач исчисления и уплаты налогов и составления налоговой отчетности, а ЭС НИС должны отвечать требованиям налогового законодательства.

В идеале НИС совместно с национальной системой розничных платежей должна обеспечивать принципиальную техническую и технологическую возмож-

ность полной сквозной автоматической обработки транзакции «формирование ЭИ → выставление ЭИ → доставка ЭИ → получение ЭИ → обработка ЭИ → оплата ЭИ → подтверждение оплаты → доставка подтверждения → получение подтверждения → обработка подтверждения» по схеме «конечное приложение — конечное приложение» (например, от одной системы управления предприятием класса ERP — к другой системе такого же класса).

НИС должна обеспечивать эмитентам и плательщикам возможность использовать различные режимы выставления и обработки инвойса. Например, помимо обычной схемы выставления ЭИ по инициативе эмитента в некоторых случаях более удобен режим запроса ЭИ со стороны плательщика.

НИС должна обеспечивать возможность развития, в частности реализации выделенными группами пользователей на основе базовой функциональности НИС «отраслевой функциональности», необходимой этим группам (например, включение в состав ЭИ специфической для какого-то бизнеса информации).

Организация доступа к сервисам НИС должна строиться на принципе свободы выбора поставщика услуг. Как эмитент, так и плательщик должны иметь возможность выбора коммерческого провайдера сервисов НИС либо прямого подключения к НИС на платной основе.

Глобализация мировой экономики, проявляющаяся в том числе в росте международных торговых отношений и, как следствие, международных расчетов, создает потребность в услугах международного инвойсинга. Очевидно, что необходимо уже на этапе проектирования архитектуры и разработки стандартов НИС учесть необходимость в дальнейшем интеграции с НИС других стран.

Организационная архитектура НИС представлена сетью «инвойсинг-сервис-провайдеров» (ИСП, рис. 11.6), на договорной основе предоставляющих конечным пользователям услуги по обработке ЭИ.

Для маршрутизации ЭИ НИС использует сервисы по маршрутизации и доставке ЭС, предоставляемые СЭВ. Передача ЭИ производится напрямую между ИСП с использованием стандартных протоколов СЭВ, обеспечивающих транзакционность, гарантированную доставку и безопасность информации.

В качестве ИСП может выступать как специализированный провайдер, предоставляющий только сервисы инвойсинга (прием ЭИ, контроль формата; маршрутизация и доставка; хранение ЭИ; передача ЭИ плательщику), так и неспециализированный (банк, оператор связи, интернет-провайдер, оператор терминальных устройств), в дополнение к базовым предлагающий смежные сервисы.

Пользователями НИС могут являться любые участники экономических процессов, имеющие потребность выставить или оплачивать инвойсы. Один и тот же субъект в зависимости от ситуации может быть продавцом или получателем услуги и с точки зрения НИС выступать как эмитент или как плательщик соответственно.

Для подключения к НИС пользователь заключает соглашение о предоставлении услуг инвойсинга с одним из коммерческих ИСП (при желании пользователь

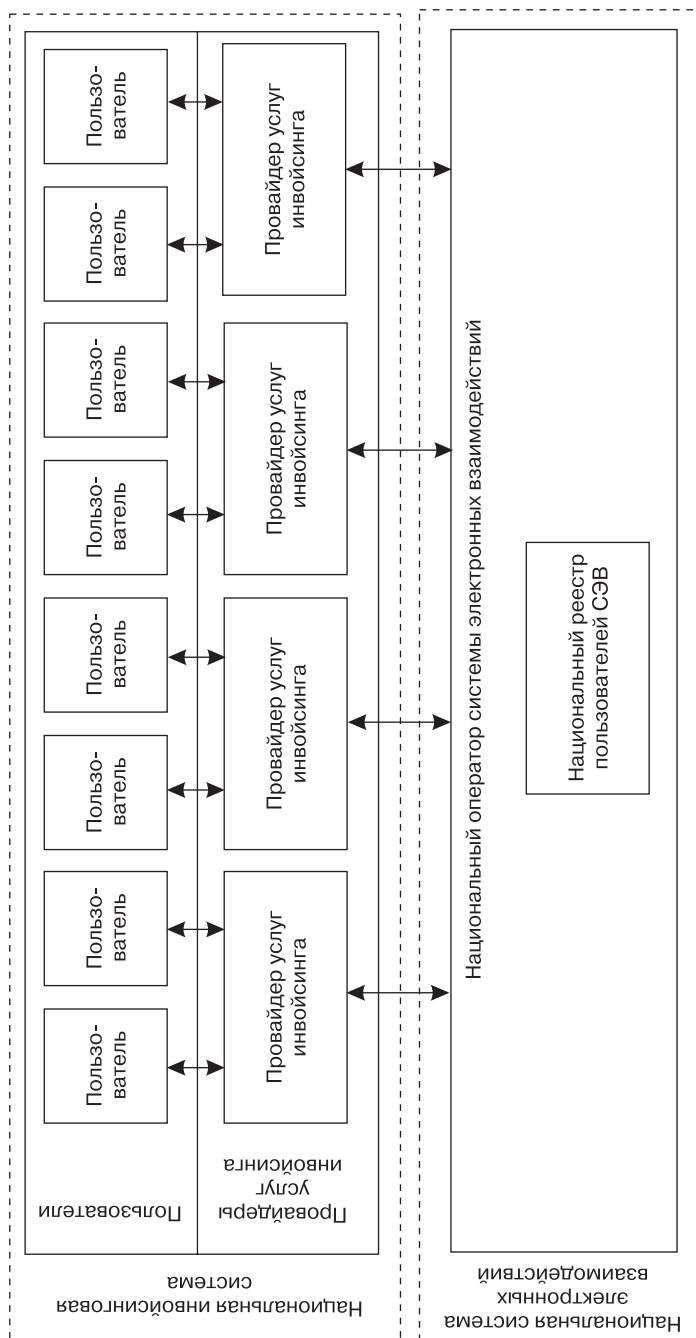


Рис. 11.6. Организационная архитектура НИС

может заключить соглашения с более чем одним ИСП, например, второй ИСП будет использоваться в случаях недоступности основного).

Режимы оплаты ЭИ, настраиваемые пользователем, могут меняться от полностью автоматической оплаты отдельных видов ЭИ от определенных «доверенных» эмитентов до оплаты исключительно в ручном режиме.

В качестве источников средств для оплаты ИСП может предлагать различные финансовые инструменты, такие как текущие счета в различных валютах, платежные карты, счета электронных денег, наличные деньги.

Одним из вариантов оплаты ЭИ, позволяющих сохранить ранее сделанные инвестиции и ускорить проникновение НИС благодаря использованию существующей инфраструктуры, является создание бумажной копии ЭИ на бумаге с печатью штрих-кода, содержащего основные атрибуты ЭИ для оплаты через отделение банка с автоматическим считыванием атрибутов.

Доступ к сервисам НИС осуществляется через любые каналы доступа (в том числе удаленного), предлагаемые ИСП, например, через точки обслуживания и продаж, Интернет, мобильные телефоны, платежные терминалы, и может комбинироваться с другими сервисами, предлагаемыми ИСП. Например, банк может предоставлять доступ к сервисам НИС и возможность оплаты ЭИ через каналы системы ДБО.

Формат ЭИ должен обеспечивать возможность реализации любых бизнес-требований, связанных с обработкой ЭИ. В частности, обеспечивать поддержку всех используемых на практике видов инвойсов и других видов документов, используемых при совершении сделок, в том числе счета-фактуры, счета на оплату более чем одной услуги, группировки нескольких счетов на одного плательщика в одном ЭИ и т.п.

Для обеспечения возможности автоматической обработки информация внутри ЭИ должна быть представлена в структурированном и максимально детализованном виде с выделением всех семантически различных значений в отдельные атрибуты.

Формат ЭИ должен обеспечивать возможность расширения, например, создания пользователями НИС собственного «пользовательского» уровня обмена информацией, т.е. передачи сообщений между пользователями без обработки этой информации НИС и (или) СЭВ. Кроме того, формат ЭИ может предусматривать возможность вложений произвольного формата и размера.

Особое внимание должно быть уделено реквизитам ЭИ, относящимся к налогам и сборам. Информация этого вида должна быть декомпозирована до «атомарных» параметров с выделением различных видов налога, параметров, использованных при вычислении сумм налогов (налоговые ставки и т.п.), налогов, начисляемых на налоги, и т.д. и обеспечивать возможность плательщику проверять правильность вычисления сумм налогов и использовать полученную в ЭИ информацию для решения собственных задач в части исчисления налогов и составления налоговой отчетности.

11.7. НАЦИОНАЛЬНАЯ СИСТЕМА РОЗНИЧНЫХ ПЛАТЕЖЕЙ

В рамках данной главы понятие «розничный платеж» не означает только платежи физических лиц или платежи на небольшие суммы. Оно используется в широком смысле и охватывает все многообразие операций, связанных с переходом денежных средств от одного участника экономических процессов к другому либо изменения формы денежных средств в распоряжении одного участника, в частности, подразумевает платежи на различные суммы — от микроплатежей до макроплатежей, выполняемые любыми категориями пользователей.

Логическая архитектура, основные компоненты НСРП показаны на рис. 11.7.

В основе НСРП лежит единый национальный формат электронных финансовых сообщений. Обмен ЭС в рамках НСРП производится с использованием базовых сервисов по транспорту и маршрутизации ЭС, предоставляемых СЭВ.

Розничный платеж представляется в виде распределенной макротранзакции, включающей несколько участников, длительность во времени которой может варьироваться от долей секунды до месяцев. На верхнем уровне розничный платеж распадается на два последовательных этапа — подтверждение оплаты и расчеты.

Этап подтверждения оплаты заключается в обмене между участниками транзакции ЭС, результатом которого является получение бенефициаром юридически значимого ЭС, подтверждающего, что бенефициару гарантируется выплата денежных средств в оплату некоторой операции, которую должен выполнить бенефициар.

Как уже отмечалось ранее, разделение розничного платежа на две фазы (подтверждение платежа и расчеты) необходимо для выполнения требования обработки операции оплаты в реальном времени.

Этап подтверждения оплаты характеризуется двумя важными особенностями:

- 1) на этом этапе речь идет только об обмене ЭС, никакие действия с денежными средствами не производятся;
- 2) в случае необходимости данный этап может выполняться в реальном времени; необходимость в данном случае определяется внешними факторами (например, особенностями технологии оплаты товара).

Если плательщик и бенефициар находятся в одном пространстве доверия, в результате передачи подтверждения оплаты у плательщика возникает обязательство перед бенефициаром, которое далее погашается в результате расчетов — перевода плательщиком в пользу бенефициара соответствующей суммы денег.

Если плательщик и бенефициар не находятся в одном пространстве доверия, в процессе исполнения этапа подтверждения оплаты возникает «цепочка денежных обязательств», в начале которой находится провайдер платежных сервисов плательщика, в конце — бенефициар, который получает юридически значимое

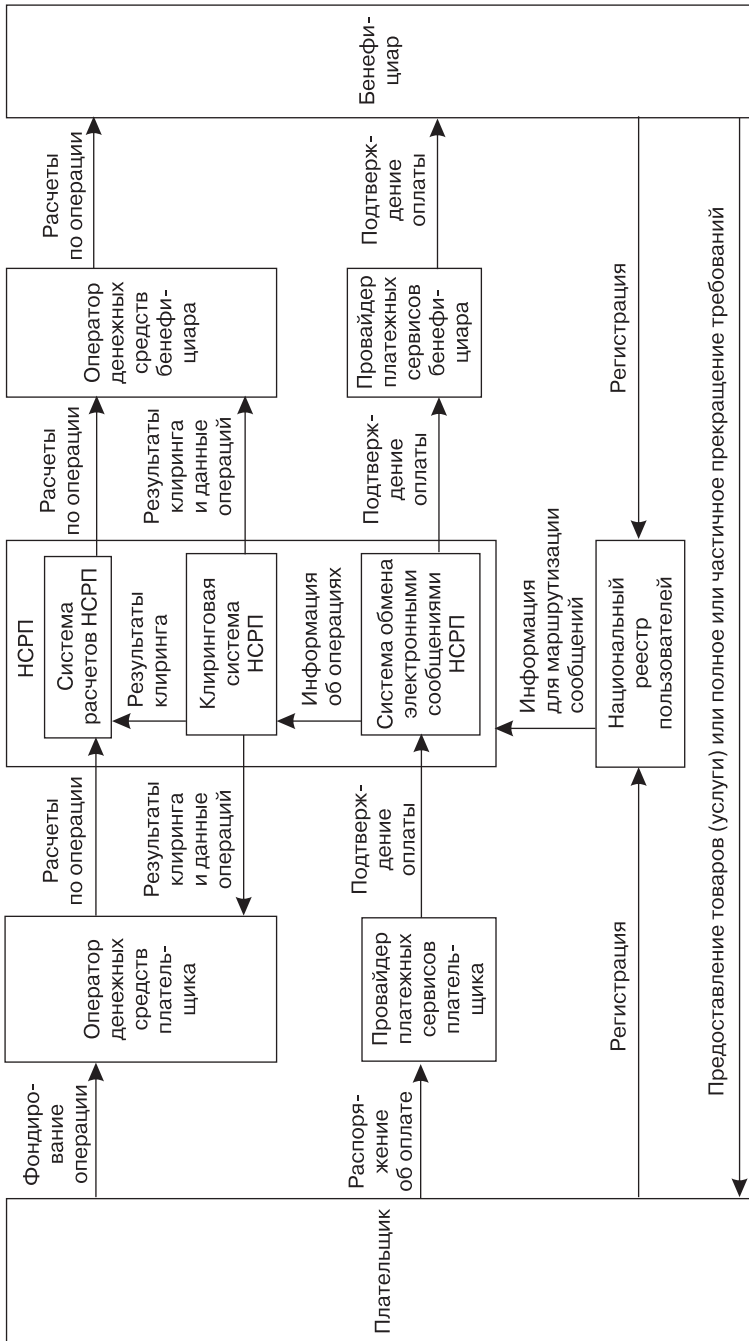


Рис. 11.7. Основные компоненты и процессы НСРП

подтверждение от своего провайдера платежных сервисов. Между названными участниками транзакции может находиться от нуля (в вырожденном случае, когда у плательщика и бенефициара общий провайдер) до нескольких других участников НСРП.

Гарантии получения провайдером платежных сервисов плательщика денежного возмещения от последнего могут иметь различную природу. Можно выделить два основных случая:

1) обязательства возникают в момент передачи провайдеру юридически значимого поручения (распоряжения) о выполнении платежа;

2) обязательства возникают в силу закона, например в случае, когда бенефициар имеет законное право безакцептно получить денежные средства плательщика, а провайдер последнего обязан выполнить законное требование бенефициара. В этом случае подтверждение оплаты будет сформировано провайдером без взаимодействия с плательщиком, а право провайдера получить возмещение (например, безакцептным списанием со счета) возникнет в силу закона.

Обратим внимание, что передача плательщиком распоряжения своему провайдеру не обязательно происходит в результате прямого взаимодействия плательщика с провайдером. Например, плательщик может использовать для инициации платежа терминал, предоставленный бенефициаром или третьей стороной (в частном случае — банкомат). Суть от этого не меняется, распоряжение является для провайдера распоряжением плательщика и, в частности, должно быть подтверждено способом, позволяющим провайдеру плательщика проверить подтверждение.

В связи с вышесказанным необходимо подчеркнуть важность строгого определения границ транзакции розничного платежа. Так, в случае денежного перевода без открытия счета через терминал самообслуживания действия по вводу купюр в приемник терминала и зачислению денежных средств на банковский счет конечного получателя не входят в состав розничного платежа. Первое действие является фондированием операции, второе — предоставлением услуги.

Под фондированием операции оплаты понимается предоставление плательщиком средств, необходимых для ее проведения. Денежные средства для фондирования могут предоставляться плательщиком в различных формах, например в виде безналичных денежных средств на банковском счете, электронных денежных средств различного вида, наличных денежных средств.

Фондирование может производиться в различных режимах и по времени не обязательно связано с самой операцией оплаты. Например, фондирование может производиться:

- в форме получения ссуды в момент оплаты с последующим погашением в соответствии с условиями кредитного соглашения между плательщиком и оператором денежных средств плательщика;
- наличными денежными средствами в момент оплаты при оплате через кассу точки обслуживания или терминал самообслуживания (компания- опе-

ратор терминальной сети в этом случае выступает в качестве оператора денежных средств плательщика);

- со счета плательщика (в частности — с банковского счета).

На этапе расчетов производятся денежные расчеты между участниками «цепочки денежных обязательств». Для расчетов используются данные, полученные в результате расчетов взаимных обязательств, выполненных клиринговой подсистемой НСРП на основании информации о транзакциях в течение клирингового периода.

Расчеты производятся между финансовыми институтами — участниками НСРП, в совокупности составляющими расчетную подсистему НСРП (см. рис. 11.7), обеспечивающими необходимый для расчетов набор финансовых сервисов (например, ведение расчетных счетов участников НСРП, предоставление ликвидности путем выдачи технических кредитов и т.п.)

УПРАВЛЕНИЕ НПС

Ключевым является вопрос управления развитием и функционированием НПС. С учетом того, что НПС является элементом инфраструктуры национальной экономики, более оптимален подход, когда такое управление находится в руках государства.

Такая позиция в целом подтверждается опытом других стран, где в последнее время наблюдается усиление роли государства в формировании национальных и наднациональных платежных систем. Также в пользу этой позиции говорит то, что в России оба существующих компонента НПС созданы усилиями государства в лице Банка России.

Очевидно, например, что управляющая рука государства абсолютно необходима в области выработки стандартов. Вряд ли можно ожидать, что такие стандарты появятся в разумное время эволюционным путем в результате «рыночного» взаимодействия конкурирующих друг с другом участников.

В случае 100%-ного рыночного подхода к выработке стандартов, скорее, можно ожидать превращения в «национальный стандарт» предложения участника, который сможет каким-либо способом навязать остальным свою «правду жизни». В этом случае наиболее вероятным представляется сценарий превращения в НПС одного из существующих решений, т.е., по сути, под лозунгами «рыночных подходов» будет иметь место не создание обществом эффективной НПС, а банальное занятие одним из участников рынка монопольного положения.

Передавая функции управления НПС в руки государства, крайне важно правильно определить ответственного за качество дизайна и развитие НПС. Это может быть любая системообразующая государственная структура, должным образом уполномоченная, обеспеченная адекватными масштабу задачи финансовыми ресурсами, имеющая опыт и специалистов в области организации платежей, расчетов и денежного обращения.

В других странах, как правило, в качестве такого ответственного выступает центральный банк или аффилированная с ним структура со значительной долей участия государства в капитале.

СЧЕТА ДЕНЕЖНЫХ СРЕДСТВ

При любом переводе денежных средств или платеже как частном случае перевода возникает как минимум две точки, в которых производятся обработка и хранение информации о переводимых денежных средствах: 1) «источник» денежных средств, находящийся в распоряжении перевододателя, и 2) «приемник» денежных средств, находящийся в распоряжении переводополучателя.

В настоящее время в России при осуществлении платежей и переводов используется несколько вариантов комбинаций источников и приемников денежных средств, которыми могут быть, например, банковские счета, счета для учета предоплаты предоставляемых услуг, ведущиеся провайдером услуг; счета электронных и цифровых денег, ведущиеся платежными системами; банковские и небанковские карты различных платежных систем¹, наличные денежные средства при осуществлении переводов без открытия счета и т.п.

Среди перечисленных источников (приемников) денежных средств только банковские счета и наличные денежные средства могут считаться полностью обеспеченными нормативно-правовым регулированием. Остальные источники (приемники) используются либо вообще вне какого-либо правового регулирования, либо их использование производится со ссылкой на общие нормы гражданского права.

Такая ситуация вряд ли может считаться нормальной, поскольку речь идет об области специальных, денежных, отношений, для которой логично применять специальное регулирование со стороны специального регулятора кредитно-денежных отношений, каковым в России является ЦБ РФ.

Многообразие форм и режимов использования источников (приемников) денежных средств, а также отсутствие единого нормативно-правового регулирования затрудняют оптимизацию и унификацию процессов обработки платежей и переводов, в частности ввод единых национальных стандартов, что в конечном итоге отрицательно сказывается на эффективности и динамике развития национальной платежной системы.

Принципиально возможны два пути решения проблемы: запретить использование любых видов источников (приемников) денежных средств, кроме уже существующих и регулируемых Банком России (банковских счетов и наличных денежных средств), либо ввести единый порядок оказания платежно-расчетных сервисов с использованием привлеченных во временное пользование денежных средств и предоставить право оказания таких сервисов всем юридическим лицам при условии соблюдения установленного порядка.

¹ В данном случае речь не идет о полностью кредитных схемах.

Очевидно, что первый вариант, основанный на исключительном использовании банковских счетов, создаст излишние ограничения и неудобства как для провайдеров, так и для потребителей платежно-расчетных сервисов. Например, поскольку в каждодневной практике денежные средства часто предоставляются во временное пользование не только банкам, но и другим видам сервис-провайдеров, например, при авансовой оплате — провайдеру услуг связи или интернет-провайдеру, запрет на использование этих денежных средств для каких-либо целей, кроме оплаты услуг, означал бы для владельца денежных средств ограничения в части возможности их использования, а для провайдера — потерю дополнительного комиссионного дохода за оказание платежно-расчетных сервисов.

Таким образом, второй вариант, при котором обеспечивается возможность распоряжения денежными средствами, переданными во временное пользование различным сервис-провайдерам, представляется более предпочтительным.

Поскольку очевидно, что в условиях многообразия режимов использования источников и приемников денежных средств реализовать второй вариант трудно, необходима унификация режимов использования, в том числе установление единого нормативно-правового регулирования со стороны единого регулятора, которым, как уже отмечалось, должен быть ЦБ РФ.

Унификация нормативно-правового регулирования порядка использования денежных средств, привлеченных во временное пользование, для оказания платежно-расчетных сервисов, позволит значительно увеличить число видов организаций, которые получают право на законных основаниях и в соответствии с едиными правилами оказывать такие сервисы. В принципе любое юридическое лицо получит возможность распоряжаться привлеченными денежными средствами в рамках, установленных законом, с целью предоставления платежно-расчетных сервисов как отдельного бизнеса либо в сочетании с другими видами услуг.

Анализируя используемые на практике виды источников и приемников денежных средств, можно заметить, что при всем их многообразии экономическое содержание их использования одинаково — во всех случаях речь идет о совершении некоторым лицом действий, заключающихся в обработке и хранении информации о денежных средствах (денежных требованиях к эмитенту денежных средств в определенной валюте), переданных ему во временное пользование другим лицом, находящимся в распоряжении этого лица.

Единообразие экономического содержания позволяет ввести единое нормативно-правовое регулирование. В качестве основы единой системы понятий предлагается использовать следующие термины: для описания основного механизма хранения информации о денежных средствах, которые одно лицо, владелец денежных средств, передало во временное пользование другому лицу, — «счет денежных средств»; для описания деятельности по обработке и хранению информации о денежных средствах — «ведение счета денежных средств» и «учет денежных средств»; для описания лица, распоряжающегося переданными ему во временное пользование денежными средствами, — «оператор счета денежных средств».

Подчеркнем, что термин «счет денежных средств» в предлагаемой системе понятий является более общим понятием, чем банковский счет, и включает в себя любые способы хранения информации о денежных требованиях к эмитенту, измеряемых в определенной валюте, любым лицом, являющимся оператором счета денежных средств. С этой точки зрения кошелек или матрац также могут считаться «счетами денежных средств».

В общем случае возможны два вида счетов денежных средств, на которых учитываются денежные средства, находящиеся в распоряжении оператора счета: 1) активный счет денежных средств, на котором учитываются собственные денежные средства оператора денежных средств, по сути являющиеся требованиями последнего к эмитенту денежных средств в данной валюте; и 2) пассивный счет денежных средств, на котором учитываются привлеченные денежные средства, предоставленные другим лицом во временное пользование оператору счета, т.е. денежные требования владельца денежных средств к оператору счета.

При разработке нормативно-правового регулирования важно правильно провести границу, отделяющую обычные коммерческие организации от кредитных. Единое регулирование отношений, возникающих в связи с привлечением во временное пользование денежных средств с целью обеспечить возможность распоряжения этими денежными средствами для оказания платежно-расчетных сервисов, не должно привести к наделению небанковских организаций полным спектром банковских функций.

Нормативно-правовой режим ведения счетов денежных средств должен, с одной стороны, предполагать ограниченный режим использования, с другой — учитывать необходимость снижения трудоемкости (как со стороны владельца счета, так и со стороны оператора) и не создавать избыточной транзакционной и «бюрократической» нагрузки на операторов и владельцев счетов в отношении всех операций, связанных с ведением и использованием счета. В частности, счет должен использоваться только для расчетов, с другой стороны — иметь облегченный режим открытия, отчетности и т.п.

В целях сохранения конкурентной среды важно обеспечить равные условия ведения бизнеса для банков и небанковских организаций в отношении аналогичных операций. В частности, это означает, что в части счетов, используемых банками для оказания платежно-расчетных сервисов ЦБ РФ должен быть установлен упрощенный режим, идентичный режиму использования аналогичных счетов в небанковских организациях.

С учетом особого характера денежных отношений функции оператора счета должны быть лицензируемым видом деятельности. Для организаций, желающих выполнять функции оператора счета денежных средств, это будет означать необходимость получения соответствующей лицензии ЦБ РФ и выполнения ряда требований, например, резервирования, отчислений в агентство по страхованию вкладов (в случае привлечения средств физических лиц) и предоставления отчетности в ЦБ РФ.

Кроме счетов денежных средств, режим которых, как уже сказано, должен регулироваться Банком России, других видов счетов быть не должно. Действительно, если принять, что в государстве действует единая система управления денежным обращением, существование какого-либо дополнительного механизма учета денежных средств теряет всякий смысл. Даже если такой механизм будет существовать, он будет подвержен таким же требованиям регулятора и с точки зрения использования при оказании платежных сервисов будет неотличим от счетов денежных средств. Если появится необходимость в счетах денежных средств с каким-либо особым режимом, то лучше такой режим предусмотреть в рамках общей системы правового регулирования счетов денежных средств.

Отметим, что с введением понятия «счет денежных средств» исчезает необходимость использования такого понятия, как «электронные денежные средства», введенного Законом об НПС.

Как следует из текста Закона, основными отличительными признаками электронных денежных средств являются использование для распоряжения ими электронных средств платежа (использование специальных средств идентификации и подтверждения сообщений, специальных каналов доступа) и учет электронных денежных средств посредством механизмов, отличных от механизма банковского счета.

Представляется, что введение нового вида денежных средств, выделенного на основании указанных признаков, не совсем корректно, так как эти признаки относятся к форме управления, а не к содержанию объекта управления.

Помимо некорректности выделения нового вида денежных средств по признаку формы управления такой подход приводит к одновременному сосуществованию в законе двух видов денежных средств, что усложняет и запутывает порядок использования привлеченных денежных средств для оказания платежно-расчетных сервисов, например, возникает необходимость регулирования взаимодействия обычных денежных средств и электронных денежных средств, возникают странные конструкции типа «обязательства по электронным денежным средствам» и т.п.

Между тем анализ текста Закона показывает, что электронные денежные средства по своей правовой природе и функционально ничем не отличаются от обычных безналичных денежных средств, а во всех положениях Закона, где рассматривается режим управления электронными денежными средствами, все описываемые действия с электронными денежными средствами близки к действиям с безналичными денежными средствами на банковских счетах. Таким образом, снова вернемся к предложенной ранее идее использования понятия счета денежных средств.

Требование счетов денежных средств как единого и исключительного механизма учета денежных средств не означает, что такие счета являются вообще единственным способом управления денежными средствами. Напротив, использование концепции счетов денежных средств предполагает многообразие техно-

логических способов использования денежных средств в рамках единой системы нормативно-правового регулирования. Счета денежных средств скорее должны рассматриваться как фундамент, над которым могут быть созданы различные надстройки в виде частных платежных систем, использующих собственные технологии учета денежных средств.

В связи с предложением передать полномочия нормативно-правового регулирования счетов денежных средств ЦБ РФ, следует понимать, что в этом случае Центральный Банк будет также устанавливать порядок отражения в бухгалтерском учете операций по таким счетам не только для банков, но и для всех организаций, получившей соответствующую лицензию.

В этой связи следует отметить, что существующие на сегодняшний день правила бухгалтерского учета, разработанные ЦБ РФ, не учитывают в полном объеме требования к оказанию платежно-расчетных сервисов, в частности, в том, что касается глобальных платежей, перекрывающих несколько часовых поясов, и расчетов в реальном времени.

Проблема состоит в том, что «бухгалтерском мире» учет построен на понятии «дискретного бухгалтерского времени», минимальный «квант» которого равен одному календарному дню, в то время как платежи и переводы денежных средств в «физическом» мире, особенно когда речь идет о платежах и переводах в реальном времени, происходят в физическом времени, которое непрерывно и измеряется в любых произвольно малых единицах — секундах, миллисекундах, микросекундах, наносекундах.

Требования осуществления платежей и переводов через несколько часовых поясов в реальном времени в сочетании с такой особенностью бухгалтерского учета, как привязка к определенному календарному дню, в некоторых случаях с другой порождает коллизии, которые не могут быть разрешены в рамках существующих правил бухгалтерского учета, что в результате делает невозможным предоставление отдельных видов сервисов (либо заставляет нарушать правила бухгалтерского учета).

Чтобы проиллюстрировать сказанное, рассмотрим пример. Банк хочет предоставить следующий сервис: если перевододатель через банкомат с функцией приема наличных денежных средств, находящийся в филиале банка, расположенном на востоке (московское время + 8 часов), пополняет счет получателя, открытый в филиале этого же банка на западе (московское время – 1 час), то получатель должен иметь возможность сразу снять деньги через кассу западного филиала.

Если операция проводится перевододателем в 6 утра местного времени дня X, то в момент снятия денег получателем со счета в западном филиале местное время 9 часов вечера дня X – 1. Это означает, что с точки зрения действующего порядка отражения операций в бухгалтерском учете денег на счете получателя в западном филиале в этот момент нет (они появятся через два часа, когда в западном филиале наступит день X). Как результат, банк не вправе разрешить получателю снятие денег и вынужден будет просить последнего подождать два часа. С точки зрения

бизнеса ситуация бессмысленная, деньги банком уже получены, но выданы быть не могут, так как будут нарушены формальные правила бухгалтерского учета.

Проблема «выдачи денег из будущего» может быть решена при использовании активного транзитного счета, на котором отразится «временной разрыв» — при снятии получателем денег через кассу счет будет дебетован бухгалтерским днем $X - 1$, на следующий бухгалтерский день X дебетовое сальдо будет закрыто в результате пополнения счета плательщиком через банкомат. В «физическом времени» порядок событий будет обратным — деньги будут внесены на счет до их снятия.

Поскольку использование активных транзитных счетов запрещено действующими правилами бухгалтерского учета, установленными ЦБ РФ, в порядок бухгалтерского учета в банках должны быть внесены изменения, в частности разрешено использование активных транзитных счетов для отражения подобных «временных разрывов».

Приложение к главе 11

Термины и сокращения

Национальная платежная система (НПС) — понимаемая как единый общественный институт совокупность, в которую входят: платежные сервисы, предусмотренные НПС; участники НПС; организационные, архитектурные, технические, технологические решения, используемые в рамках НПС; технические и технологические правила, стандарты, регламенты и протоколы НПС; нормативно-правовые акты, на основе и в рамках которых участники НПС, действуя во взаимодействии друг с другом, оказывают пользователям НПС платежные сервисы.

Пользователь НПС — любое юридическое или физическое лицо или предприниматель без образования юридического лица, резидент или нерезидент Российской Федерации, зарегистрированное в Национальном реестре пользователей СЭС, имеющее право использовать сервисы, предоставляемые НПС.

Участник НПС — любое юридическое лицо, резидент или нерезидент Российской Федерации, заключившее с национальным оператором НПС соглашение об оказании услуг другим участникам и (или) пользователям НПС.

Инвойс — документ, используемый в целях оформления расчетов при продаже товаров (услуг), в то числе счет, выставляемый продавцом, счет-проформа, счет-фактура.

Инвойсинг — деятельность по приему и доставке инвойсов.

Инвойсинг-сервис-провайдер (ИСП) — участник НИС, предоставляющий пользователям услуги инвойсинга.

Национальная система валовых расчетов — компонент национальной инфраструктуры НПС в виде совокупности национальных стандартов, организаци-

онных и технологических решений и участников НПС, обеспечивающий безналичные расчеты по совершенным сделкам.

Национальная система розничных платежей — компонент национальной инфраструктуры НПС в виде совокупности национальных стандартов, организационных и технологических решений и участников НПС, обеспечивающий обработку в реальном времени операций оплаты.

Национальная инвойсинговая система — компонент национальной инфраструктуры НПС в виде совокупности национальных стандартов, организационных и технологических решений и участников НПС, обеспечивающий обработку электронных счетов на оплату (инвойсов).

Электронный инвойс (ЭИ) — инвойс в форме электронного документа.

Эмитент — пользователь НИС, выставяющий инвойс.

Профиль пользователя (ПП) — совокупность данных пользователя, необходимых для использования пользователем сервисов, предлагаемых СЭВ, в том числе политика доставки.

Политика доставки (ПД) — совокупность параметров и правил, задающих алгоритм определения адреса, по которому должно быть передано ЭС, чтобы считаться доставленным пользователю.

ИСП — инвойсинг-сервис-провайдер.

НИК — национальный идентификационный код.

НИС — национальная инвойсинговая система.

НСРП — национальная система розничных платежей.

НСВР — национальная система валовых расчетов.

ЭС — электронное сообщение.

ГЛАВА 12

ЭВОЛЮЦИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ПРИМЕНЕНИЯ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ В РОССИЙСКОЙ НПС

Новые информационные технологии получили настолько широкое распространение, что сегодня практически все сферы общественной жизни в той или иной степени основываются и развиваются на базе этих технологий. Развитие законодательства в сфере регулирования безналичных расчетов в Российской Федерации в последние годы является, наверное, одним из самых ярких примеров воплощения на практике идей модернизации экономики и применения новых информационных технологий в финансовом секторе. Более того, учитывая те преимущества, которые предоставляют новейшие информационно-коммуникационные технологии пользователям традиционных финансовых услуг (в особенности розничный сегмент), представляется, что именно новые информационные технологии заставят финансовый сектор России в скором будущем превратиться в гораздо более высокотехнологичный и гораздо более конкурентный рынок услуг.

Еще несколько лет назад в России на законодательном уровне регулирование безналичных расчетов сводилось к нескольким статьям главы 46 «Расчеты» ГК РФ, устанавливающим основные формы безналичных расчетов (платежное поручение, аккредитив, чеки, инкассо). При этом законом установлено, что все безналичные расчеты должны осуществляться через кредитные организации, а непосредственный порядок осуществления указанных форм безналичных расчетов должен быть предусмотрен в отдельных федеральных законах, а также установленными в соответствии с ними банковскими правилами и применяемыми в банковской практике обычаями делового оборота. Вместе с тем исторически сложилось так, что все регулирование безналичных расчетов было отнесено не на законодательный уровень, а на уровень подзаконных актов ЦБ РФ, что можно объяснить субъектной «замкнутостью» указанных правоотношений (кредитные организации), с одной стороны, а с другой — спецификой традиционной банковской деятельности.

Первым изменением сложившейся ситуации в сфере законодательного регулирования безналичных расчетов явилось внесение изменений в ст. 13 Закона о банках и банковской деятельности в июле 2006 г. Тогда, прежде всего по причине массового распространения услуг мобильной связи и массовой необходимости их оплаты, а также в том числе по причине недостаточного распространения банковских отделений, некредитные организации начали оказывать услуги по приему наличных денежных средств от населения в качестве платы за услуги связи. Именно массовость услуг мобильной связи, а также технологическая возможность моментального подтверждения приема платежа стали той объективной потребностью, которая, по-видимому, заставила законодателей внести соответствующие изменения в Закон. Новая ст. 13.1 Закона о банках и банковской деятельности предусматривала, что некредитные организации вправе осуществлять прием денежных средств от населения за услуги связи и ЖКХ при одновременном соблюдении следующих условий:

- 1) обязательное наличие договора между кредитной организацией и таким лицом, по условиям которого лицо вправе лишь принимать денежные средства с целью их дальнейшего перевода получателям через кредитную организацию;
- 2) обязательное наличие договора между кредитной организацией и лицами, оказывающими услуги связи и ЖКХ, по условиям которого кредитная организация обязуется осуществлять переводы денежных средств, принятых третьими лицами в качестве оплаты услуг связи и ЖКХ.

Таким образом, законодателем была предоставлена возможность осуществления части (прием наличных денежных средств) традиционной банковской операции по переводу денежных средств некредитным организациям на основании соответствующего гражданско-правового договора с кредитной организацией. Представляется важным еще раз подчеркнуть, что такая ситуация стала возможна прежде всего в результате развития новых информационных технологий, которые позволяли моментально производить подтверждение оплаты массовых услуг связи. Именно моментальность подтверждения приема денежных средств (по сравнению, например, с трехдневным сроком зачисления денежных средств на счет получателя при традиционном банковском переводе) явилась той добавленной стоимостью для клиентов, которая обеспечила стремительное развитие данной деятельности. При этом, естественно, все расчеты между лицами, принявшими денежные средства, обслуживающими их кредитными организациями, а также получателями денежных средств продолжали осуществляться кредитными организациями в безналичной форме. Важным аспектом описанной ситуации представляется и то, что перевод денежных средств как банковская операция был разделен как на операционные составляющие (прием наличных денежных средств агентом и безналичные расчеты по банковским счетам), так и, что не менее важно, на функциональные (подтверждение (обмен) информацией и непосредственный перевод денежных средств).

В последующие годы деятельность по приему платежей населения на указанных выше правовых основаниях получила широкое распространение. Вместе с тем с дальнейшим развитием информационных технологий конструкция, состоящая из двух договоров (лицо, принимающее платежи, — кредитная организация — получатель платежа), выявила ряд неудобств с точки зрения правоприменения. На практике новые технологии позволили сделать рынок указанных услуг высококонкурентным как за счет применения недорогих специальных удаленных устройств для осуществления операций (так называемых платежных терминалов), так и все большего количества поставщиков товаров (работ, услуг), заинтересованных в дистанционной оплате своей продукции. В этих условиях выделились организации, которые начали специализироваться на предоставлении информационно-технологических услуг для целей обмена информацией о приеме платежей у физических лиц и подтверждении такого приема поставщикам услуг. Такие организации в рамках общей правоспособности юридических лиц выступали агентами поставщиков товаров (работ, услуг) и выстраивали соответствующие схемы расчетов на двусторонней основе. При этом все расчеты между указанными лицами продолжали осуществляться в безналичной форме через кредитные организации.

Сложившаяся ситуация получила логическое разрешение с принятием Закона о деятельности по приему платежей физических лиц, осуществляемой платежными агентами. Указанный Закон создал так называемую агентскую схему приема платежей в дополнение к «банковской агентской» схеме, существовавшей в соответствии с описанной выше ст. 13.1 Закона о банках и банковской деятельности. Правоспособность платежного агента возникает с момента заключения юридическим лицом гражданско-правового договора об осуществлении деятельности по приему платежей, физических лиц либо с оператором по приему платежей либо с поставщиком товаров (работ, услуг). Закон подробным образом описывает существенные условия такого договора, требования к информационному обеспечению деятельности платежных агентов, способы обеспечения обязательств, а также порядок осуществления государственного контроля за деятельностью платежных агентов. Корреспондирующие изменения были также внесены и в «банковский закон» с целью предотвращения возможности регуляторного арбитража между двумя параллельными алгоритмами работы.

Важной новеллой упомянутых изменений является норма, предусматривающая, что денежное обязательство плательщика — физического лица перед поставщиком товаров (работ, услуг) считается исполненным в размере внесенных платежному агенту денежных средств с момента их передачи платежному агенту. Указанное требование, с одной стороны, позволило значительно защитить интересы клиентов — физических лиц, а с другой стороны, внесло определенную правовую неясность в отношении того, участвуют ли платежные агенты непосредственно в безналичных расчетах или нет.

После устранения правовых рисков деятельности платежных агентов с принятием в июне 2009 г. Закона о деятельности по приему платежей физических лиц, осуществляемой платежными агентами, объем операций, проводимых через платежных агентов, вырос в несколько раз.

Вместе с тем дальнейшее развитие информационных технологий привело к появлению таких платежных инноваций, как электронные деньги, платежи через Интернет, платежи с использованием средств мобильной связи. С массовости использования указанных инноваций населением, а также их высокой социальной значимости возникла необходимость правового обеспечения данной деятельности. Кроме того, при создании правового регулирования требовалось учитывать то, что каждая из указанных инноваций имеет свои технологические особенности, а также свой специфичный состав участников правоотношений.

В дополнение к этому существующее на тот момент правовое регулирование безналичных расчетов не давало комплексного понимания структуры рынка платежных услуг, субъектного состава участников, возможностей и функций госрегулирования данного сектора услуг. Кроме того, возникли объективные потребности законодательно определить организационные и правовые основы функционирования розничных платежных систем как институтов, существенно снижающих издержки участников, уменьшающих технологические и операционные риски расчетов.

С учетом в том числе изложенных выше потребностей регулирования был разработан Закон о НПС.

Прежде всего необходимо отметить, что впервые на законодательном уровне было закреплено понятие «перевод денежных средств» как именно банковской операции, осуществляемой исключительно кредитными организациями в рамках применяемых форм безналичных расчетов по предоставлению получателю средств денежных средств плательщика. Перевод денежных средств наряду с приемом платежей (что является самостоятельной услугой) и почтовыми переводами были объединены в общую категорию платежной услуги. В продолжение данной логики национальная платежная система была определена как совокупность лиц, оказывающих платежные услуги в национальной экономике (кредитные организации, банковские платежные агенты, платежные агенты, организации федеральной почтовой связи, а также обслуживающие их инфраструктурные компании).

В части регулирования электронных денег Закон о НПС установил, что перевод электронных денег — это новая форма безналичных расчетов, осуществляемая исключительно кредитными организациями по поручениям своих клиентов с использованием электронных средств платежа. Сами электронные деньги определены как денежные средства, внесенные клиентами в кредитные организации и учитываемые без открытия им банковских счетов. Кредитным организациям, осуществляющим исключительно операции с электронными деньгами, Банк России будет выдавать новый вид «облегченных» лицензий.

В Законе подробным образом регулируются вопросы использования электронных средств платежа, под которыми понимаются различные способы удаленного управления денежными средствами, находящимися в кредитных организациях как на банковских счетах, так и без использования банковских счетов (электронные деньги). В этих целях в Законе закреплены основные права и обязанности участников данных отношений, которые до этого отсутствовали в национальном законодательстве.

Дополнительно проработан вопрос об ответственности сторон (оператор по переводу денежных средств и его клиент, применяющий ЭСП) за денежные средства, распоряжение которыми осуществляется с применением ЭСП. Концепция ответственности сторон строится на обмене информации: стороны обязаны в максимально сжатые сроки сообщать друг другу об операциях, проводимых с использованием ЭСП (оператор — в любом случае, пользователь — в случае несанкционированного использования ЭСП). На начальном этапе введения данного регулирования было принято решение максимально защитить пользователей ЭСП как более слабую сторону в рассматриваемых правоотношениях.

Законом вводятся три вида ЭСП для осуществления переводов электронных денежных средств: 1) неперсонифицированное ЭСП (идентификация клиента не производится, максимальный остаток электронных денег в любой момент времени не может превышать 15 тыс. руб., лимит по обороту в месяц — 40 тыс. руб., основное предназначение — для проведения микроплатежей в Интернете); 2) персонифицированное ЭСП (производится обязательная идентификация клиента, максимальный остаток электронных денег — 100 тыс. руб. (эквивалент в валюте) в любой момент времени); 3) корпоративное ЭСП (используется юридическими лицами — клиентами кредитной организации, максимальный остаток на конец рабочего дня — 100 тыс. руб., основное использование — в электронной коммерции).

Представляется, что снятие правовых рисков для участников этой деятельности (с использованием указанного подхода к регулированию электронных денег) позволит придать стимул ускоренному развитию института электронных денег как инновационной формы безналичных расчетов.

Еще одной важной новеллой Закона о НПС является легитимизация так называемых мобильных платежей. Фактически в последние годы уровень проникновения мобильной связи в несколько раз превысил уровень проникновения банковских услуг (из расчета количества банковских карт на душу населения). С учетом массовости использования устройств мобильной связи, а также совершенствования технологий на практике возникла практика осуществления розничных платежей абонентами операторов сотовых сетей, использующая средства «на счете» своего мобильного телефона.

Вместе с тем сложившаяся ситуация выявила как ряд очевидных правовых рисков для многочисленных участников описанных правоотношений (плательщик, оператор связи, банк, обслуживающий оператора связи, банк получателя

средств, получатель средств), так и явную необходимость законодательного закрепления требований по информационному обеспечению пользователей данных услуг.

Таким образом, ст. 13 Закона о НПС подробно описывает порядок взаимодействия оператора связи (у которого находятся средства абонента) и оператора электронных денежных средств (которому эти средства переводятся по поручению абонента) для осуществления последующих расчетов уже оператором электронных денежных средств. Таким же подробным образом описан порядок обмена информацией между операторами и клиентами (отдельно проработан вопрос раскрытия информации о комиссиях), вопросы обеспечения интересов клиентов (возможность отказаться от проведения операции также с использованием аппарата мобильной связи) и т.д.

В Законе о НПС также проведена работа по совершенствованию регулирования деятельности банковских платежных агентов. Для этой цели в законопроекте выделяется отдельная статья (которая мигрировала из Закона о банках и банковской деятельности), в которой детально описываются порядок и условия привлечения кредитными организациями указанной категории агентов. При этом существенно расширен функционал операций, осуществляемых такого рода агентами, включая в том числе проведение процедур идентификации клиентов в интересах кредитной организации.

Помимо иных важных новаций Закон о НПС впервые вводит в правовое поле понятие платежной системы, функции участников платежной системы и требования к их деятельности. В платежной системе обязательно должны быть: оператор, который разрабатывает правила платежной системы, операторы услуг платежной инфраструктуры (операционный, платежный клиринговый и расчетный центры) и как минимум три участника платежной системы (кредитные организации). Закон подробным образом описывает требования, предъявляемые к основному документу платежной системы — правилам платежной системы, которые являются публичными и не должны содержать никаких дискриминационных положений.

Подводя итог, хотелось бы отметить, что законодатель априори не в состоянии успеть в регулировании постоянно развивающихся правоотношений, тем более в случае широкого применения инновационных технологий. Вместе с тем пример регулирования сферы безналичных расчетов и платежных услуг в последние годы, на наш взгляд, является ярким показателем того, как законодательство способно обеспечивать необходимые условия для применения новейших технологий на практике и закладывать основу для их дальнейшего опережающего развития в будущем.

ПРИЛОЖЕНИЕ

ФЕДЕРАЛЬНЫЙ ЗАКОН

от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»

Принят Государственной Думой 14 июня 2011 г.

Одобрен Советом Федерации 22 июня 2011 г.

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа).

Статья 1. Предмет регулирования настоящего Федерального закона

Настоящий Федеральный закон устанавливает правовые и организационные основы национальной платежной системы, регулирует порядок оказания платежных услуг, в том числе осуществления перевода денежных средств, использования электронных средств платежа, деятельность субъектов национальной платежной системы, а также определяет требования к организации и функционированию платежных систем, порядок осуществления надзора и наблюдения в национальной платежной системе.

Статья 2. Нормативно-правовое регулирование отношений в национальной платежной системе¹

1. Законодательство Российской Федерации о национальной платежной системе основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и иных федеральных законов.

2. Правительство Российской Федерации и федеральные органы исполнительной власти в пределах своих полномочий в случаях, предусмотренных настоящим Федеральным законом и иными федеральными законами, могут принимать нормативные правовые акты в целях регулирования отношений в национальной платежной системе.

3. Центральный банк Российской Федерации (Банк России) в пределах своих полномочий в случаях, предусмотренных настоящим Федеральным законом и иными федеральными законами, может принимать нормативные акты в целях регулирования отношений в национальной платежной системе.

¹ Статья 2 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа).

Статья 3. Основные понятия, используемые в настоящем Федеральном законе

В настоящем Федеральном законе используются следующие основные понятия:

Пункт 1 статьи 3 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа).

1) **национальная платежная система** — совокупность операторов по переводу денежных средств (включая операторов электронных денежных средств), банковских платежных агентов (субагентов), платежных агентов, организаций федеральной почтовой связи при оказании ими платежных услуг в соответствии с законодательством Российской Федерации, операторов платежных систем, операторов услуг платежной инфраструктуры (субъекты национальной платежной системы);

2) **оператор по переводу денежных средств** — организация, которая в соответствии с законодательством Российской Федерации вправе осуществлять перевод денежных средств;

3) **оператор электронных денежных средств** — оператор по переводу денежных средств, осуществляющий перевод электронных денежных средств без открытия банковского счета (перевод электронных денежных средств);

4) **банковский платежный агент** — юридическое лицо, за исключением кредитной организации, или индивидуальный предприниматель, которые привлекаются кредитной организацией в целях осуществления деятельности, предусмотренной настоящим Федеральным законом;

5) **банковский платежный субагент** — юридическое лицо, за исключением кредитной организации, или индивидуальный предприниматель, которые привлекаются банковским платежным агентом в целях осуществления деятельности, предусмотренной настоящим Федеральным законом.

Пункт 6 статьи 3 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа);

6) **оператор платежной системы** — организация, определяющая правила платежной системы, а также выполняющая иные обязанности, предусмотренные настоящим Федеральным законом.

Пункт 7 статьи 3 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа);

7) **оператор услуг платежной инфраструктуры** — операционный центр, платежный клиринговый центр и расчетный центр.

Пункт 8 статьи 3 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа);

8) **операционный центр** — организация, обеспечивающая в рамках платежной системы для участников платежной системы и их клиентов доступ к услугам по переводу денежных средств, в том числе с использованием электронных средств платежа, а также обмен электронными сообщениями (далее — операционные услуги).

Пункт 9 статьи 3 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа);

9) платежный клиринговый центр — организация, созданная в соответствии с законодательством Российской Федерации, обеспечивающая в рамках платежной системы прием к исполнению распоряжений участников платежной системы об осуществлении перевода денежных средств и выполнение иных действий, предусмотренных настоящим Федеральным законом (далее — услуги платежного клиринга).

Пункт 10 статьи 3 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа);

10) центральный платежный клиринговый контрагент — платежный клиринговый центр, выступающий в соответствии с настоящим Федеральным законом плательщиком и получателем средств по переводам денежных средств участников платежной системы.

Пункт 11 статьи 3 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа);

11) расчетный центр — организация, созданная в соответствии с законодательством Российской Федерации, обеспечивающая в рамках платежной системы исполнение распоряжений участников платежной системы посредством списания и зачисления денежных средств по банковским счетам участников платежной системы, а также направление подтверждений, касающихся исполнения распоряжений участников платежной системы (далее — расчетные услуги).

Пункт 12 статьи 3 данного документа вступает в силу по истечении 180 дней после дня официального опубликования (пункт 2 статьи 39 данного документа);

12) перевод денежных средств — действия оператора по переводу денежных средств в рамках применяемых форм безналичных расчетов по предоставлению получателю средств денежных средств плательщика.

Пункт 13 статьи 3 данного документа вступает в силу по истечении 180 дней после дня официального опубликования (пункт 2 статьи 39 данного документа);

13) трансграничный перевод денежных средств — перевод денежных средств, при осуществлении которого плательщик либо получатель средств находится за пределами Российской Федерации, и (или) перевод денежных средств, при осуществлении которого плательщика или получателя средств обслуживает иностранный центральный (национальный) банк или иностранный банк.

Пункт 14 статьи 3 данного документа вступает в силу по истечении 180 дней после дня официального опубликования (пункт 2 статьи 39 данного документа);

14) безотзывность перевода денежных средств — характеристика перевода денежных средств, обозначающая отсутствие или прекращение возможности отзыва распоряжения об осуществлении перевода денежных средств в определенный момент времени.

Пункт 15 статьи 3 данного документа вступает в силу по истечении 180 дней после дня официального опубликования (пункт 2 статьи 39 данного документа);

15) **безусловность перевода денежных средств** — характеристика перевода денежных средств, обозначающая отсутствие условий или выполнение всех условий для осуществления перевода денежных средств в определенный момент времени.

Пункт 16 статьи 3 данного документа вступает в силу по истечении 180 дней после дня официального опубликования (пункт 2 статьи 39 данного документа);

16) **окончателность перевода денежных средств** — характеристика перевода денежных средств, обозначающая предоставление денежных средств получателю средств в определенный момент времени;

17) **платежная услуга** — услуга по переводу денежных средств, услуга почтового перевода и услуга по приему платежей;

18) **электронные денежные средства** — денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа. При этом не являются электронными денежными средствами денежные средства, полученные организациями, осуществляющими профессиональную деятельность на рынке ценных бумаг, клиринговую деятельность и (или) деятельность по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами и осуществляющими учет информации о размере предоставленных денежных средств без открытия банковского счета в соответствии с законодательством, регулирующим деятельность указанных организаций;

19) **электронное средство платежа** — средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

Пункт 20 статьи 3 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа);

20) **платежная система** — совокупность организаций, взаимодействующих по правилам платежной системы в целях осуществления перевода денежных средств, включающая оператора платежной системы, операторов услуг платежной инфраструктуры и участников платежной системы, из которых как минимум три организации являются операторами по переводу денежных средств.

Пункт 21 статьи 3 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа);

21) **значимая платежная система** — платежная система, отвечающая критериям, установленным настоящим Федеральным законом (системно значимая платежная система или социально значимая платежная система).

Пункт 22 статьи 3 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа);

22) **правила платежной системы** — документ (документы), содержащий (содержащие) условия участия в платежной системе, осуществления перевода денежных средств, оказания услуг платежной инфраструктуры и иные условия, определяемые оператором платежной системы в соответствии с настоящим Федеральным законом.

Пункт 23 статьи 3 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа);

23) **участники платежной системы** — организации, присоединившиеся к правилам платежной системы в целях оказания услуг по переводу денежных средств.

Пункт 24 статьи 3 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа);

24) **обмен электронными сообщениями** — получение операционным центром электронных сообщений, содержащих распоряжения участников платежной системы, передача указанных сообщений в платежный клиринговый центр, расчетный центр, а также передача извещений (подтверждений) о приеме и об исполнении распоряжений участников платежной системы.

Пункт 25 статьи 3 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа);

25) **платежные клиринговые позиции** — суммы денежных средств, подлежащих списанию и зачислению расчетным центром по банковским счетам участников платежной системы.

Глава 2. ПОРЯДОК ОКАЗАНИЯ ПЛАТЕЖНЫХ УСЛУГ, В ТОМ ЧИСЛЕ ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ, И ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА

Статья 4. Порядок оказания платежных услуг

1. Оператор по переводу денежных средств оказывает услуги по переводу денежных средств на основании договоров, заключаемых с клиентами и между операторами по переводу денежных средств, в рамках применяемых форм безналичных расчетов в соответствии с требованиями законодательства Российской Федерации.

2. Банковские платежные агенты и банковские платежные субагенты участвуют в оказании услуг по переводу денежных средств на основании договоров, заключаемых соответственно с операторами по переводу денежных средств и банковскими платежными агентами в соответствии с требованиями статьи 14 настоящего Федерального закона.

3. Организации федеральной почтовой связи оказывают услуги почтового перевода денежных средств в соответствии с требованиями Федерального закона от 17 июля 1999 года № 176-ФЗ «О почтовой связи».

4. Платежные агенты оказывают услуги по приему платежей в соответствии с Федеральным законом от 3 июня 2009 года № 103-ФЗ «О деятельности по приему платежей физических лиц, осуществляемой платежными агентами».

Статья 5 данного документа вступает в силу по истечении 180 дней после дня официального опубликования (пункт 2 статьи 39 данного документа).

Статья 5. Порядок осуществления перевода денежных средств

1. Оператор по переводу денежных средств осуществляет перевод денежных средств по распоряжению клиента (плательщика или получателя средств), оформленному в рамках применяемой формы безналичных расчетов (далее — распоряжение клиента).

2. Перевод денежных средств осуществляется за счет денежных средств плательщика, находящихся на его банковском счете или предоставленных им без открытия банковского счета.

3. Перевод денежных средств осуществляется в рамках применяемых форм безналичных расчетов посредством зачисления денежных средств на банковский счет получателя средств, выдачи получателю средств наличных денежных средств либо учета денежных средств в пользу получателя средств без открытия банковского счета при переводе электронных денежных средств.

4. Внесение наличных денежных средств на свой банковский счет или получение наличных денежных средств со своего банковского счета у одного оператора по переводу денежных средств не является переводом денежных средств.

5. Перевод денежных средств, за исключением перевода электронных денежных средств, осуществляется в срок не более трех рабочих дней начиная со дня списания денежных средств с банковского счета плательщика или со дня предоставления плательщиком наличных денежных средств в целях перевода денежных средств без открытия банковского счета.

6. В осуществлении перевода денежных средств наряду с оператором по переводу денежных средств, обслуживающим плательщика, и оператором по переводу денежных средств, обслуживающим получателя средств, могут участвовать другие операторы по переводу денежных средств (далее — посредники в переводе).

7. Если иное не обусловлено применяемой формой безналичных расчетов или федеральным законом, безотзывность перевода денежных средств, за исключением перевода электронных денежных средств, наступает с момента списания денежных средств с банковского счета плательщика или с момента предоставления плательщиком наличных денежных средств в целях перевода денежных средств без открытия банковского счета.

8. Безусловность перевода денежных средств наступает в момент выполнения определенных плательщиком и (или) получателем средств либо иными ли-

цами условий осуществления перевода денежных средств, в том числе осуществления встречного перевода денежных средств в иной валюте, встречной передачи ценных бумаг, представления документов, либо при отсутствии указанных условий.

9. В случае если плательщика средств и получателя средств обслуживает один оператор по переводу денежных средств, окончательность перевода денежных средств, за исключением перевода электронных денежных средств, наступает в момент зачисления денежных средств на банковский счет получателя средств или обеспечения получателю средств возможности получения наличных денежных средств.

10. В случае если плательщика средств и получателя средств обслуживают разные операторы по переводу денежных средств, окончательность перевода денежных средств наступает в момент зачисления денежных средств на банковский счет оператора по переводу денежных средств, обслуживающего получателя средств, с учетом требований статьи 25 настоящего Федерального закона.

11. При переводе денежных средств обязательство оператора по переводу денежных средств, обслуживающего плательщика, перед плательщиком прекращается в момент наступления его окончательности.

12. Оператор по переводу денежных средств до осуществления перевода денежных средств обязан предоставлять клиентам возможность ознакомления в доступной для них форме с условиями осуществления перевода денежных средств в рамках применяемой формы безналичных расчетов, в том числе:

- 1) с размером вознаграждения и порядком его взимания в случае, если оно предусмотрено договором;
- 2) со способом определения обменного курса, применяемого при осуществлении перевода денежных средств в иностранной валюте (при различии валюты денежных средств, предоставленных плательщиком, и валюты переводимых денежных средств);
- 3) с порядком предъявления претензий, включая информацию для связи с оператором по переводу денежных средств;
- 4) с иной информацией, обусловленной применяемой формой безналичных расчетов.

13. Клиент обязан предоставить оператору по переводу денежных средств достоверную информацию для связи с клиентом, а в случае ее изменения своевременно предоставить обновленную информацию. Обязанность оператора по переводу денежных средств по направлению клиенту уведомлений, предусмотренных настоящим Федеральным законом, считается исполненной при направлении уведомления в соответствии с имеющейся у оператора по переводу денежных средств информацией для связи с клиентом.

Статья 6 данного документа вступает в силу по истечении 180 дней после дня официального опубликования (пункт 2 статьи 39 данного документа).

Статья 6. Особенности осуществления перевода денежных средств по требованию получателя средств

1. При осуществлении безналичных расчетов в форме перевода денежных средств по требованию получателя средств (прямым дебетованием) оператор по переводу денежных средств на основании договора с плательщиком осуществляет списание денежных средств с банковского счета плательщика с его согласия (акцепта плательщика) по распоряжению получателя средств (далее — требование получателя средств).

2. Право получателя средств предъявлять требования к банковскому счету плательщика должно быть предусмотрено договором между обслуживающим плательщика оператором по переводу денежных средств и плательщиком.

3. Акцепт плательщика может быть дан до поступления требования получателя средств (заранее данный акцепт плательщика) или после его поступления обслуживающему плательщика оператору по переводу денежных средств. Акцепт плательщика может быть дан в договоре между обслуживающим плательщика оператором по переводу денежных средств и плательщиком либо в виде отдельного документа или сообщения.

4. Акцепт плательщика может быть дан в отношении одного или нескольких получателей средств, одного или нескольких требований получателя средств.

5. Требование получателя средств может направляться непосредственно обслуживающему плательщика оператору по переводу денежных средств или через оператора по переводу денежных средств, обслуживающего получателя средств.

6. В случае отсутствия заранее данного акцепта плательщика оператор по переводу денежных средств передает поступившее требование получателя средств для акцепта плательщику не позднее дня, следующего за днем поступления требования получателя средств.

7. Акцепт плательщика должен быть дан в течение пяти рабочих дней, если более короткий срок не предусмотрен договором между оператором по переводу денежных средств и плательщиком.

8. При акцепте плательщика требование получателя средств исполняется в сумме акцепта плательщика.

9. Допускается акцепт плательщика в части суммы требования получателя средств (частичный акцепт плательщика), если иное не предусмотрено договором между оператором по переводу денежных средств и плательщиком.

10. В случае частичного акцепта плательщика оператор по переводу денежных средств обязан указать на это при подтверждении получателю средств исполнения его требования.

11. При отказе плательщика от акцепта или неполучении акцепта в установленный срок требование получателя средств подлежит возврату получателю средств с указанием причины возврата.

12. При поступлении требования получателя средств с заранее данным акцептом плательщика обслуживающий плательщика оператор по переводу денежных

средств обязан проверить соответствие требования получателя средств условиям заранее данного акцепта плательщика.

13. При соответствии требования получателя средств условиям заранее данного акцепта плательщика оно исполняется в сумме и в срок, которые предусмотрены условиями заранее данного акцепта плательщика.

14. При несоответствии требования получателя средств условиям заранее данного акцепта плательщика или невозможности их проверки обслуживающий плательщика оператор по переводу денежных средств обязан возвратить требование получателя средств без исполнения, если договором не предусмотрена обязанность обслуживающего плательщика оператора по переводу денежных средств в указанном случае запросить акцепт плательщика.

15. Оператор по переводу денежных средств обязан направить плательщику уведомление об исполнении требования получателя средств не позднее дня, следующего за днем исполнения.

Статья 7. Особенности осуществления перевода электронных денежных средств

1. При осуществлении безналичных расчетов в форме перевода электронных денежных средств клиент предоставляет денежные средства оператору электронных денежных средств на основании заключенного с ним договора.

2. Клиент — физическое лицо может предоставлять денежные средства оператору электронных денежных средств с использованием своего банковского счета или без использования банковского счета.

3. Клиент — юридическое лицо или индивидуальный предприниматель предоставляет денежные средства оператору электронных денежных средств только с использованием своего банковского счета.

4. Оператор электронных денежных средств учитывает денежные средства, предоставленные клиентом, путем формирования записи, отражающей размер обязательств оператора электронных денежных средств перед клиентом в сумме предоставленных им денежных средств (далее — остаток электронных денежных средств).

5. Оператор электронных денежных средств не вправе предоставлять клиенту денежные средства для увеличения остатка электронных денежных средств клиента.

6. Оператор электронных денежных средств не вправе осуществлять начисление процентов на остаток электронных денежных средств или выплату любого вознаграждения клиенту.

7. Перевод электронных денежных средств осуществляется на основании распоряжений плательщиков в пользу получателей средств. В случаях, предусмотренных договорами между плательщиком и оператором электронных денежных средств, между плательщиком и получателем средств, перевод электронных денежных средств может осуществляться на основании требований получателей средств в соответствии со статьей 6 настоящего Федерального закона с учетом особенностей перевода электронных денежных средств, за исключением слу-

чаев использования электронных средств платежа, предусмотренных частью 4 статьи 10 настоящего Федерального закона.

8. Перевод электронных денежных средств может осуществляться между плательщиками и получателями средств, являющимися клиентами одного оператора электронных денежных средств или нескольких операторов электронных денежных средств.

9. При переводе электронных денежных средств юридические лица или индивидуальные предприниматели могут являться получателями средств, а также плательщиками в случае, если получателем средств является физическое лицо, использующее электронные средства платежа, указанные в части 2 статьи 10 настоящего Федерального закона.

10. Перевод электронных денежных средств осуществляется путем одновременного принятия оператором электронных денежных средств распоряжения клиента, уменьшения им остатка электронных денежных средств плательщика и увеличения им остатка электронных денежных средств получателя средств на сумму перевода электронных денежных средств.

11. Перевод электронных денежных средств осуществляется незамедлительно после принятия оператором электронных денежных средств распоряжения клиента.

12. Договором, заключенным оператором электронных денежных средств с клиентом, может быть предусмотрена возможность использования плательщиком — физическим лицом и получателем средств — юридическим лицом или индивидуальным предпринимателем электронных средств платежа, когда действия, указанные в части 10 настоящей статьи, осуществляются одновременно (далее — автономный режим использования электронного средства платежа). В таком случае получатель средств обязан ежедневно передавать информацию о совершенных операциях оператору электронных денежных средств для ее учета не позднее окончания рабочего дня оператора электронных денежных средств.

13. Оператор электронных денежных средств незамедлительно после исполнения распоряжения клиента об осуществлении перевода электронных денежных средств направляет клиенту подтверждение об исполнении указанного распоряжения.

14. В случае автономного режима использования электронного средства платежа оператор электронных денежных средств направляет плательщику и в случае, предусмотренном договором, получателю средств подтверждения об осуществлении перевода электронных денежных средств незамедлительно после учета оператором электронных денежных средств информации, полученной в соответствии с частью 12 настоящей статьи.

15. Перевод электронных денежных средств становится безотзывным и окончательным после осуществления оператором электронных денежных средств действий, указанных в части 10 настоящей статьи.

16. В случае автономного режима использования электронного средства платежа перевод электронных денежных средств становится безотзывным в мо-

мент использования клиентом электронного средства платежа в соответствии с требованиями части 12 настоящей статьи и окончательным после учета оператором электронных денежных средств информации, полученной в соответствии с частью 12 настоящей статьи.

17. Денежное обязательство плательщика перед получателем средств прекращается при наступлении окончательности перевода электронных денежных средств.

18. В случае автономного режима использования электронного средства платежа денежное обязательство плательщика перед получателем средств прекращается в момент наступления безотзывности перевода электронных денежных средств.

19. Оператор электронных денежных средств осуществляет на постоянной основе учет информации об остатках электронных денежных средств и осуществленных переводах электронных денежных средств.

20. Помимо осуществления перевода электронных денежных средств остаток (его часть) электронных денежных средств клиента — физического лица, использующего электронное средство платежа, предусмотренное частью 4 статьи 10 настоящего Федерального закона, может быть по его распоряжению переведен только на банковский счет. Такой остаток (его часть) электронных денежных средств клиента — физического лица не может быть выдан наличными денежными средствами.

21. Помимо осуществления перевода электронных денежных средств остаток (его часть) электронных денежных средств клиента — физического лица, использующего электронное средство платежа, предусмотренное частью 2 статьи 10 настоящего Федерального закона, может быть по его распоряжению переведен на банковский счет, переведен без открытия банковского счета или выдан наличными денежными средствами.

22. Помимо осуществления перевода электронных денежных средств остаток (его часть) электронных денежных средств клиента — юридического лица или индивидуального предпринимателя может быть по его распоряжению зачислен или переведен только на его банковский счет.

23. Клиент — юридическое лицо или индивидуальный предприниматель обязан иметь банковский счет, открытый у оператора электронных денежных средств для перевода остатка (его части) электронных денежных средств, или предоставить ему информацию о банковском счете этого юридического лица или индивидуального предпринимателя, открытом в иной кредитной организации, на который может осуществляться перевод остатка (его части) электронных денежных средств.

24. На переводы электронных денежных средств в иностранной валюте между резидентами, на переводы электронных денежных средств в иностранной валюте и валюте Российской Федерации между резидентами и нерезидентами, а также на переводы электронных денежных средств в иностранной валюте и валюте Российской Федерации между нерезидентами распространяются

требования валютного законодательства Российской Федерации, актов органов валютного регулирования и актов органов валютного контроля. Используемые в настоящем пункте понятия и термины применяются в том значении, в каком они используются в Федеральном законе от 10 декабря 2003 года № 173-ФЗ «О валютном регулировании и валютном контроле», если иное не предусмотрено настоящим Федеральным законом.

25. Оператор электронных денежных средств до заключения договора с клиентом — физическим лицом обязан предоставить ему следующую информацию:

1) о наименовании и месте нахождения оператора электронных денежных средств, а также о номере его лицензии на осуществление банковских операций;

2) об условиях использования электронного средства платежа, в том числе в автономном режиме;

3) о способах и местах осуществления перевода электронных денежных средств;

4) о способах и местах предоставления денежных средств клиентом — физическим лицом оператору электронных денежных средств;

5) о размере и порядке взимания оператором электронных денежных средств вознаграждения с физического лица в случае взимания вознаграждения;

6) о способах подачи претензий и порядке их рассмотрения, включая информацию для связи с оператором электронных денежных средств.

Статья 8 данного документа вступает в силу по истечении 180 дней после дня официального опубликования (пункт 2 статьи 39 данного документа).

Статья 8. Распоряжение клиента, порядок его приема к исполнению и исполнения

1. Распоряжение клиента должно содержать информацию, позволяющую осуществить перевод денежных средств в рамках применяемых форм безналичных расчетов (далее — реквизиты перевода). Перечень реквизитов перевода устанавливается нормативными актами Банка России, нормативными правовыми актами федеральных органов исполнительной власти и договором, заключенным оператором по переводу денежных средств с клиентом или между операторами по переводу денежных средств.

2. Распоряжение клиента может передаваться, приниматься к исполнению, исполняться и храниться в электронном виде, если иное не предусмотрено законодательством Российской Федерации, нормативными актами Банка России, нормативными правовыми актами Российской Федерации или договором, заключенным оператором по переводу денежных средств с клиентом или между операторами по переводу денежных средств.

3. Оператор по переводу денежных средств вправе составить распоряжение от своего имени для исполнения распоряжения клиента.

4. При приеме к исполнению распоряжения клиента оператор по переводу денежных средств обязан удостовериться в праве клиента распоряжаться денежными средствами, проверить реквизиты перевода, достаточность денежных

средств для исполнения распоряжения клиента, а также выполнить иные процедуры приема к исполнению распоряжений клиентов, предусмотренные законодательством Российской Федерации.

5. Если право клиента распоряжаться денежными средствами не удостоверено, а также если реквизиты перевода не соответствуют установленным требованиям, оператор по переводу денежных средств не принимает распоряжение клиента к исполнению и направляет клиенту уведомление об этом не позднее дня, следующего за днем получения распоряжения клиента.

6. Достаточность денежных средств, находящихся на банковском счете клиента, для исполнения его распоряжения определяется в порядке, установленном нормативными актами Банка России. При недостаточности денежных средств, находящихся на банковском счете клиента, оператор по переводу денежных средств не принимает распоряжение клиента к исполнению, если иное не предусмотрено законодательством Российской Федерации и договором, а также направляет клиенту уведомление об этом не позднее дня, следующего за днем получения распоряжения клиента.

7. При недостаточности денежных средств распоряжение клиента о переводе денежных средств без открытия банковского счета, включая перевод электронных денежных средств, не принимается к исполнению оператором по переводу денежных средств и клиенту незамедлительно направляется уведомление об этом.

8. Прием распоряжения клиента к исполнению подтверждается оператором по переводу денежных средств клиенту в порядке, предусмотренном законодательством Российской Федерации или договором.

9. Распоряжение клиента может быть до наступления безотзывности перевода денежных средств отозвано клиентом в порядке, предусмотренном законодательством Российской Федерации и договором.

10. Распоряжение клиента исполняется оператором по переводу денежных средств в рамках применяемых форм безналичных расчетов в размере суммы, указанной в распоряжении клиента. Вознаграждение оператора по переводу денежных средств (при его взимании) не может быть удержано из суммы перевода денежных средств, за исключением случаев осуществления трансграничных переводов денежных средств.

11. Исполнение распоряжения клиента подтверждается оператором по переводу денежных средств клиенту в порядке, предусмотренном законодательством Российской Федерации и договором.

12. Положения настоящей статьи применяются также в случае приема и исполнения распоряжений посредниками в переводе и в случае составления операторами по переводу денежных средств распоряжений от своего имени в целях исполнения распоряжений клиентов в рамках применяемых форм безналичных расчетов с учетом особенностей, предусмотренных законодательством Российской Федерации и договорами между операторами по переводу денежных средств.

Статья 9. Порядок использования электронных средств платежа

1. Использование электронных средств платежа осуществляется на основании договора об использовании электронного средства платежа, заключенного оператором по переводу денежных средств с клиентом, а также договоров, заключенных между операторами по переводу денежных средств.

Часть 2 статьи 9 данного документ вступает в силу по истечении 18 месяцев после дня официального опубликования (часть 4 статьи 39 данного документа).

2. Оператор по переводу денежных средств вправе отказать клиенту в заключении договора об использовании электронного средства платежа.

3. До заключения с клиентом договора об использовании электронного средства платежа оператор по переводу денежных средств обязан информировать клиента об условиях использования электронного средства платежа, в частности о любых ограничениях способов и мест использования, случаях повышенного риска использования электронного средства платежа.

Часть 4 статьи 9 вступают в силу по истечении 18 месяцев после дня официального опубликования (часть 4 статьи 39 данного документа).

4. Оператор по переводу денежных средств обязан информировать клиента о совершении каждой операции с использованием электронного средства платежа путем направления клиенту соответствующего уведомления в порядке, установленном договором с клиентом.

Часть 5 статьи 9 вступают в силу по истечении 18 месяцев после дня официального опубликования (часть 4 статьи 39 данного документа).

5. Оператор по переводу денежных средств обязан обеспечить возможность направления ему клиентом уведомления об утрате электронного средства платежа и (или) о его использовании без согласия клиента.

Часть 6 статьи 9 вступают в силу по истечении 18 месяцев после дня официального опубликования (часть 4 статьи 39 данного документа).

6. Оператор по переводу денежных средств обязан фиксировать направленные клиенту и полученные от клиента уведомления, а также хранить соответствующую информацию не менее трех лет.

Часть 7 статьи 9 вступают в силу по истечении 18 месяцев после дня официального опубликования (часть 4 статьи 39 данного документа).

7. Оператор по переводу денежных средств обязан предоставлять клиенту документы и информацию, которые связаны с использованием клиентом его электронного средства платежа, в порядке, установленном договором.

Часть 8 статьи 9 вступают в силу по истечении 18 месяцев после дня официального опубликования (часть 4 статьи 39 данного документа).

8. Оператор по переводу денежных средств обязан рассматривать заявления клиента, в том числе при возникновении споров, связанных с использованием клиентом его электронного средства платежа, а также предоставить клиенту возможность получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме по требованию клиента, в срок, установленный до-

говором, но не более 30 дней со дня получения таких заявлений, а также не более 60 дней со дня получения заявлений в случае использования электронного средства платежа для осуществления трансграничного перевода денежных средств.

9. Использование клиентом электронного средства платежа может быть приостановлено или прекращено оператором по переводу денежных средств на основании полученного от клиента уведомления или по инициативе оператора по переводу денежных средств при нарушении клиентом порядка использования электронного средства платежа в соответствии с договором.

10. Приостановление или прекращение использования клиентом электронного средства платежа не прекращает обязательств клиента и оператора по переводу денежных средств, возникших до момента приостановления или прекращения указанного использования.

Часть 11 статьи 9 вступают в силу по истечении 18 месяцев после дня официального опубликования (часть 4 статьи 39 данного документа).

11. В случае утраты электронного средства платежа и (или) его использования без согласия клиента клиент обязан направить соответствующее уведомление оператору по переводу денежных средств в предусмотренной договором форме незамедлительно после обнаружения факта утраты электронного средства платежа и (или) его использования без согласия клиента, но не позднее дня, следующего за днем получения от оператора по переводу денежных средств уведомления о совершенной операции.

Часть 12 статьи 9 вступают в силу по истечении 18 месяцев после дня официального опубликования (часть 4 статьи 39 данного документа).

12. После получения оператором по переводу денежных средств уведомления клиента в соответствии с частью 11 настоящей статьи оператор по переводу денежных средств обязан возместить клиенту сумму операции, совершенной без согласия клиента после получения указанного уведомления.

Часть 13 статьи 9 вступают в силу по истечении 18 месяцев после дня официального опубликования (часть 4 статьи 39 данного документа).

13. В случае, если оператор по переводу денежных средств не исполняет обязанность по информированию клиента о совершенной операции в соответствии с частью 4 настоящей статьи, оператор по переводу денежных средств обязан возместить клиенту сумму операции, о которой клиент не был проинформирован и которая была совершена без согласия клиента.

Часть 14 статьи 9 вступают в силу по истечении 18 месяцев после дня официального опубликования (часть 4 статьи 39 данного документа).

14. В случае, если оператор по переводу денежных средств исполняет обязанность по информированию клиента о совершенной операции в соответствии с частью 4 настоящей статьи и клиент не направил оператору по переводу денежных средств уведомление в соответствии с частью 11 настоящей статьи, оператор по переводу денежных средств не обязан возместить клиенту сумму операции, совершенной без согласия клиента.

Часть 15 статьи 9 вступают в силу по истечении 18 месяцев после дня официального опубликования (часть 4 статьи 39 данного документа).

15. В случае если оператор по переводу денежных средств исполняет обязанность по уведомлению клиента — физического лица о совершенной операции в соответствии с частью 4 настоящей статьи и клиент — физическое лицо направил оператору по переводу денежных средств уведомление в соответствии с частью 11 настоящей статьи, оператор по переводу денежных средств должен возместить клиенту сумму указанной операции, совершенной без согласия клиента до момента направления клиентом — физическим лицом уведомления. В указанном случае оператор по переводу денежных средств обязан возместить сумму операции, совершенной без согласия клиента, если не докажет, что клиент нарушил порядок использования электронного средства платежа, что повлекло совершение операции без согласия клиента — физического лица.

Часть 16 статьи 9 вступают в силу по истечении 18 месяцев после дня официального опубликования (часть 4 статьи 39 данного документа).

16. Положения части 15 настоящей статьи в части обязанности оператора по переводу денежных средств возместить сумму операции, совершенной без согласия клиента до момента направления клиентом — физическим лицом уведомления, не применяются в случае совершения операции с использованием клиентом — физическим лицом электронного средства платежа, предусмотренного частью 4 статьи 10 настоящего Федерального закона.

Статья 10. Порядок использования электронных средств платежа при осуществлении перевода электронных денежных средств

1. Перевод электронных денежных средств осуществляется с проведением идентификации клиента или без проведения идентификации в соответствии с Федеральным законом от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

2. В случае проведения оператором электронных денежных средств идентификации клиента — физического лица в соответствии с Федеральным законом от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» использование электронного средства платежа осуществляется клиентом — физическим лицом при условии, что остаток электронных денежных средств в любой момент не превышает 100 тысяч рублей либо сумму в иностранной валюте, эквивалентную 100 тысячам рублей по официальному курсу Банка России. Указанное электронное средство платежа является персонифицированным.

3. Допускается превышение суммы, указанной в части 2 настоящей статьи, вследствие изменения официального курса иностранной валюты, устанавливаемого Банком России.

4. В случае непроведения оператором электронных денежных средств идентификации клиента — физического лица в соответствии с Федеральным законом

от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» использование электронного средства платежа осуществляется клиентом — физическим лицом при условии, что остаток электронных денежных средств в любой момент не превышает 15 тысяч рублей. Указанное электронное средство платежа является неперсонифицированным.

5. Общая сумма переводимых электронных денежных средств с использованием одного неперсонифицированного электронного средства платежа не может превышать 40 тысяч рублей в течение календарного месяца.

6. Оператор электронных денежных средств не осуществляет перевод электронных денежных средств, если в результате такого перевода будут превышены суммы, указанные в частях 2, 4 и 5 настоящей статьи. При этом физическое лицо вправе получить остаток (его часть) электронных денежных средств в соответствии с частями 20 и 21 статьи 7 настоящего Федерального закона.

7. Использование электронного средства платежа клиентом — юридическим лицом или индивидуальным предпринимателем осуществляется с проведением его идентификации оператором электронных денежных средств в соответствии с Федеральным законом от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Указанное электронное средство платежа является корпоративным. Использование корпоративного электронного средства платежа осуществляется при условии, что остаток электронных денежных средств не превышает 100 тысяч рублей либо сумму в иностранной валюте, эквивалентную 100 тысячам рублей по официальному курсу Банка России, на конец рабочего дня оператора электронных денежных средств.

8. Допускается превышение суммы, указанной в части 7 настоящей статьи, вследствие изменения официального курса иностранной валюты, устанавливаемого Банком России.

9. В случае превышения суммы, указанной в части 7 настоящей статьи, оператор электронных денежных средств обязан осуществить зачисление или перевод денежных средств в размере превышения указанного ограничения на банковский счет юридического лица или индивидуального предпринимателя без его распоряжения.

10. Оператор электронных средств платежа обязан обеспечивать при использовании электронных средств платежа, предусмотренных настоящей статьей, возможность их определения клиентами как неперсонифицированных, персонифицированных или корпоративных электронных средств платежа.

11. Переводы электронных денежных средств с использованием персонифицированных электронных средств платежа, корпоративных электронных средств платежа могут быть приостановлены в порядке и случаях, которые аналогичны порядку и случаям приостановления операций по банковскому счету, которые предусмотрены законодательством Российской Федерации.

12. При переводе электронных денежных средств с использованием персонализированных электронных средств платежа и корпоративных электронных средств платежа на остаток электронных денежных средств может быть обращено взыскание в соответствии с законодательством Российской Федерации.

13. Оператор электронных денежных средств обязан обеспечить невозможность использования электронного средства платежа до ознакомления клиента — физического лица с информацией, указанной в части 25 статьи 7 настоящего Федерального закона.

14. Положения настоящей статьи о порядке использования корпоративных электронных средств платежа применяются также к электронным средствам платежа, используемым нотариусом, занимающимся частной практикой, или адвокатом, учредившим адвокатский кабинет.

Глава 3. СУБЪЕКТЫ НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЫ И ТРЕБОВАНИЯ К ИХ ДЕЯТЕЛЬНОСТИ

Статья 11. Оператор по переводу денежных средств и требования к его деятельности

1. Операторами по переводу денежных средств являются:

- 1) Банк России;
- 2) кредитные организации, имеющие право на осуществление перевода денежных средств;
- 3) государственная корпорация «Банк развития и внешнеэкономической деятельности (Внешэкономбанк)» (далее — Внешэкономбанк).

2. Банк России осуществляет деятельность оператора по переводу денежных средств в соответствии с настоящим Федеральным законом, Федеральным законом от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» и нормативными актами Банка России.

3. Кредитные организации осуществляют деятельность операторов по переводу денежных средств в соответствии с настоящим Федеральным законом, Федеральным законом «О банках и банковской деятельности» и нормативными актами Банка России.

4. Внешэкономбанк осуществляет деятельность оператора по переводу денежных средств в соответствии с настоящим Федеральным законом и Федеральным законом от 17 мая 2007 года № 82-ФЗ «О банке развития».

Статья 12. Оператор электронных денежных средств и требования к его деятельности

1. Оператором электронных денежных средств является кредитная организация, в том числе небанковская кредитная организация, имеющая право на осуществление переводов денежных средств без открытия банковских счетов и связанных с ними иных банковских операций, предусмотренная пунктом 1 части третьей статьи 1 Федерального закона «О банках и банковской деятельности».

2. Лицо, не являющееся оператором электронных денежных средств, не вправе становиться обязанным по электронным денежным средствам и осуществлять перевод электронных денежных средств.

3. Лицо, не являющееся оператором электронных денежных средств, не вправе становиться обязанным по денежным обязательствам, которые используются для исполнения денежных обязательств между иными лицами или совершения иных сделок, влекущих прекращение обязательств между иными лицами, на основании распоряжений, передаваемых в электронном виде обязанному лицу. Положения настоящей части не распространяются на прекращение денежных обязательств с участием организаций, осуществляющих профессиональную деятельность на рынке ценных бумаг, клиринговую деятельность, деятельность центрального контрагента и (или) деятельность по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами, в соответствии с законодательством, регулирующим деятельность указанных организаций.

4. Оператор электронных денежных средств обязан уведомить Банк России в установленном им порядке о начале деятельности по осуществлению перевода электронных денежных средств не позднее 10 рабочих дней со дня первого увеличения остатка электронных денежных средств. В уведомлении должны быть указаны:

- 1) наименование и место нахождения оператора электронных денежных средств, а также номер его лицензии на осуществление банковских операций;
- 2) вид (виды) предоставляемых клиентам электронных средств платежа;
- 3) наименования организаций, привлеченных оператором электронных денежных средств для оказания операционных услуг и (или) услуг платежного клиринга (при их привлечении).

5. Оператор электронных денежных средств обязан установить правила осуществления перевода электронных денежных средств, включая:

- 1) порядок деятельности оператора электронных денежных средств, связанной с переводом электронных денежных средств;
- 2) порядок предоставления клиентам электронных средств платежа и осуществления перевода электронных денежных средств с их использованием;
- 3) порядок деятельности оператора электронных денежных средств при привлечении банковских платежных агентов, организаций, оказывающих операционные услуги и (или) услуги платежного клиринга;
- 4) порядок обеспечения бесперебойности осуществления перевода электронных денежных средств;
- 5) порядок рассмотрения претензий оператором электронных денежных средств, включая процедуры оперативного взаимодействия с клиентами;
- 6) порядок обмена информацией при осуществлении переводов электронных денежных средств.

6. Оператор электронных денежных средств обязан обеспечить бесперебойность осуществления перевода электронных денежных средств в соответствии с требованиями, установленными нормативными актами Банка России.

7. Оператор электронных денежных средств вправе заключать договоры с другими организациями, по условиям которых эти организации вправе оказывать оператору электронных денежных средств операционные услуги и (или) услуги платежного клиринга при осуществлении перевода электронных денежных средств.

Статья 13. Требования к деятельности оператора электронных денежных средств при увеличении остатков электронных денежных средств физических лиц — абонентов оператора связи

1. Оператор электронных денежных средств вправе заключить с оператором связи, имеющим право самостоятельно оказывать услуги радиотелефонной подвижной связи (далее — оператор связи), договор, по условиям которого оператор электронных денежных средств вправе увеличивать остаток электронных денежных средств физического лица — абонента такого оператора связи за счет его денежных средств, являющихся авансом за услуги связи, в порядке, установленном настоящей статьей. Увеличение остатка электронных денежных средств оператором электронных денежных средств осуществляется при наличии договора, заключенного с таким физическим лицом, предусмотренного частью 1 статьи 7 настоящего Федерального закона.

2. Оператор связи не вправе предоставлять физическому лицу — абоненту денежные средства в целях увеличения оператором электронных денежных средств остатка электронных денежных средств.

3. Оператор электронных денежных средств и оператор связи осуществляют информационное и технологическое взаимодействие в целях увеличения остатков электронных денежных средств в порядке, предусмотренном договором.

4. Увеличение остатка электронных денежных средств физического лица — абонента оператора связи осуществляется на основании его распоряжения, передаваемого оператором связи оператору электронных денежных средств, в соответствии с соглашением между физическим лицом — абонентом и оператором связи.

5. Оператор связи обязан уменьшить сумму денежных средств физического лица — абонента, внесенных им в качестве аванса за услуги связи, незамедлительно после получения подтверждения оператора электронных денежных средств об увеличении остатка электронных денежных средств указанного физического лица — абонента. С момента увеличения остатка электронных денежных средств оператор электронных денежных средств становится обязанным перед физическим лицом в размере суммы, на которую был увеличен остаток электронных денежных средств.

6. Оператор связи до предоставления возможности передачи распоряжений физического лица — абонента, указанных в части 4 настоящей статьи, обязан обеспечить физическому лицу — абоненту возможность ознакомления с инфор-

мацией о деятельности оператора электронных денежных средств, указанной в части 25 статьи 7 настоящего Федерального закона.

Положения части 7 статьи 13 данного документа не применяются в случае, если с физического лица — абонента не взимается вознаграждение оператором связи, а также оператором электронных денежных средств за увеличение остатка электронных денежных средств (часть 9 статьи 13 данного документа).

7. Оператор связи должен предоставлять физическому лицу — абоненту до передачи его распоряжения оператору электронных денежных средств следующую информацию:

- 1) об электронном средстве платежа физического лица;
- 2) о сумме увеличения остатка электронных денежных средств;
- 3) о размере вознаграждения, уплачиваемого физическим лицом — абонентом, в случае его взимания;
- 4) о дате и времени предоставления информации.

Положения части 8 статьи 13 данного документа не применяются в случае, если с физического лица — абонента не взимается вознаграждение оператором связи, а также оператором электронных денежных средств за увеличение остатка электронных денежных средств (часть 9 статьи 13 данного документа).

8. Физическое лицо — абонент вправе отказаться от передачи распоряжения оператору электронных денежных средств после получения информации, указанной в части 7 настоящей статьи, а оператор связи обязан обеспечить ему такую возможность.

9. Положения частей 7 и 8 настоящей статьи не применяются в случае, если с физического лица — абонента не взимается вознаграждение оператором связи, а также оператором электронных денежных средств за увеличение остатка электронных денежных средств.

10. Оператор электронных денежных средств не вправе осуществлять увеличение остатка электронных денежных средств физического лица — абонента при превышении сумм, установленных статьей 10 настоящего Федерального закона.

11. Оператор связи обязан направить физическому лицу — абоненту с использованием сетей радиотелефонной подвижной связи подтверждение увеличения остатка электронных денежных средств незамедлительно после получения соответствующей информации от оператора электронных денежных средств. Такое подтверждение должно включать в себя информацию, предусмотренную частью 7 настоящей статьи.

12. Оператор связи обязан осуществлять расчеты с оператором электронных денежных средств в сумме увеличенных остатков электронных денежных средств не позднее рабочего дня, следующего за днем увеличения остатков электронных денежных средств. При неисполнении оператором связи указанной обязанности оператор электронных денежных средств приостанавливает увеличение остатков электронных денежных средств до исполнения такой обязанности оператором связи.

Действие статьи 14 распространяется на отношения, возникшие из договоров, ранее заключенных кредитными организациями и организациями, не являющимися кредитными организациями, а также индивидуальными предпринимателями в соответствии со статьей 13.1 Федерального закона «О банках и банковской деятельности» (часть 9 статьи 38 данного документа).

Статья 14. Требования к деятельности оператора по переводу денежных средств при привлечении банковского платежного агента (субагента)

1. Оператор по переводу денежных средств, являющийся кредитной организацией, в том числе небанковской кредитной организацией, имеющей право на осуществление переводов денежных средств без открытия банковских счетов и связанных с ними иных банковских операций в соответствии с Федеральным законом «О банках и банковской деятельности», вправе на основании договора привлекать банковского платежного агента:

1) для принятия от физического лица наличных денежных средств и (или) выдачи физическому лицу наличных денежных средств, в том числе с применением платежных терминалов и банкоматов;

2) для предоставления клиентам электронных средств платежа и обеспечения возможности использования указанных электронных средств платежа в соответствии с условиями, установленными оператором по переводу денежных средств;

3) для проведения идентификации клиента — физического лица, его представителя и (или) выгодоприобретателя в целях осуществления перевода денежных средств без открытия банковского счета в соответствии с требованиями законодательства Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

2. Банковский платежный агент, являющийся юридическим лицом, в случаях, предусмотренных договором с оператором по переводу денежных средств, вправе привлекать банковского платежного субагента на основании заключаемого с ним договора для осуществления деятельности (ее части), указанной в пунктах 1 и 2 части 1 настоящей статьи. При таком привлечении соответствующие полномочия банковского платежного субагента не требуют нотариального удостоверения.

3. Привлечение оператором по переводу денежных средств банковского платежного агента может осуществляться при одновременном соблюдении следующих требований:

1) осуществлении указанной в части 1 настоящей статьи деятельности (ее части) (далее — операции банковского платежного агента) от имени оператора по переводу денежных средств;

2) проведении банковским платежным агентом в соответствии с требованиями законодательства Российской Федерации о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма идентификации клиента — физического лица, его представителя и (или) выгодоприобретателя в целях осуществления перевода денежных средств без открытия банковского счета;

3) использовании банковским платежным агентом специального банковского счета (счетов) для зачисления в полном объеме полученных от физических лиц наличных денежных средств в соответствии с частями 5 и 6 настоящей статьи;

4) подтверждении банковским платежным агентом принятия (выдачи) наличных денежных средств путем выдачи кассового чека, соответствующего требованиям частей 10—13 настоящей статьи;

5) предоставлении банковским платежным агентом физическим лицам информации, предусмотренной частью 15 настоящей статьи;

6) применении банковским платежным агентом платежных терминалов и банкоматов в соответствии с требованиями законодательства Российской Федерации о применении контрольно-кассовой техники при осуществлении наличных денежных расчетов.

4. Привлечение банковским платежным агентом банковского платежного субагента может осуществляться при одновременном соблюдении следующих требований:

1) осуществлении указанной в части 1 настоящей статьи деятельности (ее части) (далее — операции банковского платежного субагента) от имени оператора по переводу денежных средств;

2) осуществлении операций банковского платежного субагента, не требующих идентификации физического лица в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

3) запрете для платежного банковского субагента на привлечение других лиц к осуществлению операций банковского платежного субагента;

4) использовании банковским платежным субагентом специального банковского счета (счетов) для зачисления в полном объеме полученных от физических лиц наличных денежных средств в соответствии с частями 5 и 6 настоящей статьи;

5) подтверждении банковским платежным субагентом принятия (выдачи) наличных денежных средств путем выдачи кассового чека, соответствующего требованиям частей 10—13 настоящей статьи;

6) предоставлении банковским платежным субагентом физическим лицам информации, предусмотренной частью 15 настоящей статьи;

7) применении банковским платежным субагентом платежных терминалов и банкоматов в соответствии с требованиями законодательства Российской Федерации о применении контрольно-кассовой техники при осуществлении наличных денежных расчетов.

5. По специальному банковскому счету банковского платежного агента (субагента) могут осуществляться следующие операции:

1) зачисление принятых от физических лиц наличных денежных средств;

2) зачисление денежных средств, списанных с другого специального банковского счета банковского платежного агента (субагента);

3) списание денежных средств на банковские счета.

6. Осуществление иных операций, помимо предусмотренных частью 5 настоящей статьи, по специальному банковскому счету не допускается.

7. Контроль за соблюдением банковскими платежными агентами (субагентами) обязанностей по сдаче оператору по переводу денежных средств полученных от физических лиц наличных денежных средств для зачисления в полном объеме на свой специальный банковский счет (счета), а также по использованию банковскими платежными агентами (субагентами) специальных банковских счетов для осуществления расчетов осуществляют налоговые органы Российской Федерации.

8. Оператор по переводу денежных средств обязан выдавать налоговым органам справки о наличии у него специальных банковских счетов и (или) об остатках денежных средств на специальных банковских счетах, выписки по операциям на специальных банковских счетах организаций (индивидуальных предпринимателей), являющихся банковскими платежными агентами (субагентами), в течение трех дней со дня получения мотивированного запроса налогового органа. Справки о наличии специальных банковских счетов и (или) об остатках денежных средств на специальных банковских счетах, а также выписки по операциям на специальных банковских счетах организаций (индивидуальных предпринимателей), являющихся банковскими платежными агентами (субагентами) у такого оператора по переводу денежных средств, могут быть запрошены налоговыми органами в случаях проведения контроля, предусмотренного частью 7 настоящей статьи, в отношении этих организаций (индивидуальных предпринимателей), являющихся банковскими платежными агентами (субагентами).

9. Форма (форматы) и порядок направления налоговыми органами запроса оператору по переводу денежных средств устанавливаются федеральным органом исполнительной власти, уполномоченным по контролю и надзору в области налогов и сборов. Форма и порядок предоставления оператором по переводу денежных средств информации по запросам налоговых органов устанавливаются федеральным органом исполнительной власти, уполномоченным по контролю и надзору в области налогов и сборов, по согласованию с Центральным банком Российской Федерации. Форматы предоставления оператором по переводу денежных средств в электронном виде информации по запросам налоговых органов утверждаются Центральным банком Российской Федерации по согласованию с федеральным органом исполнительной власти, уполномоченным по контролю и надзору в области налогов и сборов.

10. Контрольно-кассовая техника в составе платежного терминала, банкомата, применяемого банковскими платежными агентами (субагентами), должна обеспечивать выдачу кассового чека, содержащего следующие обязательные реквизиты:

- 1) наименование документа — кассовый чек;
- 2) общую сумму принятых (выданных) денежных средств;
- 3) наименование операции банковского платежного агента (субагента);

4) размер вознаграждения, уплачиваемого физическим лицом в виде общей суммы, включающей в том числе вознаграждение банковского платежного агента (субагента) в случае его взимания;

5) дату, время приема (выдачи) денежных средств;

6) номер кассового чека и контрольно-кассовой техники;

7) адрес места приема (выдачи) денежных средств;

8) наименование и место нахождения оператора по переводу денежных средств и банковского платежного агента (субагента), а также их идентификационные номера налогоплательщика;

9) номера телефонов оператора по переводу денежных средств, банковского платежного агента и банковского платежного субагента.

11. Все реквизиты, напечатанные на кассовом чеке, должны быть четкими и легко читаемыми в течение не менее шести месяцев.

12. Кассовый чек может содержать также иные реквизиты в случаях, если это предусмотрено договором между оператором по переводу денежных средств и банковским платежным агентом.

13. Применяемые банковским платежным агентом (субагентом) платежные терминалы или банкоматы должны обеспечивать печать на кассовом чеке своего номера и реквизитов, предусмотренных частью 10 настоящей статьи, в некорректируемом виде, обеспечивающем идентичность информации, зарегистрированной на кассовом чеке, контрольной ленте и в фискальной памяти контрольно-кассовой техники.

14. В случае изменения адреса места установки платежного терминала или банкомата банковский платежный агент (субагент) обязан в день осуществления такого изменения направить соответствующее уведомление в налоговый орган с указанием нового адреса места установки контрольно-кассовой техники, входящей в состав платежного терминала или банкомата.

15. При привлечении банковского платежного агента (субагента) в каждом месте осуществления операций банковского платежного агента (субагента) до начала осуществления каждой операции физическим лицам должна предоставляться следующая информация:

1) адрес места осуществления операций банковского платежного агента (субагента);

2) наименование и место нахождения оператора по переводу денежных средств и банковского платежного агента (субагента), а также их идентификационные номера налогоплательщика;

3) номер лицензии оператора по переводу денежных средств на осуществление банковских операций;

4) реквизиты договора между оператором по переводу денежных средств и банковским платежным агентом, а также реквизиты договора между банковским платежным агентом и банковским платежным субагентом в случае его привлечения;

5) размер вознаграждения, уплачиваемого физическим лицом в виде общей суммы, включающей в том числе вознаграждение банковского платежного агента (субагента) в случае его взимания;

6) способы подачи претензий и порядок их рассмотрения;

7) номера телефонов оператора по переводу денежных средств, банковского платежного агента и банковского платежного субагента.

16. При использовании банковским платежным агентом (субагентом) платежного терминала или банкомата информация, предусмотренная частью 15 настоящей статьи, должна предоставляться физическим лицам в автоматическом режиме.

17. Банковский платежный агент вправе взимать с физических лиц вознаграждение, если это предусмотрено договором с оператором по переводу денежных средств.

18. Банковский платежный субагент вправе взимать с физических лиц вознаграждение, если это предусмотрено договором с банковским платежным агентом и договором банковского платежного агента с оператором по переводу денежных средств.

19. Оператор по переводу денежных средств должен вести перечень банковских платежных агентов (субагентов), в котором указываются адреса всех мест осуществления операций банковских платежных агентов (субагентов) по каждому банковскому платежному агенту (субагенту) и с которым можно ознакомиться по запросу физических лиц. Оператор по переводу денежных средств обязан предоставлять перечень банковских платежных агентов (субагентов) налоговым органам по их запросу. Банковский платежный агент обязан передавать оператору по переводу денежных средств информацию о привлеченных банковских платежных субагентах, необходимую для включения в указанный перечень, в порядке, установленном договором с оператором по переводу денежных средств.

20. Оператор по переводу денежных средств должен осуществлять контроль за соблюдением банковским платежным агентом условий его привлечения, установленных настоящей статьей и договором между оператором по переводу денежных средств и банковским платежным агентом, а также законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

21. Несоблюдение банковским платежным агентом условий его привлечения, требований настоящей статьи и законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма является основанием для одностороннего отказа оператора по переводу денежных средств от исполнения договора с таким банковским платежным агентом.

22. Банковский платежный агент должен осуществлять контроль за соблюдением банковским платежным субагентом условий его привлечения, установленных настоящей статьей и договором между банковским платежным агентом и банковским платежным субагентом, а также требований настоящей статьи.

23. Несоблюдение банковским платежным субагентом условий его привлечения и требований настоящей статьи является основанием для одностороннего отказа банковского платежного агента от исполнения договора с таким банковским платежным субагентом, в том числе по требованию оператора по переводу денежных средств.

24. Порядок осуществления контроля оператором по переводу денежных средств за деятельностью банковских платежных агентов устанавливается нормативными актами Банка России и договором между оператором по переводу денежных средств и банковским платежным агентом.

25. Порядок осуществления контроля банковским платежным агентом за деятельностью банковского платежного субагента устанавливается договором между оператором по переводу денежных средств и банковским платежным агентом, а также договором между банковским платежным агентом и банковским платежным субагентом.

Статья 15 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа).

Статья 15. Оператор платежной системы и требования к его деятельности

1. Оператором платежной системы может являться кредитная организация, организация, не являющаяся кредитной организацией и созданная в соответствии с законодательством Российской Федерации, Банк России или Внешэкономбанк.

2. Оператор платежной системы, являющийся кредитной организацией, Банком России или Внешэкономбанком, может совмещать свою деятельность с деятельностью оператора по переводу денежных средств, оператора услуг платежной инфраструктуры и с иной деятельностью, если это не противоречит законодательству Российской Федерации.

3. Оператор платежной системы, не являющийся кредитной организацией, может совмещать свою деятельность с деятельностью оператора услуг платежной инфраструктуры (за исключением расчетного центра) и с иной деятельностью, если это не противоречит законодательству Российской Федерации.

4. Банк России осуществляет деятельность оператора платежной системы на основании настоящего Федерального закона в соответствии с нормативными актами Банка России и заключаемыми договорами.

5. Оператор платежной системы обязан:

1) определять правила платежной системы, организовывать и осуществлять контроль за их соблюдением участниками платежной системы, операторами услуг платежной инфраструктуры;

2) осуществлять привлечение операторов услуг платежной инфраструктуры, за исключением случая, когда оператор платежной системы совмещает функции оператора услуг платежной инфраструктуры, исходя из характера и объема операций в платежной системе, обеспечивать контроль за оказанием услуг платежной инфраструктуры участникам платежной системы, а также вести перечень операторов услуг платежной инфраструктуры;

3) организовывать систему управления рисками в платежной системе в соответствии со статьей 28 настоящего Федерального закона, осуществлять оценку и управление рисками в платежной системе;

4) обеспечивать возможность досудебного и (или) третейского рассмотрения споров с участниками платежной системы и операторами услуг платежной инфраструктуры в соответствии с правилами платежной системы.

6. Оператор платежной системы, не являющийся кредитной организацией, обязан привлечь в качестве расчетного центра кредитную организацию, которая не менее одного года осуществляет перевод денежных средств по открытым в этой кредитной организации банковским счетам.

7. Организация, намеревающаяся стать оператором платежной системы, должна направить в Банк России регистрационное заявление по форме и в порядке, которые установлены Банком России.

8. К регистрационному заявлению кредитной организации, намеревающейся стать оператором платежной системы, прилагаются следующие документы:

1) решение органа управления кредитной организации об организации платежной системы;

2) бизнес-план развития платежной системы на ближайшие два календарных года с указанием целей и планируемых результатов организации платежной системы, включая анализ рыночных и инфраструктурных факторов;

3) правила платежной системы, соответствующие требованиям настоящего Федерального закона;

4) перечень операторов услуг платежной инфраструктуры, которые будут привлекаться для оказания услуг платежной инфраструктуры в платежной системе.

9. Организация, не являющаяся кредитной организацией, намеревающаяся стать оператором платежной системы, должна соответствовать следующим требованиям:

1) обладать чистыми активами в размере не менее 10 миллионов рублей;

2) физические лица, занимающие должности единоличного исполнительного органа и главного бухгалтера такой организации, должны иметь высшее экономическое, высшее юридическое образование или высшее образование в сфере информационных и коммуникационных технологий, а при наличии иного высшего профессионального образования — опыт руководства отделом или иным подразделением кредитной организации или оператора платежной системы не менее двух лет;

3) физические лица, занимающие должности единоличного исполнительного органа и главного бухгалтера такой организации, не должны иметь судимость за преступления в сфере экономики, а также фактов расторжения трудового договора с ними по инициативе работодателя на основании, предусмотренном пунктом 7 части первой статьи 81 Трудового кодекса Российской Федерации, в течение двух лет, предшествовавших дню подачи в Банк России регистрационного заявления.

10. К регистрационному заявлению организации, не являющейся кредитной организацией, намеревающейся стать оператором платежной системы, прилагаются следующие документы:

- 1) учредительные документы;
- 2) решение уполномоченного органа такой организации об организации платежной системы;
- 3) бизнес-план развития платежной системы на ближайшие два календарных года с указанием целей и планируемых результатов организации платежной системы, включая анализ рыночных и инфраструктурных факторов;
- 4) правила платежной системы, соответствующие требованиям настоящего Федерального закона;
- 5) перечень операторов услуг платежной инфраструктуры, которые будут привлекаться для оказания услуг платежной инфраструктуры в платежной системе;
- 6) письменное согласие кредитной организации, в том числе в форме заключенного с ней договора, стать расчетным центром платежной системы с учетом требований части 6 настоящей статьи;
- 7) документы, содержащие сведения о размере чистых активов организации, с приложением форм бухгалтерской отчетности, составленной на последнюю отчетную дату, предшествующую дате представления документов в Банк России для регистрации. Указанные формы отчетности должны быть подписаны единоличным исполнительным органом организации и главным бухгалтером (их заместителями);
- 8) документы, подтверждающие соблюдение требований, предусмотренных пунктами 2 и 3 части 9 настоящей статьи.

11. В срок, не превышающий 30 календарных дней со дня получения регистрационного заявления от организации, намеревающейся стать оператором платежной системы, Банк России принимает решение о регистрации указанной организации в качестве оператора платежной системы или решение об отказе в такой регистрации.

12. В случае принятия решения о регистрации организации в качестве оператора платежной системы Банк России присваивает организации регистрационный номер, включает информацию о ней в реестр операторов платежных систем, который является общедоступным, и направляет организации регистрационное свидетельство по форме, установленной Банком России, в срок не позднее пяти рабочих дней с даты принятия указанного решения. Порядок ведения реестра операторов платежных систем устанавливается Банком России.

13. Организация, направившая в Банк России регистрационное заявление, вправе стать оператором платежной системы со дня получения регистрационного свидетельства Банка России.

14. Оператор платежной системы обязан указывать свой регистрационный номер при предоставлении информации о платежной системе.

15. Платежная система должна иметь наименование, указанное в правилах платежной системы, содержащее слова «платежная система». Ни одна организация в Российской Федерации, за исключением организации, зарегистрированной в реестре операторов платежных систем, не может использовать в своем наименовании (фирменном наименовании) слова «платежная система» или иным образом указывать на осуществление деятельности оператора платежной системы. Операторы услуг платежной инфраструктуры, участники платежной системы вправе указывать на принадлежность к платежной системе в соответствии с правилами платежной системы. Банк России вправе использовать слова «платежная система» в отношении платежной системы Банка России.

16. Оператор платежной системы, не являющийся кредитной организацией, обязан соблюдать требования, предусмотренные частью 9 настоящей статьи, в течение всего времени осуществления деятельности оператора платежной системы.

17. Банк России отказывает кредитной организации в регистрации в качестве оператора платежной системы в случае:

- 1) непредставления документов, предусмотренных частью 8 настоящей статьи;
- 2) несоответствия разработанных правил платежной системы требованиям настоящего Федерального закона.

18. Банк России отказывает организации, не являющейся кредитной организацией, в регистрации в качестве оператора платежной системы в случае:

- 1) непредставления документов, предусмотренных частью 10 настоящей статьи;
- 2) установления несоответствия организации требованиям, предусмотренным частью 9 настоящей статьи;
- 3) несоответствия разработанных правил платежной системы требованиям настоящего Федерального закона.

19. В случае отказа в регистрации в качестве оператора платежной системы Банк России в письменной форме уведомляет об этом организацию, направившую регистрационное заявление, с указанием оснований отказа и приложением представленных для регистрации документов в срок не позднее пяти рабочих дней с даты принятия решения об отказе в регистрации.

20. Организация, являющаяся оператором платежной системы, намеревающаяся стать оператором другой платежной системы, обязана направить в Банк России дополнительное регистрационное заявление по форме и в порядке, которые установлены Банком России, с указанием регистрационного номера в реестре операторов платежных систем.

21. К дополнительному регистрационному заявлению кредитной организации, являющейся оператором платежной системы, намеревающейся стать оператором другой платежной системы, прилагаются документы, предусмотренные частью 8 настоящей статьи.

22. К дополнительному регистрационному заявлению организации, не являющейся кредитной организацией, являющейся оператором платежной системы,

намеревающейся стать оператором другой платежной системы, прилагаются документы, предусмотренные пунктами 2—8 части 10 настоящей статьи.

23. Банк России принимает решение о регистрации организации, являющейся оператором платежной системы, намеревающейся стать оператором другой платежной системы, или решение об отказе в такой регистрации в срок, не превышающий 30 календарных дней со дня получения дополнительного регистрационного заявления.

24. В случае принятия решения о регистрации организации, являющейся оператором платежной системы, в качестве оператора другой платежной системы Банк России включает информацию в реестр операторов платежных систем без присвоения нового регистрационного номера и направляет организации уведомление по форме, установленной Банком России, в срок не позднее пяти рабочих дней с даты принятия соответствующего решения.

25. Организация вправе стать оператором другой платежной системы со дня получения уведомления Банка России о регистрации организации, являющейся оператором платежной системы, в качестве оператора другой платежной системы.

26. Не позднее дня, следующего за днем получения уведомления Банка России, организация обязана направить в Банк России ранее выданное регистрационное свидетельство.

27. Банк России направляет организации новое регистрационное свидетельство с указанием платежных систем, оператором которых является организация, на следующий рабочий день после дня получения от организации ранее выданного регистрационного свидетельства.

28. Банк России принимает решение об отказе в регистрации кредитной организации, являющейся оператором платежной системы, в качестве оператора другой платежной системы при непредставлении документов, предусмотренных частью 8 настоящей статьи.

29. Банк России принимает решение об отказе в регистрации организации, не являющейся кредитной организацией, являющейся оператором платежной системы, в качестве оператора другой платежной системы при непредставлении документов, предусмотренных пунктами 2—8 части 10 настоящей статьи, либо при несоответствии оператора платежной системы установленным требованиям.

30. При изменении сведений об операторе платежной системы, указанных при его регистрации, оператор платежной системы обязан уведомить Банк России по установленной им форме в течение трех рабочих дней после дня наступления таких изменений. На основании полученного уведомления оператора платежной системы Банк России в течение трех рабочих дней со дня его получения вносит соответствующие изменения в реестр операторов платежных систем.

31. Банк России вправе принимать решения об исключении сведений об организации из реестра операторов платежных систем по следующим основаниям и в следующие сроки:

1) на основании заявления оператора платежной системы с указанием им рабочего дня, в который сведения об организации исключаются из реестра операторов платежных систем, — в рабочий день, указанный в заявлении, но не ранее дня представления заявления оператора платежной системы;

2) в случаях, предусмотренных частями 8 и 9 статьи 34 настоящего Федерального закона, — в рабочий день, следующий за днем принятия решения Банком России;

3) в случае установления Банком России при осуществлении надзора факта существенного несоответствия сведениям, на основании которых осуществлялась регистрация оператора платежной системы, — в рабочий день, следующий за днем принятия решения Банком России;

4) при отзыве Банком России лицензии на осуществление банковских операций у кредитной организации, являющейся оператором платежной системы, — в рабочий день, следующий за днем отзыва лицензии Банком России;

5) в случае ликвидации оператора платежной системы как юридического лица — в рабочий день, следующий за днем, в который Банку России стало известно о ликвидации юридического лица, являющегося оператором платежной системы.

32. Исключение сведений об организации из реестра операторов платежных систем по иным основаниям, за исключением оснований, предусмотренных частью 31 настоящей статьи, не допускается.

33. При исключении сведений об организации из реестра операторов платежных систем Банк России вносит соответствующую запись в реестр операторов платежных систем и не позднее дня, следующего за днем такого исключения, направляет организации уведомление об исключении сведений о ней из реестра операторов платежных систем, за исключением случая, предусмотренного пунктом 5 части 31 настоящей статьи. Не позднее дня, следующего за днем получения уведомления Банка России, организация обязана возвратить Банку России свое регистрационное свидетельство.

34. Со дня, следующего за днем получения оператором платежной системы, не являющимся кредитной организацией, уведомления об исключении сведений из реестра операторов платежных систем, осуществление переводов денежных средств в рамках платежной системы прекращается, а переводы денежных средств, осуществление которых было начато до указанного дня, должны быть завершены центральным платежным клиринговым контрагентом и (или) расчетным центром в течение срока, установленного частью 5 статьи 5 настоящего Федерального закона. В отношении значимых платежных систем срок прекращения осуществления и завершения переводов денежных средств может быть увеличен Банком России, но не более чем до одного месяца.

35. Порядок завершения переводов денежных средств центральным платежным клиринговым контрагентом и (или) расчетным центром в случае отзыва у них лицензий на осуществление банковских операций определяется федеральным законом.

36. Оператор платежной системы обязан представлять в Банк России изменения правил платежной системы, изменения перечня операторов услуг платежной инфраструктуры не позднее 10 дней со дня внесения соответствующих изменений.

37. Операторы платежных систем могут заключить договор о взаимодействии своих платежных систем при условии отражения порядка такого взаимодействия в правилах платежных систем.

38. Деятельность оператора платежной системы, в рамках которой осуществляется перевод денежных средств между операторами по переводу денежных средств, находящимися на территории Российской Федерации, может осуществляться только организацией, созданной в соответствии с законодательством Российской Федерации и соответствующей требованиям настоящего Федерального закона.

39. Оператор по переводу денежных средств, за исключением Банка России, у которого открыты банковские счета не менее трех других операторов по переводу денежных средств и между этими счетами осуществляются переводы денежных средств в течение трех месяцев подряд в размере, превышающем значение, установленное Банком России, обязан обеспечить в соответствии с требованиями настоящей статьи направление в Банк России заявления о регистрации оператора платежной системы в течение 30 дней после дня начала соответствия указанному требованию. По истечении четырех месяцев после дня начала соответствия указанному требованию осуществление перевода денежных средств между банковскими счетами операторов по переводу денежных средств, открытыми у такого оператора по переводу денежных средств, допускается только в рамках платежной системы. Требования настоящей части не распространяются на операторов по переводу денежных средств, являющихся расчетными центрами платежных систем, операторы платежных систем которых зарегистрированы Банком России, в части переводов денежных средств, осуществляемых в рамках указанных платежных систем.

40. Банк России направляет организации, осуществляющей деятельность оператора платежной системы и не направившей в Банк России регистрационное заявление в соответствии с настоящей статьей, требование о регистрации такой организации в качестве оператора платежной системы. Указанная организация обязана направить в Банк России регистрационное заявление не позднее 30 календарных дней со дня получения такого требования либо прекратить осуществление деятельности оператора платежной системы.

Статья 16 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа).

Статья 16. Оператор услуг платежной инфраструктуры и требования к его деятельности

1. Оператором услуг платежной инфраструктуры может являться кредитная организация, организация, не являющаяся кредитной организацией, Банк России или Внешэкономбанк.

2. Оператор услуг платежной инфраструктуры, являющийся кредитной организацией, Банком России или Внешэкономбанком, может совмещать оказание операционных услуг, услуг платежного клиринга и расчетных услуг, в том числе в рамках одной организации.

3. Оператор услуг платежной инфраструктуры, не являющийся кредитной организацией, Банком России или Внешэкономбанком, может совмещать оказание операционных услуг, услуг платежного клиринга, в том числе в рамках одной организации.

4. Оператор услуг платежной инфраструктуры, являющийся кредитной организацией, Банком России или Внешэкономбанком, может совмещать свою деятельность с деятельностью оператора по переводу денежных средств, оператора платежной системы и иной деятельностью, если это не противоречит законодательству Российской Федерации.

5. Оператор услуг платежной инфраструктуры, не являющийся кредитной организацией, может совмещать свою деятельность с деятельностью оператора платежной системы и иной деятельностью, если это не противоречит законодательству Российской Федерации.

6. Банк России осуществляет деятельность оператора услуг платежной инфраструктуры на основании настоящего Федерального закона в соответствии с нормативными актами Банка России и заключаемыми договорами.

7. Оператор услуг платежной инфраструктуры осуществляет свою деятельность в соответствии с правилами платежной системы и договорами, заключаемыми с участниками платежной системы и другими операторами услуг платежной инфраструктуры.

8. Правилами платежной системы должны определяться требования к операторам услуг платежной инфраструктуры, с которыми могут заключаться договоры в соответствии с настоящим Федеральным законом.

9. В отношении операторов услуг платежной инфраструктуры должны быть определены требования к их финансовому состоянию, технологическому обеспечению и другим факторам, влияющим на бесперебойность функционирования платежной системы, которые должны быть объективными, доступными для публичного ознакомления и обеспечивать равноправный доступ операторов услуг платежной инфраструктуры в платежную систему.

10. Операторы услуг платежной инфраструктуры обязаны предоставлять оператору платежной системы информацию о своей деятельности (в части оказания услуг платежной инфраструктуры) в соответствии с правилами платежной системы.

Положения части 11 статьи 16 в части привлечения операционного центра и (или) платежного клирингового центра применяются по истечении трех лет после дня официального опубликования настоящего Федерального закона (часть 7 статьи 38 данного документа).

11. При осуществлении перевода денежных средств в рамках платежной системы операторами по переводу денежных средств, находящимися на террито-

рии Российской Федерации, должны привлекаться операторы услуг платежной инфраструктуры, которые соответствуют требованиям настоящего Федерального закона и находятся на территории Российской Федерации, за исключением случая, предусмотренного частью 8 статьи 17 настоящего Федерального закона.

Статья 17. Требования к деятельности операционного центра

Часть 1 статьи 17 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа).

1. Операционный центр осуществляет свою деятельность в соответствии с правилами платежной системы и на основании договоров об оказании операционных услуг с оператором платежной системы, участниками платежной системы, платежным клиринговым центром и расчетным центром, если заключение таких договоров предусмотрено правилами платежной системы.

Часть 2 статьи 17 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа).

2. В платежной системе может быть несколько операционных центров.

Часть 3 статьи 17 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа).

3. Операционный центр обеспечивает обмен электронными сообщениями между участниками платежной системы, между участниками платежной системы и их клиентами, платежным клиринговым центром, расчетным центром, между платежным клиринговым центром и расчетным центром.

Часть 4 статьи 17 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа).

4. Операционный центр может осуществлять иные действия, связанные с использованием информационно-коммуникационных технологий, необходимые для функционирования платежной системы и предусмотренные правилами платежной системы.

Часть 5 статьи 17 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа).

5. Операционный центр несет ответственность за реальный ущерб, причиненный участникам платежной системы, платежному клиринговому центру и расчетному центру вследствие неоказания (ненадлежащего оказания) операционных услуг.

Часть 6 статьи 17 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа).

6. Правилами платежной системы и договором об оказании операционных услуг ответственность операционного центра за реальный ущерб может быть ограничена размером неустойки, за исключением случаев умышленного неоказания (ненадлежащего оказания) операционных услуг.

Часть 7 статьи 17 данного документа вступает в силу по истечении одного года после дня официального опубликования (пункт 3 статьи 39 данного документа).

7. В случае, если правилами платежной системы и договором об оказании операционных услуг предусмотрена обязанность операционного центра обеспе-

чить гарантированный уровень бесперебойности оказания операционных услуг в течение определенного времени, могут быть установлены ответственность операционного центра за реальный ущерб и неустойка.

8. Оператор платежной системы в случаях и порядке, предусмотренных правилами платежной системы, вправе привлекать операционный центр, находящийся за пределами Российской Федерации, для оказания операционных услуг участникам платежной системы. В указанном случае оператор платежной системы несет ответственность за надлежащее оказание операционных услуг участникам платежной системы.

Статья 18 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа)

Статья 18. Требования к деятельности платежного клирингового центра

1. Платежный клиринговый центр осуществляет свою деятельность в соответствии с правилами платежной системы и на основании договоров об оказании услуг платежного клиринга, заключаемых с участниками платежной системы, операционным центром и расчетным центром, если заключение таких договоров предусмотрено правилами платежной системы.

2. В платежных системах, в рамках которых осуществляются переводы денежных средств по сделкам, совершенным на организованных торгах, услуги платежного клиринга могут оказываться в рамках клиринговой услуги клиринговой организацией, осуществляющей свою деятельность в соответствии с Федеральным законом от 7 февраля 2011 года № 7-ФЗ «О клиринге и клиринговой деятельности».

3. В платежной системе может быть несколько платежных клиринговых центров.

4. Договор об оказании услуг платежного клиринга, заключаемый с участниками платежной системы, является договором присоединения.

5. В соответствии с договором об оказании услуг платежного клиринга, заключаемым с расчетным центром, платежный клиринговый центр обязуется передавать расчетному центру от имени участников платежной системы подлежащие исполнению распоряжения участников платежной системы.

6. Платежный клиринговый центр несет ответственность за убытки, причиненные участникам платежной системы и расчетному центру вследствие неоказания (ненадлежащего оказания) услуг платежного клиринга.

7. Правилами платежной системы и договором об оказании услуг платежного клиринга ответственность платежного клирингового центра за убытки может быть ограничена размером неустойки, за исключением случаев умышленного не оказания (ненадлежащего оказания) услуг платежного клиринга.

8. Центральным платежным клиринговым контрагентом может выступать кредитная организация, Банк России или Внешэкономбанк в порядке, предусмотренном правилами платежной системы и договорами об оказании услуг платежного клиринга.

9. Центральный платежный клиринговый контрагент обязан:

1) обладать денежными средствами, достаточными для исполнения своих обязательств, либо обеспечивать исполнение своих обязательств, в том числе за счет гарантийного фонда, в размере наибольшего обязательства, по которому центральный платежный клиринговый контрагент становится плательщиком, за период, определяемый правилами платежной системы;

2) ежедневно осуществлять контроль за рисками неисполнения (ненадлежащего исполнения) участниками платежной системы своих обязательств по переводу денежных средств, применять в отношении участников платежной системы, анализ финансового состояния которых свидетельствует о повышенном риске, ограничительные меры, включая установление максимального размера платежной клиринговой позиции, и предъявлять требования о повышенном размере обеспечения исполнения обязательств участников платежной системы по переводу денежных средств.

Статья 19 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа)

Статья 19. Требования к деятельности расчетного центра

1. Расчетным центром может выступать кредитная организация, Банк России или Внешэкономбанк.

2. В платежной системе может быть несколько расчетных центров.

3. Расчетный центр осуществляет свою деятельность в соответствии с правилами платежной системы и на основании договоров банковского счета, заключаемых с участниками платежной системы и (или) центральным платежным клиринговым контрагентом (при его наличии), а также договоров, заключаемых с операционным центром и платежным клиринговым центром, если заключение таких договоров предусмотрено правилами платежной системы.

4. Расчетный центр исполняет поступившие от платежного клирингового центра распоряжения участников платежной системы посредством списания и зачисления денежных средств по банковским счетам участников платежной системы и (или) банковскому счету центрального платежного клирингового контрагента (при его наличии).

5. Расчетный центр платежной системы в случае, предусмотренном частью 2 статьи 18 настоящего Федерального закона, может исполнять распоряжения участников платежной системы, поступившие от клиринговой организации, осуществляющей свою деятельность в соответствии с Федеральным законом от 7 февраля 2011 года № 7-ФЗ «О клиринге и клиринговой деятельности».

Глава 4. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЮ ПЛАТЕЖНЫХ СИСТЕМ

Статья 20 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа)

Статья 20. Правила платежной системы

1. Правилами платежной системы должны определяться:

- 1) порядок взаимодействия между оператором платежной системы, участниками платежной системы и операторами услуг платежной инфраструктуры;
- 2) порядок осуществления контроля за соблюдением правил платежной системы;
- 3) ответственность за несоблюдение правил платежной системы;
- 4) критерии участия, приостановления и прекращения участия в платежной системе;
- 5) порядок привлечения операторов услуг платежной инфраструктуры и ведения перечня операторов услуг платежной инфраструктуры;
- 6) применяемые формы безналичных расчетов;
- 7) порядок осуществления перевода денежных средств в рамках платежной системы, включая моменты наступления его безотзывности, безусловности и окончательности;
- 8) порядок сопровождения перевода денежных средств сведениями о платежнике в соответствии с требованиями Федерального закона от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» в случае, если они не содержатся в распоряжении участника платежной системы;
- 9) порядок оплаты услуг по переводу денежных средств, являющийся единообразным в рамках платежной системы;
- 10) порядок осуществления платежного клиринга и расчета;
- 11) порядок оплаты услуг платежной инфраструктуры, являющийся единообразным в рамках платежной системы;
- 12) порядок предоставления участниками платежной системы и операторами услуг платежной инфраструктуры информации о своей деятельности оператору платежной системы;
- 13) система управления рисками в платежной системе, включая используемую модель управления рисками, перечень мероприятий и способов управления рисками;
- 14) порядок обеспечения бесперебойности функционирования платежной системы;
- 15) временной регламент функционирования платежной системы;
- 16) порядок присвоения кода (номера), позволяющего однозначно установить участника платежной системы и вид его участия в платежной системе;
- 17) порядок обеспечения исполнения обязательств участников платежной системы по переводу денежных средств;
- 18) порядок взаимодействия в рамках платежной системы в спорных и чрезвычайных ситуациях, включая информирование операторами услуг платежной инфраструктуры, участниками значимой платежной системы оператора значимой платежной системы о событиях, вызвавших операционные сбои, об их причинах и последствиях;

- 19) требования к защите информации;
- 20) перечень платежных систем, с которыми осуществляется взаимодействие, и порядок такого взаимодействия;
- 21) порядок изменения правил платежной системы;
- 22) порядок досудебного разрешения споров с участниками платежной системы и операторами услуг платежной инфраструктуры.

2. Правилами платежной системы могут быть предусмотрены другие положения, необходимые для обеспечения функционирования платежной системы.

3. Правила платежной системы, за исключением правил платежной системы Банка России, являются договором. Правила платежной системы могут быть составлены в виде единого документа или нескольких взаимосвязанных документов.

4. В правилах платежной системы запрещается установление:

1) требований, препятствующих участию в платежной системе, не соответствующих требованиям части 10 статьи 21 настоящего Федерального закона;

2) требований к участникам платежной системы о неучастии в других платежных системах (условие об исключительном участии);

3) требований к участникам платежной системы об ограничении (запрете) осуществления между ними клиринга и расчета вне рамок платежной системы на основании договоров, заключаемых между участниками платежной системы, под ответственность таких участников;

4) требований к операторам услуг платежной инфраструктуры об ограничении (запрете) оказания услуг платежной инфраструктуры в рамках других платежных систем (условие об исключительном оказании услуг платежной инфраструктуры);

5) минимального размера оплаты услуг по переводу денежных средств участниками платежной системы и их клиентами.

5. Оператор платежной системы обязан предоставлять организациям, намеревающимся участвовать в платежной системе, правила платежной системы для предварительного ознакомления без взимания платы, за исключением расходов на изготовление копий правил платежной системы.

6. Правила платежной системы, включая тарифы, являются публично доступными. Оператор платежной системы вправе не раскрывать информацию о требованиях к защите информации и информацию, доступ к которой ограничен в соответствии с федеральным законом.

7. Участники платежной системы присоединяются к правилам платежной системы только путем принятия их в целом.

8. Оператор платежной системы может в одностороннем порядке вносить изменения в правила платежной системы при условии:

1) обеспечения участникам платежной системы возможности предварительного ознакомления с предлагаемыми изменениями и направления своего мнения оператору платежной системы в установленный им срок, который не может быть менее одного месяца;

2) установления срока внесения изменений не менее одного месяца со дня окончания срока, указанного в пункте 1 настоящей части.

9. Правила платежной системы Банка России определяются нормативными актами Банка России на основании настоящего Федерального закона.

10. Особенности правил платежных систем, в рамках которых осуществляются переводы денежных средств по сделкам, совершенным на организованных торгах, устанавливаются Банком России по согласованию с уполномоченным федеральным органом исполнительной власти.

Статья 21 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа)

Статья 21. Участники платежной системы

1. Участниками платежной системы могут стать следующие организации при условии их присоединения к правилам платежной системы в порядке, установленном правилами платежной системы:

1) операторы по переводу денежных средств (включая операторов электронных денежных средств);

2) профессиональные участники рынка ценных бумаг, а также юридические лица, являющиеся участниками организованных торгов и (или) участниками клиринга в соответствии с Федеральным законом от 7 февраля 2011 года № 7-ФЗ «О клиринге и клиринговой деятельности»;

3) страховые организации, осуществляющие обязательное страхование гражданской ответственности в соответствии с законодательством Российской Федерации;

4) органы Федерального казначейства;

5) организации федеральной почтовой связи.

2. В случае заключения между операторами платежных систем договора о взаимодействии платежных систем участниками платежной системы могут являться центральный платежный клиринговый контрагент и (или) расчетный центр другой платежной системы, действующие по поручению оператора такой платежной системы.

3. Участниками платежной системы могут являться международные финансовые организации, иностранные центральные (национальные) банки, иностранные банки.

4. Правилами платежной системы должно быть предусмотрено прямое участие в платежной системе и может быть предусмотрено косвенное участие в платежной системе.

5. Правилами платежной системы могут быть предусмотрены различные виды прямого и косвенного участия в платежной системе.

6. Прямое участие в платежной системе требует открытия в расчетном центре банковского счета организации, становящейся прямым участником, в целях осуществления расчета с другими участниками платежной системы.

7. Прямыми участниками платежной системы могут являться только операторы по переводу денежных средств, включая операторов электронных денеж-

ных средств, профессиональные участники рынка ценных бумаг, юридические лица, являющиеся участниками организованных торгов и (или) участниками клиринга в соответствии с Федеральным законом от 7 февраля 2011 года № 7-ФЗ «О клиринге и клиринговой деятельности» (при осуществлении ими переводов денежных средств по сделкам, совершенным на организованных торгах), страховые организации, осуществляющие обязательное страхование гражданской ответственности в соответствии с законодательством Российской Федерации (при осуществлении ими расчетов по обязательным видам страхования гражданской ответственности, предусмотренным законодательством Российской Федерации), и органы Федерального казначейства.

8. Косвенное участие в платежной системе требует открытия банковского счета косвенному участнику — организации, предусмотренной частью 1 настоящей статьи, прямым участником платежной системы, являющимся оператором по переводу денежных средств, в целях осуществления расчета с другими участниками платежной системы.

9. Отношения между прямыми и косвенными участниками платежной системы регулируются правилами платежной системы и заключенными договорами банковского счета.

10. Для каждого вида участия в платежной системе правилами такой платежной системы устанавливаются отдельные критерии участия, которые должны включать доступные для публичного ознакомления требования, обеспечивающие равноправный доступ участников платежной системы одного вида в платежную систему. Указанные требования могут касаться финансового состояния, технологического обеспечения и других факторов, влияющих на бесперебойность функционирования платежной системы.

11. Операторы по переводу денежных средств, за исключением Банка России, могут участвовать в платежных системах в целях осуществления трансграничного перевода денежных средств при условии уведомления об этом Банка России не позднее 10 календарных дней со дня начала участия в платежной системе в порядке, установленном Банком России.

12. Операторы по переводу денежных средств не могут участвовать в платежной системе, в рамках которой осуществляется перевод денежных средств на территории Российской Федерации, при наличии одного из следующих условий:

1) отсутствия на территории Российской Федерации юридического лица, выполняющего функции оператора платежной системы, соответствующего требованиям настоящего Федерального закона;

2) отсутствия правил платежной системы, соответствующих требованиям настоящего Федерального закона;

Положения пункта 3 части 12 статьи 21 в части привлечения операционного центра и (или) платежного клирингового центра применяются по истечении трех лет после дня официального опубликования настоящего Федерального закона (часть 7 статьи 38 данного документа).

- 3) нарушения требований части 11 статьи 16 настоящего Федерального закона;
- 4) нарушения требований части 10 статьи 29 настоящего Федерального закона.

Статья 22 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа)

Статья 22. Признание платежной системы значимой

1. Платежная система является системно значимой в случае ее соответствия хотя бы одному из следующих критериев:

1) осуществления в рамках платежной системы в течение трех календарных месяцев подряд переводов денежных средств с общим объемом на сумму и отдельными переводами денежных средств на сумму не менее значений, установленных Банком России;

2) осуществления в рамках платежной системы Банком России переводов денежных средств при рефинансировании кредитных организаций и осуществлении операций на открытом рынке;

3) осуществления в рамках платежной системы переводов денежных средств по сделкам, совершенным на организованных торгах.

2. Платежная система является социально значимой в случае ее соответствия хотя бы одному из следующих критериев:

1) осуществления в рамках платежной системы в течение трех календарных месяцев подряд переводов денежных средств с общим объемом на сумму не менее значений, установленных Банком России, и более половины этих переводов денежных средств на сумму не более значения, установленного Банком России;

2) осуществления в течение календарного года в рамках платежной системы переводов денежных средств с использованием платежных карт в количестве не менее значения, установленного Банком России;

3) осуществления в течение календарного года в рамках платежной системы переводов денежных средств без открытия банковского счета в количестве не менее значения, установленного Банком России;

4) осуществления в течение календарного года в рамках платежной системы переводов денежных средств клиентов — физических лиц по их банковским счетам (за исключением переводов денежных средств с использованием платежных карт) в количестве не менее значения, установленного Банком России.

3. Признание платежной системы значимой осуществляется Банком России на основании информации, подтверждающей соответствие платежной системы установленным критериям значимости:

1) при регистрации Банком России оператора платежной системы;

2) при осуществлении Банком России надзора и наблюдения в национальной платежной системе;

3) на основании письменного заявления оператора платежной системы с приложением документов, подтверждающих соответствие платежной системы установленным критериям значимости.

4. При принятии решения о признании платежной системы значимой Банк России в течение семи календарных дней:

1) включает информацию о признании платежной системы значимой в реестр операторов платежных систем;

2) в письменной форме уведомляет оператора платежной системы о признании платежной системы значимой.

5. Банк России публикует информацию о включении платежной системы в перечень значимых платежных систем в официальном издании Банка России «Вестник Банка России».

6. Платежная система признается значимой со дня включения информации о признании ее значимой в реестр операторов платежных систем.

7. Оператор значимой платежной системы обязан:

1) в течение 90 календарных дней со дня получения уведомления Банка России о признании платежной системы значимой обеспечить соблюдение требований, предъявляемых Банком России в соответствии со статьей 24 настоящего Федерального закона;

2) в течение 120 календарных дней со дня получения уведомления Банка России о признании платежной системы значимой внести необходимые изменения в правила платежной системы в целях соблюдения требований статьи 24 настоящего Федерального закона и направить измененные правила платежной системы в Банк России либо не позднее семи календарных дней уведомить Банк России о соответствии правил платежной системы, представленных Банку России при регистрации оператора платежной системы, требованиям статьи 24 настоящего Федерального закона.

8. Банк России осуществляет анализ соответствия значимой платежной системы установленным критериям значимости. В случае, если ранее признанная значимой платежная система не соответствует в течение шести календарных месяцев ни одному из установленных критериев значимости, Банк России выносит решение о признании такой платежной системы утратившей системную или социальную значимость.

9. После принятия решения о признании платежной системы утратившей системную или социальную значимость Банк России в течение семи календарных дней:

1) включает информацию о признании платежной системы утратившей системную или социальную значимость в реестр операторов платежных систем;

2) в письменной форме уведомляет оператора платежной системы о признании платежной системы утратившей системную или социальную значимость.

10. Банк России публикует информацию о признании платежной системы утратившей системную или социальную значимость в официальном издании Банка России «Вестник Банка России».

11. Платежная система Банка России признается системно значимой платежной системой.

12. Банк России обязан обеспечить соблюдение платежной системой Банка России требований к системно значимым платежным системам, предусмотренных статьями 24 настоящего Федерального закона.

Статья 23 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа)

Статья 23. Порядок проверки Банком России соответствия правил значимой платежной системы установленным требованиям

1. Проверка соответствия правил значимой платежной системы требованиям, установленным настоящим Федеральным законом и принятыми в соответствии с ним нормативными актами Банка России (далее — проверка соответствия), осуществляется Банком России после признания платежной системы значимой.

2. Оператор значимой платежной системы в срок, указанный в пункте 2 части 7 статьи 22 настоящего Федерального закона, представляет в Банк России для проверки соответствия правила платежной системы в двух экземплярах либо сообщает Банку России о возможности проверки соответствия правил платежной системы, представленных Банку России при регистрации оператора платежной системы.

3. Проверка соответствия правил значимой платежной системы осуществляется Банком России в срок, не превышающий 90 календарных дней со дня представления правил значимой платежной системы для проверки соответствия правил платежной системы или со дня сообщения Банку России о возможности проверки соответствия правил платежной системы, представленных Банку России при регистрации оператора платежной системы.

4. При соответствии правил платежной системы требованиям настоящего Федерального закона и принятых в соответствии с ним нормативных актов Банка России Банк России проставляет на правилах платежной системы отметку о соответствии и направляет один экземпляр правил значимой платежной системы оператору значимой платежной системы.

5. При несоответствии правил платежной системы требованиям настоящего Федерального закона и принятых в соответствии с ним нормативных актов Банка России Банк России в письменной форме уведомляет оператора платежной системы о таком несоответствии. В уведомлении указываются требования, которым не соответствуют представленные Банку России правила платежной системы, а также срок, который не может быть более 90 дней, для их изменения и повторного представления Банку России для проверки соответствия.

6. При внесении изменений в правила значимой платежной системы, в том числе по требованию Банка России, предъявленному при осуществлении Банком России надзора в национальной платежной системе, оператор значимой платежной системы обязан представить изменения указанных правил в Банк России для проверки соответствия не позднее 10 дней после внесения указанных изменений.

Статья 24 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа)

Статья 24. Требования к значимой платежной системе

1. Банк России устанавливает следующие требования к системно значимой платежной системе:

1) осуществление оператором платежной системы, и (или) платежным клиринговым центром, и (или) расчетным центром мониторинга и анализа рисков в режиме реального времени;

2) осуществление расчета в платежной системе в режиме реального времени или в течение одного дня;

3) осуществление расчета через расчетный центр, соответствующий требованиям финансовой устойчивости и управления рисками, установленным Банком России;

4) обеспечение гарантированного уровня бесперебойности оказания операционных услуг;

5) соответствие системы управления рисками значимой платежной системы требованиям, установленным частью 8 статьи 28 настоящего Федерального закона.

2. Банк России устанавливает следующие требования к социально значимой платежной системе:

1) осуществление оператором платежной системы, и (или) платежным клиринговым центром, и (или) расчетным центром мониторинга и анализа рисков на постоянной основе;

2) осуществление расчета через расчетный центр, являющийся банком — участником системы обязательного страхования вкладов физических лиц в банках Российской Федерации, соответствующий требованиям управления рисками, установленным Банком России, или через небанковскую кредитную организацию, осуществляющую расчет по счетам других кредитных организаций не менее трех лет;

3) соответствие требованиям, предусмотренным пунктами 4 и 5 части 1 настоящей статьи.

3. Требования Банка России к значимой платежной системе применяются по истечении 90 календарных дней со дня получения оператором платежной системы уведомления Банка России о признании платежной системы значимой.

4. При утрате платежной системой значимости установленные Банком России требования к значимой платежной системе могут не соблюдаться со дня получения оператором платежной системы уведомления Банка России о признании платежной системы утратившей системную или социальную значимость.

Статья 25 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа)

Статья 25. Осуществление платежного клиринга и расчета в платежной системе

1. Платежный клиринг в платежной системе осуществляется платежным клиринговым центром посредством:

1) выполнения процедур приема к исполнению распоряжений участников платежной системы, включая проверку соответствия распоряжений участников платежной системы установленным требованиям, определение достаточности денежных средств для исполнения распоряжений участников платежной системы и определение платежных клиринговых позиций;

2) передачи расчетному центру для исполнения принятых распоряжений участников платежной системы;

3) направления участникам платежной системы извещений (подтверждений), касающихся приема к исполнению распоряжений участников платежной системы, а также передачи извещений (подтверждений), касающихся исполнения распоряжений участников платежной системы.

2. Процедуры приема к исполнению распоряжений участников платежной системы выполняются платежным клиринговым центром в соответствии с правилами платежной системы.

3. Определение платежной клиринговой позиции участника платежной системы может осуществляться на валовой основе и (или) на нетто-основе.

4. Платежная клиринговая позиция на валовой основе определяется в размере суммы индивидуального распоряжения участника платежной системы или общей суммы распоряжений участников платежной системы, по которым участник платежной системы является плательщиком или получателем средств.

5. После определения платежной клиринговой позиции на валовой основе распоряжения участников платежной системы передаются платежным клиринговым центром расчетному центру для исполнения.

6. Платежная клиринговая позиция на нетто-основе определяется в размере разницы между общей суммой подлежащих исполнению распоряжений участников платежной системы, по которым участник платежной системы является плательщиком, и общей суммой распоряжений участников платежной системы, по которым участник платежной системы является получателем средств.

7. После определения платежной клиринговой позиции на нетто-основе платежный клиринговый центр передает расчетному центру для исполнения распоряжения платежного клирингового центра на сумму определенных платежных клиринговых позиций на нетто-основе участников платежной системы и (или) принятые распоряжения участников платежной системы.

8. Расчет в платежной системе осуществляется расчетным центром посредством списания и зачисления денежных средств по банковским счетам участников платежной системы и (или) центрального платежного клирингового контрагента на основании поступивших от платежного клирингового центра распоряжений в размере сумм определенных платежных клиринговых позиций.

9. При заключении между операторами платежных систем договора о взаимодействии между платежными системами платежный клиринг и расчет в целях перевода денежных средств между участниками одной платежной системы осуществляются соответственно платежным клиринговым центром и расчетным

центром этой платежной системы, если иное не предусмотрено договором о взаимодействии между платежными системами. Платежный клиринг и расчет в целях перевода денежных средств между участниками различных платежных систем осуществляются в порядке, предусмотренном договором о взаимодействии между платежными системами.

Статья 26. Обеспечение банковской тайны в платежной системе

Операторы по переводу денежных средств, операторы платежных систем, операторы услуг платежной инфраструктуры и банковские платежные агенты (субагенты) обязаны гарантировать банковскую тайну в соответствии с законодательством Российской Федерации о банках и банковской деятельности.

Статья 27 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа).

Статья 27. Обеспечение защиты информации в платежной системе

1. Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обязаны обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации. Правительство Российской Федерации устанавливает требования к защите указанной информации.

2. Контроль и надзор за выполнением требований, установленных Правительством Российской Федерации, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с защищаемой информацией.

3. Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обязаны обеспечивать защиту информации при осуществлении переводов денежных средств в соответствии с требованиями, установленными Банком России, согласованными с федеральными органами исполнительной власти, предусмотренными частью 2 настоящей статьи. Контроль за соблюдением установленных требований осуществляется Банком России в рамках надзора в национальной платежной системе в установленном им порядке, согласованном с федеральными органами исполнительной власти, предусмотренными частью 2 настоящей статьи.

Статья 28 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа).

Статья 28. Система управления рисками в платежной системе

1. В целях настоящего Федерального закона под системой управления рисками в платежной системе понимается комплекс мероприятий и способов снижения вероятности возникновения неблагоприятных последствий для бесперебой-

ности функционирования платежной системы с учетом размера причиняемого ущерба.

2. Оператор платежной системы обязан определить одну из следующих используемых в платежной системе организационных моделей управления рисками в платежной системе:

1) самостоятельное управление рисками в платежной системе оператором платежной системы;

2) распределение функций по оценке и управлению рисками между оператором платежной системы, операторами услуг платежной инфраструктуры и участниками платежной системы;

3) передача функций по оценке и управлению рисками оператором платежной системы, не являющимся кредитной организацией, расчетному центру.

3. Система управления рисками должна предусматривать следующие мероприятия:

1) определение организационной структуры управления рисками, обеспечивающей контроль за выполнением участниками платежной системы требований к управлению рисками, установленных правилами платежной системы;

2) определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений;

3) доведение до органов управления оператора платежной системы соответствующей информации о рисках;

4) определение показателей бесперебойности функционирования платежной системы в соответствии с требованиями нормативных актов Банка России;

5) определение порядка обеспечения бесперебойности функционирования платежной системы в соответствии с требованиями нормативных актов Банка России;

6) определение методик анализа рисков в платежной системе, включая профили рисков, в соответствии с требованиями нормативных актов Банка России;

7) определение порядка обмена информацией, необходимой для управления рисками;

8) определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев;

9) определение порядка изменения операционных и технологических средств и процедур;

10) определение порядка оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией;

11) определение порядка обеспечения защиты информации в платежной системе.

4. Способы управления рисками в платежной системе определяются оператором платежной системы с учетом особенностей организации платежной системы, модели управления рисками, процедур платежного клиринга и расчета, количества переводов денежных средств и их сумм, времени окончательного расчета.

5. Система управления рисками может предусматривать следующие способы управления рисками:

- 1) установление предельных размеров (лимитов) обязательств участников платежной системы с учетом уровня риска;
- 2) создание гарантийного фонда платежной системы;
- 3) управление очередностью исполнения распоряжений участников платежной системы;
- 4) осуществление расчета в платежной системе до конца рабочего дня;
- 5) осуществление расчета в пределах предоставленных участниками платежной системы денежных средств;
- 6) обеспечение возможности предоставления кредита;
- 7) использование безотзывных банковской гарантии или аккредитива;
- 8) другие способы управления рисками, предусмотренные правилами платежной системы.

6. Правилами платежной системы может быть предусмотрено создание оператором платежной системы коллегиального органа по управлению рисками в платежной системе, в состав которого включаются ответственные за управление рисками представители оператора платежной системы, операторов услуг платежной инфраструктуры, участников платежной системы. В состав органа по управлению рисками по согласованию с Банком России могут быть включены представители Банка России с правом совещательного голоса.

7. В функциональные обязанности и компетенцию органа управления рисками входят:

- 1) установление критериев оценки системы управления рисками, включая системный риск, и проведение указанной оценки;
- 2) формирование предложений и рекомендаций по итогам проведения оценки системы управления рисками.

8. Система управления рисками значимой платежной системы должна предусматривать создание органа управления рисками значимой платежной системы, указанного в части 6 настоящей статьи, и использование не менее двух способов управления рисками, указанных в пунктах 1 — 7 части 5 настоящей статьи.

Статья 29 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа).

Статья 29. Обеспечение исполнения обязательств участников платежной системы

1. Порядок обеспечения исполнения обязательств участников платежной системы устанавливается правилами платежной системы.

2. При осуществлении расчета на нетто-основе в значимой платежной системе должно обеспечиваться исполнение наибольшего по размеру обязательства участника значимой платежной системы.

3. Правилами платежной системы может быть предусмотрено создание оператором платежной системы либо по его поручению центральным платежным клиринго-

вым контрагентом или расчетным центром гарантийного фонда платежной системы за счет денежных средств (гарантийных взносов) участников платежной системы. Правилами платежной системы может быть предусмотрено внесение в гарантийный фонд платежной системы денежных средств оператора платежной системы, центрального платежного клирингового контрагента и (или) расчетного центра.

4. Порядок определения размера гарантийного взноса устанавливается правилами платежной системы.

5. Гарантийный фонд платежной системы используется оператором платежной системы либо по его поручению центральным платежным клиринговым контрагентом или расчетным центром в целях обеспечения исполнения обязательств участников платежной системы.

6. В случае неисполнения (ненадлежащего исполнения) обязательств участником платежной системы его гарантийный взнос используется для удовлетворения требований по таким обязательствам.

7. При недостаточности гарантийного взноса участника платежной системы используются гарантийные взносы других участников платежной системы в порядке, предусмотренном правилами платежной системы. В этом случае указанный участник платежной системы обязан возместить сумму использованных гарантийных взносов, а также уплатить проценты за их использование, если это предусмотрено правилами платежной системы.

8. В случае прекращения участия в платежной системе участнику платежной системы возвращается его гарантийный взнос в порядке и сроки, которые предусмотрены правилами платежной системы.

9. Гарантийный фонд платежной системы учитывается на отдельном банковском счете, открываемом оператору платежной системы, центральному платежному клиринговому контрагенту или участникам платежной системы (далее — счет гарантийного фонда платежной системы) в соответствии со статьей 30 настоящего Федерального закона.

10. Счет гарантийного фонда платежной системы может быть открыт только в Банке России, Внешэкономбанке, а также в банке — участнике системы страхования вкладов или небанковской кредитной организации, не имеющей права осуществлять размещение привлеченных во вклады денежных средств.

Статья 30 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа).

Статья 30. Счет гарантийного фонда платежной системы

1. При открытии счета гарантийного фонда платежной системы оператору платежной системы операции по указанному счету осуществляются на основании распоряжений оператора платежной системы.

2. При открытии счета гарантийного фонда платежной системы центральному платежному клиринговому контрагенту операции по указанному счету осуществляются либо на основании распоряжений оператора платежной системы без распоряжения центрального платежного клирингового контрагента, либо на

основании распоряжений центрального платежного клирингового контрагента с согласия оператора платежной системы.

3. При открытии счета гарантийного фонда платежной системы участнику платежной системы операции по указанному счету осуществляются либо на основании распоряжений оператора платежной системы или центрального платежного клирингового контрагента без распоряжения участника платежной системы, которому открыт данный счет, либо на основании распоряжений участника платежной системы, которому открыт такой счет, с согласия оператора платежной системы или центрального платежного клирингового контрагента.

4. При открытии счета гарантийного фонда платежной системы центральному платежному клиринговому контрагенту или участнику платежной системы соответственно оператор платежной системы или оператор платежной системы и центральный платежный клиринговый контрагент имеют право получать от оператора по переводу денежных средств, у которого открыт счет гарантийного фонда платежной системы, информацию об операциях по этому счету.

5. При открытии счета гарантийного фонда платежной системы центральному платежному клиринговому контрагенту или участнику платежной системы указывается лицо, которое вправе давать распоряжения по этому счету в соответствии с требованиями частей 2 и 3 настоящей статьи.

6. Согласие оператора платежной системы или центрального платежного клирингового контрагента на совершение операций по счету гарантийного фонда платежной системы дается способом, предусмотренным договором банковского счета в соответствии с правилами платежной системы.

7. Оператор платежной системы, центральный платежный клиринговый контрагент, участник платежной системы вправе переводить на счет гарантийного фонда платежной системы собственные денежные средства в случаях, предусмотренных частями 3 и 7 статьи 29 настоящего Федерального закона.

8. В случае признания оператора платежной системы, центрального платежного клирингового контрагента, участника платежной системы банкротом денежные средства, находящиеся на счете гарантийного фонда платежной системы, в конкурсную массу не включаются и подлежат возврату предоставившим их лицам в размере денежных средств, оставшихся после исполнения всех обязательств участников платежной системы.

9. По долгам оператора платежной системы, центрального платежного клирингового контрагента, участника платежной системы не может быть наложен арест на денежные средства, находящиеся на счете гарантийного фонда платежной системы, а также не могут быть приостановлены операции по указанному счету. Приостановление операций по счету гарантийного фонда платежной системы по основаниям, предусмотренным законодательством Российской Федерации о налогах и сборах, не допускается.

10. На денежные средства, находящиеся на счете гарантийного фонда платежной системы, не может быть обращено взыскание по обязательствам опера-

тора платежной системы, центрального платежного клирингового контрагента или участника платежной системы.

Глава 5. НАДЗОР И НАБЛЮДЕНИЕ В НАЦИОНАЛЬНОЙ ПЛАТЕЖНОЙ СИСТЕМЕ

Статья 31 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа).

Статья 31. Цели надзора и наблюдения в национальной платежной системе

1. Основными целями надзора и наблюдения в национальной платежной системе являются обеспечение стабильности национальной платежной системы и ее развитие.

2. В целях настоящего Федерального закона надзор в национальной платежной системе означает деятельность Банка России по контролю за соблюдением операторами по переводу денежных средств, являющимися кредитными организациями, операторами платежных систем, операторами услуг платежной инфраструктуры требований настоящего Федерального закона и принимаемых в соответствии с ним нормативных актов Банка России.

3. Надзор за соблюдением кредитными организациями требований настоящего Федерального закона и принимаемых в соответствии с ним нормативных актов Банка России осуществляется Банком России в соответствии с законодательством Российской Федерации о банках и банковской деятельности, за исключением случая, указанного в части 8 статьи 34 настоящего Федерального закона.

4. Надзор за соблюдением не являющимися кредитными организациями операторами платежных систем, операторами услуг платежной инфраструктуры (далее — поднадзорные организации) требований настоящего Федерального закона и принимаемых в соответствии с ним нормативных актов Банка России осуществляется Банком России в соответствии с настоящим Федеральным законом.

5. В целях настоящего Федерального закона наблюдение в национальной платежной системе означает деятельность Банка России по совершенствованию операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры (далее — наблюдаемые организации), другими субъектами национальной платежной системы своей деятельности и оказываемых ими услуг, а также по развитию платежных систем, платежной инфраструктуры (далее — объекты наблюдения) на основе рекомендаций Банка России.

Статья 32 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа).

Статья 32. Осуществление надзора в национальной платежной системе

1. При осуществлении надзора в национальной платежной системе Банк России:

1) анализирует документы и информацию (в том числе данные отчетности), которые касаются деятельности поднадзорных организаций и участников платежных систем, а также организации и функционирования платежных систем;

2) проводит инспекционные проверки поднадзорных организаций в соответствии со статьей 33 настоящего Федерального закона;

3) осуществляет действия и применяет меры принуждения в соответствии со статьей 34 настоящего Федерального закона в случае нарушения поднадзорными организациями требований настоящего Федерального закона или принятых в соответствии с ним нормативных актов Банка России.

2. Банк России определяет формы и сроки предоставления отчетности, в том числе в виде отчетности поднадзорной организации и сводной отчетности по платежной системе, методику составления указанной отчетности.

3. При осуществлении надзора в национальной платежной системе Банк России вправе запрашивать и получать от поднадзорных организаций и участников платежной системы документы и иную необходимую информацию, в том числе содержащую персональные данные.

4. Порядок осуществления надзора в национальной платежной системе определяется в соответствии с нормативными актами Банка России.

Статья 33 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа).

Статья 33. Порядок проведения инспекционных проверок поднадзорных организаций

1. Банк России проводит плановые инспекционные проверки поднадзорных организаций не чаще одного раза в два года в соответствии с утвержденным Банком России планом проверок.

2. При нарушении бесперебойности функционирования значимой платежной системы Банк России проводит внеплановые инспекционные проверки.

3. Инспекционные проверки могут проводиться по отдельным вопросам деятельности поднадзорных организаций либо являться комплексными.

4. При проведении инспекционной проверки поднадзорной организации уполномоченные представители (служащие) Банка России имеют право:

1) получать и проверять документы поднадзорной организации;

2) при необходимости получать копии документов для приобщения к материалам проверки;

3) получать устные и письменные пояснения по вопросам деятельности поднадзорной организации;

4) получать доступ в места осуществления деятельности поднадзорной организации;

5) получать доступ к информационным системам поднадзорной организации, включая получение информации в электронном виде.

5. По итогам инспекционной проверки уполномоченные представители (служащие) Банка России составляют акт инспекционной проверки, содержащий общую информацию о деятельности поднадзорной организации, информацию о выявленных в ходе проверки нарушениях с приложением подтверждающих документов, сведения о фактах противодействия проверке.

6. Срок проведения инспекционной проверки Банка России не может превышать три месяца.

7. Порядок проведения инспекционных проверок поднадзорных организаций регулируется нормативными актами Банка России.

Статья 34 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа).

Статья 34. Действия и меры принуждения, применяемые Банком России в случае нарушения поднадзорной организацией требований настоящего Федерального закона или принятых в соответствии с ним нормативных актов Банка России

1. В случаях, если нарушения требований настоящего Федерального закона или принятых в соответствии с ним нормативных актов Банка России поднадзорной организацией непосредственно не влияют на бесперебойность функционирования платежной системы, а также не влияют на услуги, оказываемые участникам платежной системы и их клиентам, Банк России осуществляет следующие действия:

1) доводит до сведения органов управления поднадзорной организации информацию о выявленном нарушении в письменной форме с указанием допущенного нарушения и срока, в течение которого такое нарушение должно быть устранено, при этом указанный срок не может быть менее 10 рабочих дней;

2) направляет органам управления поднадзорной организации рекомендации надзорного органа по устранению выявленного нарушения и рекомендует им представить в надзорный орган программу мероприятий, направленных на устранение нарушения.

2. В случаях, если нарушения требований настоящего Федерального закона или принятых в соответствии с ним нормативных актов Банка России поднадзорной организацией влияют на бесперебойность функционирования платежной системы либо на услуги, оказываемые участникам платежной системы и их клиентам, Банк России применяет одну из следующих мер принуждения:

1) направляет предписание об устранении нарушения с указанием срока для его устранения;

2) ограничивает (приостанавливает) предписанием оказание операционных услуг, в том числе при привлечении операционного центра, находящегося за пределами Российской Федерации, и (или) услуг платежного клиринга.

3. В предписание об устранении нарушения не включается информация о неприменении поднадзорной организацией документов (актов) Банка России, не являющихся нормативными актами, предписаниями Банка России или актами Банка России, предусмотренными пунктом 1 части 1 настоящей статьи.

4. Меры принуждения, предусмотренные частью 2 настоящей статьи, применяются Банком России также в следующих случаях:

1) при повторном в течение последних 12 месяцев нарушении поднадзорной организацией требования настоящего Федерального закона или принято-

го в соответствии с ним нормативного акта Банка России, если в отношении поднадзорной организации Банком России за нарушение этого требования осуществлялись действия, предусмотренные пунктом 1 части 1 настоящей статьи, или применялись меры принуждения, предусмотренные частью 2 настоящей статьи;

2) при действиях (бездействии) поднадзорной организации, повлекших (повлекшем) приостановление (прекращение) осуществления переводов денежных средств в рамках платежной системы либо их несвоевременное осуществление, если в отношении поднадзорной организации Банком России осуществлялись действия, предусмотренные пунктом 1 части 1 настоящей статьи, или применялись меры принуждения, предусмотренные частью 2 настоящей статьи;

3) если предписание Банка России не было выполнено поднадзорной организацией в установленный срок;

4) при неустранении нарушения, информация о котором была доведена Банком России до сведения поднадзорной организации в соответствии с пунктом 1 части 1 настоящей статьи, в установленный срок.

5. Мера принуждения, указанная в пункте 2 части 2 настоящей статьи, вводится на определенный предписанием срок и может включать ограничения:

1) предельного размера позиций на нетто-основе участника (участников) платежной системы;

2) предельного количества распоряжений участника (участников) платежной системы и (или) общей суммы указанных распоряжений в течение дня.

6. В случае, если по истечении срока действия меры принуждения, указанной в пункте 2 части 2 настоящей статьи, допущенные нарушения не устранены, срок действия данной меры принуждения может быть продлен предписанием Банка России до устранения нарушения.

7. Предписание Банка России о применении меры принуждения, указанной в пункте 2 части 2 настоящей статьи, направляется оператору платежной системы и оператору услуг платежной инфраструктуры, в отношении которых вводится ограничение.

8. В случае неоднократного невыполнения предписаний с требованием об устранении нарушения, влияющего на бесперебойность функционирования платежной системы, в течение одного года со дня направления первого предписания Банка России об устранении такого нарушения Банк России исключает оператора платежной системы из реестра операторов платежных систем.

9. В случае неоднократного в течение года применения к оператору платежной системы, являющемуся кредитной организацией, за нарушение требований настоящего Федерального закона или принятых в соответствии с ним нормативных актов Банка России, если указанное нарушение влияет на бесперебойность функционирования платежной системы, мер, предусмотренных статьей 74 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Россий-

ской Федерации (Банке России)», Банк России исключает оператора платежной системы, являющегося кредитной организацией, из реестра операторов платежных систем.

10. Решение об исключении оператора платежной системы из реестра операторов платежных систем оформляется в виде приказа Банка России и публикуется в официальном издании Банка России «Вестник Банка России». Обжалование решения Банка России об исключении оператора платежной системы из реестра операторов платежных систем, а также применение мер по обеспечению иска (обеспечительных мер) не приостанавливает действия указанного решения Банка России.

11. Банк России привлекает поднадзорную организацию и ее должностных лиц к административной ответственности в соответствии с Кодексом Российской Федерации об административных правонарушениях.

Статья 35 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа).

Статья 35. Содержание и приоритеты наблюдения в национальной платежной системе

1. Наблюдение в национальной платежной системе включает следующие виды деятельности:

К отношениям, регулируемым Федеральным законом от 03.06.2009 № 103-ФЗ «О деятельности по приему платежей физических лиц, осуществляемой платежными агентами» нормы данного документа применяются только в части осуществления Банком России мониторинга в соответствии с пунктом 1 части 1 статьи 35 (часть 3 статьи 1 Федерального закона от 03.06.2009 N 103-ФЗ).

1) сбор, систематизацию и анализ информации о деятельности наблюдаемых организаций, других субъектов национальной платежной системы и связанных с ними объектов наблюдения (далее — мониторинг);

2) оценку деятельности наблюдаемых организаций и связанных с ними объектов наблюдения (далее — оценка);

3) подготовку по результатам указанной оценки предложений по изменению деятельности оцениваемых наблюдаемых организаций и связанных с ними объектов наблюдения (далее — инициирование изменений).

2. Приоритетным является наблюдение за значимыми платежными системами, которое осуществляется Банком России посредством всех видов деятельности, указанных в части 1 настоящей статьи. В отношении наблюдаемых организаций, других субъектов национальной платежной системы, платежных систем, не являющихся значимыми, а также других объектов наблюдения Банк России осуществляет мониторинг.

3. При осуществлении мониторинга Банк России вправе запрашивать и получать от наблюдаемых организаций, других субъектов национальной платежной системы информацию об оказываемых ими платежных услугах, услугах платежной инфраструктуры.

4. Банк России вправе запрашивать и получать от организаций федеральной почтовой связи информацию об осуществлении ими почтовых переводов денежных средств, за исключением сведений, отнесенных Федеральным законом от 17 июля 1999 года № 176-ФЗ «О почтовой связи» к тайне связи, в порядке, установленном Банком России, по согласованию с федеральным органом исполнительной власти в области связи.

5. При осуществлении оценки Банк России определяет степень соответствия наблюдаемых организаций и связанных с ними объектов наблюдения рекомендациям Банка России, к которым относятся собственные рекомендации Банка России, а также рекомендации по использованию стандартов или лучшей мировой и отечественной практики, при условии опубликования соответствующих документов в изданиях Банка России на русском языке. При необходимости Банк России издает методические разъяснения по использованию указанных рекомендаций.

6. Банк России осуществляет оценку в соответствии с методиками оценки, которые опубликовываются в официальном издании Банка России «Вестник Банка России», размещаются на интернет-сайте Банка России и при необходимости дополнительно доводятся до сведения наблюдаемых организаций.

7. До проведения оценки Банк России предлагает оператору значимой платежной системы самостоятельно провести предварительную оценку с применением опубликованных методик оценки и направлением результатов оценки в Банк России. Предварительная оценка, проведенная оператором значимой платежной системы, учитывается при проведении оценки Банком России.

8. Обобщенные результаты оценки опубликовываются и размещаются на интернет-сайте Банка России. Детализированные результаты оценки могут быть опубликованы Банком России с согласия оператора оцениваемой значимой платежной системы.

9. При иницировании изменений по результатам оценки Банк России может:

1) довести материалы оценки и ее результаты до органов управления наблюдаемой организации с их последующим обсуждением;

2) совместно с наблюдаемыми организациями разработать мероприятия по предлагаемым изменениям;

3) опубликовать и разместить на интернет-сайте Банка России информацию об отказе наблюдаемой организации принять предложенные Банком России изменения, а также позицию наблюдаемой организации по данному вопросу.

10. Банк России публикует обзор результатов наблюдения за значимыми платежными системами и общий обзор результатов наблюдения в национальной платежной системе не реже одного раза в два года.

11. Порядок осуществления наблюдения в национальной платежной системе определяется нормативными актами Банка России.

Статья 36 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа).

Статья 36. Взаимодействие Банка России с федеральными органами исполнительной власти при осуществлении надзора и наблюдения в национальной платежной системе

1. При осуществлении надзора и наблюдения в национальной платежной системе Банк России взаимодействует с федеральными органами исполнительной власти.

2. При осуществлении надзора и наблюдения за платежными системами, в которых осуществляются переводы денежных средств в целях расчета по сделкам с ценными бумагами и (или) сделкам, совершенным на организованных торгах, Банк России взаимодействует с федеральным органом исполнительной власти по финансовым рынкам, в том числе по вопросам участия в платежных системах профессиональных участников рынка ценных бумаг, юридических лиц — участников организованных торгов и (или) участников клиринга, а также по вопросам взаимодействия операторов услуг платежной инфраструктуры с клиринговыми организациями, центральными контрагентами и (или) депозитариями.

3. При осуществлении надзора и наблюдения за платежными системами, в которых осуществляются переводы денежных средств в целях расчетов по обязательным видам страхования гражданской ответственности, предусмотренным законодательством Российской Федерации, Банк России взаимодействует с уполномоченным федеральным органом исполнительной власти.

Статья 37 данного документа вступает в силу по истечении одного года после дня официального опубликования (часть 3 статьи 39 данного документа).

Статья 37. Международное сотрудничество Банка России по вопросам надзора и наблюдения в национальной платежной системе

1. Сотрудничество Банка России с центральными банками и иными органами надзора и наблюдения в национальных платежных системах иностранных государств осуществляется в соответствии с заключенными с ними соглашениями (меморандумами) о сотрудничестве.

2. Банк России может запросить центральный банк и иной орган надзора и наблюдения в национальной платежной системе иностранного государства о предоставлении информации или документов, которые получены в ходе исполнения функций надзора и наблюдения, а также может предоставить центральному банку и иному органу надзора и наблюдения в национальной платежной системе иностранного государства указанные информацию или документы, которые не содержат сведений о переводах денежных средств, при условии обеспечения указанным органом надзора и наблюдения в национальной платежной системе режима сохранности информации, соответствующего установленным законодательством Российской Федерации требованиям обеспечения сохранности информации, предъявляемым к Банку России. В отношении информации и документов, которые получены от центральных банков и иных органов надзора и наблюдения в национальных платежных системах

иностранных государств, Банк России обязан соблюдать требования по раскрытию информации в соответствии с заключенными соглашениями (меморандумами) о сотрудничестве.

Глава 6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Статья 38. Заключительные положения

1. Организации, которые на день вступления в силу настоящего Федерального закона являлись обязанными лицами по денежным обязательствам, предусмотренным частью 3 статьи 12 настоящего Федерального закона (далее — обязанные организации), вправе продолжать принятие на себя таких денежных обязательств в течение 15 месяцев со дня официального опубликования настоящего Федерального закона.

2. В течение срока, указанного в части 1 настоящей статьи, обязанная организация вправе также осуществить уступку прав требования и перевод долга по принятым денежным обязательствам, предусмотренным частью 3 статьи 12 настоящего Федерального закона, кредитной организации, имеющей право осуществлять переводы денежных средств без открытия банковских счетов, в том числе электронных денежных средств. В этом случае обязанная организация обязана уведомить физических лиц о предстоящей уступке прав требования и переводе долга путем размещения соответствующего объявления в средствах массовой информации, на своем интернет-сайте, а также вправе направить уведомление иным способом.

3. Если в течение 30 календарных дней с момента первого размещения уведомления в средствах массовой информации или на своем интернет-сайте физическое лицо не направило в адрес обязанной организации в письменном или электронном виде свои возражения против уступки прав требования и перевода долга, считается, что физическое лицо выразило согласие на уступку прав требования и перевод долга.

4. Если физическое лицо в срок, указанный в части 3 настоящей статьи, направило в адрес обязанной организации в письменном или электронном виде свои возражения против уступки прав требования и перевода долга, обязанная организация не вправе осуществить уступку прав требования и перевод долга. В этом случае обязательства между обязанной организацией и физическим лицом в части денежных обязательств, предусмотренных частью 3 статьи 12 настоящего Федерального закона, прекращаются с момента получения обязанной организацией возражений физического лица. При этом обязанная организация должна в течение трех рабочих дней со дня обращения физического лица возвратить остаток денежных средств, переданных ей физическим лицом в целях принятия обязанной организацией денежных обязательств, предусмотренных частью 3 статьи 12 настоящего Федерального закона.

5. Кредитные организации, осуществляющие перевод электронных денежных средств на день вступления в силу настоящего Федерального закона, обязаны привести свою деятельность в соответствие с требованиями настоящего Фе-

дерального закона в течение трех месяцев со дня вступления в силу настоящего Федерального закона.

6. Организации, осуществляющие деятельность операторов платежных систем, обязаны привести свою деятельность в соответствие с требованиями настоящего Федерального закона и направить в Банк России регистрационное заявление в соответствии со статьей 15 настоящего Федерального закона в течение шести месяцев со дня вступления в силу указанной статьи настоящего Федерального закона.

7. Положения части 11 статьи 16 и пункта 3 части 12 статьи 21 настоящего Федерального закона в части привлечения операционного центра и (или) платежного клирингового центра применяются по истечении трех лет после дня официального опубликования настоящего Федерального закона.

8. Со дня вступления в силу настоящего Федерального закона деятельность банковских платежных агентов (субагентов) без использования специального банковского счета (счетов) для зачисления в полном объеме полученных от физических лиц наличных денежных средств в соответствии с частями 5 и 6 статьи 14 настоящего Федерального закона не допускается.

9. Действие статьи 14 настоящего Федерального закона распространяется на отношения, возникшие из договоров, ранее заключенных кредитными организациями и организациями, не являющимися кредитными организациями, а также индивидуальными предпринимателями в соответствии со статьей 13.1 Федерального закона «О банках и банковской деятельности».

Статья 39. Порядок вступления в силу настоящего Федерального закона

1. Настоящий Федеральный закон вступает в силу по истечении девяноста дней после дня его официального опубликования, за исключением положений, для которых настоящей статьёй установлены иные сроки вступления их в силу.

2. Пункты 12—16 статьи 3, статьи 5, 6 и 8 настоящего Федерального закона вступают в силу по истечении ста восьмидесяти дней после дня официального опубликования настоящего Федерального закона.

3. Статьи 1, 2, пункты 1, 6—11, 20—25 статьи 3, статьи 15 и 16, части 1—7 статьи 17, статьи 18—25, 27—37 настоящего Федерального закона вступают в силу по истечении одного года после дня официального опубликования настоящего Федерального закона.

4. Части 2, 4—8, 11—16 статьи 9 настоящего Федерального закона вступают в силу по истечении 18 месяцев после дня официального опубликования настоящего Федерального закона.