ВЛАДИМИР
ОВЧИНСКИЙ

МАФИЯ

НОВЫЕ МИРОВЫЕ ТЕНДЕНЦИИ

Коллекция Изборского клуба

Владимир Овчинский

Мафия. Новые мировые тенденции

«Книжный мир»
2016

Овчинский В. С.

Мафия. Новые мировые тенденции / В. С. Овчинский — «Книжный мир», 2016 — (Коллекция Изборского клуба)

ISBN 978-5-8041-0872-5

В ближайшем будущем нашу планету ждет новая научно-техническая революция, цифровой мир, виртуализация всего и вся – в том числе и организованной преступности. Переход мафии в киберпространство сулит ей невиданный взлет преступных прибылей, сетевая организация международной организованной преступности делает ее практически неуязвимой для «старых» – национальных и офлайновых – органов правопорядка.Мафия замахнулась на самое святое, что есть у человечества – на государство. Боссы преступных синдикатов стремятся не только контролировать глобальный процесс трансформации национального государства в государство-корпорацию, но и заменить последнее мафиозным государством.В каких киберпространствах развернутся в ближайшие годы сражения с мафией? Как это отразится на мировой политике, отдельных государствах и на каждом из нас? Сможет ли мировое сообщество во главе с ООН, Интерполом и Европолом дать достойный ответ врагам рода человеческого, или мир погрузится в пучину криминального беспредела? Что надо сделать в России, чтобы достойно встретить преступные вызовы грядущего десятилетия?Об этом – в книге доктора юридических наук, генерал-майора В.С. Овчинского.

ISBN 978-5-8041-0872-5

Содержание

Владимир Овчинский
Мафия: новые мировые тенденции

Вместо предисловия
О мафии, ее огосударствлении, мафиозном государстве и системной мафиозной модели

С середины 80-х годов прошлого века, работая в системе МВД, я в практическом и научном плане начал анализировать ситуацию, связанную с организованной преступностью. При этом я всегда полагал, что для определения самой организованной преступности нет смысла заново «придумывать велосипед». Целесообразно использовать понятийный аппарат, содержащийся в документах ООН. Как известно, там на многих конгрессах и конференциях выработано *понятие организованной преступности (в разных модификациях) как сложного переплетения противоправных действий, совершаемых преступными формированиями, целью которых является достижение сверхприбылей с использованием коррупции, насилия и запугивания конкурентов и населения*.

При этом я полагаю, что в качестве синонима термина «организованная преступность» в научном плане можно использовать термин «**мафия**» (имея в виду, конечно, не классическую итальянскую мафию, а любые структуры организованной преступности).

Независимо от того, какое определение мы возьмем за основу исследования данного явления, его материальное выражение в любом случае едино – это организованные преступные группы, организации и сообщества. Причем иные устойчивые формирования могут иметь главарей, планировать преступления, распределять роли между соучастниками, но при всем этом не входить в структуру организованной преступности. Здесь важны не количественные, а качественные признаки, присущие в полной мере «мафии». Перекочевав в наш язык, этот термин уже успел стать привычным. Начиная с 1992 г., он используется даже в официальных документах. Не вдаваясь в дискуссию с другими, как зарубежными, так и отечественными исследователями, мы называем мафией *тайные преступные организации, включенные в систему организованной преступности, имеющие коррумпированные связи и ролевой статус в преступной среде или теневой экономике*. Все эти признаки переплетаются между собой и дополняют друг друга.

• Как тайные организации мафия основывается на конспирации, жесткой дисциплине, определенной иерархии, законах «омерты» и «вендетты» (кара за нарушенный обет молчания и кровная месть);

• как преступные организации она может быть универсальной (совершать любые наборы преступлений – от вымогательства до киберпреступлений, от перевозки наркотиков до диверсий и террористических актов) и специализированной (например, ориентированной только на наркобизнес или на похищение и перепродажу автомобилей);

• как элемент системы организованной преступности мафия участвует в процессе рациональной реорганизации преступного мира;

• как организации, имеющие коррумпированные связи, она стремится уменьшить риск судебного преследования, но, подкупая представителей власти и спецслужб, тем самым заставляет их служить себе (по данным милиции и социологов, половина доходов, получаемых преступным путем, идет на подкуп властных структур и правоохранительных органов);

• что касается ролевого статуса в преступной среде, то мафия включена в относительно устойчивую систему взаимоотношений между различными категориями преступников (известно, что в криминальной среде действуют свои неписаные законы, субкультура общения, делятся сферы преступного бизнеса и территории и т. д.); здесь формируется своя идеология с широким набором нравственных, «правовых», эстетических и даже философских идей, оправдывающих преступность;

• роль мафии в теневой экономике проявляется в стимулировании роста дефицита на потребительском рынке, контроле за сферой скрытого производства, закупок и распределения товаров[1].

К концу 90-х годов у меня созрело полное убеждение в том, что *организованная преступность (мафия) стала формой социальной организации жизни во многих странах мира, в т. ч. и в России*. Базируясь на этом убеждении, я солидарен с российскими социологами в том, что организованное преступное сообщество можно рассматривать как новую особую форму социальной организации индивидов, имеющих определенные материальные цели и интересы и объединенных противоправным способом их достижения и удовлетворения.

Но организованная преступность, на мой взгляд, это не только и не столько совокупность различных организованных групп и сообществ, это и форма жизнедеятельности отдельных индивидов, групп лиц, которые моделируют в своем индивидуальном поведении и образе жизни стереотипы поведения и образ жизни преступных сообществ.

Таким образом, в социальную ткань общества вклиниваются как высокоорганизованные преступные сообщества, так и не связанные с ними непосредственно отдельные индивиды или группы индивидов, которые действуют в парадигме этих преступных сообществ.

Такие формы социальной организации жизни в большей мере относятся к архаическим и иерархическим отношениям между членами общества (хотя в последние годы они приобретают все более *сетевой характер*, используя горизонтальные связи). Но, в любом случае, они далеки от отношений общества граждан или гражданского общества.

Если использовать термин «мафия» как синоним понятия «организованная преступность», то можно констатировать, что в современном мире отношения между индивидом и сообществом в большей мере выстраиваются не по типу гражданского общества, а по типу общества мафиозного.

По определению философов, гражданское общество – это тип общества, где сам эпитет «гражданское» означает высшее из доселе известных истории проявление экономической культуры, политической культуры и правовой культуры.

По аналогии с этим определением мафиозное общество – тип общественных отношений, связанный с проявлением субкультуры («воровской культуры»), теневой экономической, политической, антиправовой контркультуры.

Свои особые отношения выстаивает организованная преступность и с государством. Если исходить из концептуального подхода Андрея Фурсова о превращении нации-государства в корпорацию-государство, то следует констатировать, что это превращение подразумевает разные типы взаимоотношений государства и мафии.

Нация-государство предполагает, что организованная преступность (при всех возможных точках соприкосновения) является врагом государства.

Корпорация-государство, учитывая, что принцип ее организации – клан, а цель – приватизация совокупного общественного процесса, включает наиболее крупные и успешные сегменты организованной преступности в клановую структуру и активно использует их в приватизации общественного процесса.

Иными словами, мафия из врага государства (как нации) превращается в элемент государства (как корпорации).

Подобный процесс еще в 1990 г. в коллективной книге (с участием автора) «Постперестройка» был назван «***огосударствлением мафии***»[2]. Под «огосударствлением» мы понимаем такую социально-политическую ситуацию, где государственные структуры отражают интересы

---

[1] См.: Овчинский В.С. Мафия: необъявленный визит. М., 1993; Овчинский В.С. Стратегия борьбы с мафией. М., 1993; Овчинский В.С., Овчинский С.С. Борьба с мафией в России. М., 1993; Основы борьбы с организованной преступностью. Под ред. В.С. Овчинского, В.Е. Эминова, Н.П. Яблокова. М., 1996.

[2] См.: Постперестройка. М., 1990.

крупных криминально-олигархических кланов, а сами мафиозные структуры и их лидеры участвуют в принятии важнейших политических и экономических решений.

В XXI веке многие социологи, криминологи и журналисты пошли дальше и ввели в обиход термин «***мафиозное государство***», под которым понимается модель государственного управления, при которой коррупция пронизывает все эшелоны государственной власти вплоть до симбиоза между государственным аппаратом и организованной преступностью[3].

Часто это понятие используется в идеологических целях в период информационных войн против России и других государств. Но ряд исследователей дали интересные научные трактовки «мафиозного государства» независимо от идеологических пристрастий.

Например, Мойзес Наим в статье «Мафиозные государства: организованная преступность рвется к власти»[4] пишет, что в период глобального экономического кризиса реальные очертания приобретает новая угроза – мафиозное государство. Преступники по всему земному шару внедряются в правительства в беспрецедентных масштабах.

«Наблюдается и обратный процесс: вместо того чтобы ликвидировать мощные банды, некоторые правительства предпочитают брать под контроль их противозаконную деятельность.

Правительственные чиновники мафиозных государств заняты обогащением себя, своих семей и друзей путем эксплуатации денежных потоков, физических ресурсов, политического влияния и глобальных связей с криминальными синдикатами ради укрепления и расширения собственной власти. И действительно, руководящие посты в некоторых наиболее прибыльных нелегальных предприятиях в мире заполняются уже не только профессиональными преступниками – их занимают высшие государственные чины, законодатели, руководители спецслужб, главы полицейских управлений, армейские чины и, в самых крайних случаях, даже главы государств и члены их семейств»[5].

По мнению Мойзеса Наима, сущность организованной преступности за последние два десятилетия претерпела столь разительные перемены, что криминальные сети вышли за пределы своих традиционных рынков и начали пользоваться всеми преимуществами политических и экономических изменений, поставив себе на службу новые технологии.

Сегодня во многих странах преступники вовсе не утруждают себя подпольной деятельностью, да и к маргиналам они ни в малейшей мере не относятся. В реальности предположительные лидеры многих преступных сообществ стали своеобразными знаменитостями. Зажиточные лица с сомнительным прошлым в бизнесе превратились в желанных всеми филантропов и установили контроль над радиостанциями и телеканалами, стали владельцами влиятельных газет.

Накопление преступниками богатства и власти, пишет Мойзес Наим, зависит теперь не только от их собственной нелегальной деятельности, но и от действий среднестатистических членов общества. Например, миллионы граждан заняты в китайской индустрии контрафактной продукции и афганской наркоторговле. От них не отстают миллионы жителей Запада, регулярно курящие марихуану, сотни тысяч мигрантов, каждый год нанимающие преступников, чтобы те нелегально доставили их в Европу, и преуспевающие профессионалы из Манхэттена и Милана, предоставляющие рабочие места нянь и уборщиков нелегальным иммигрантам. Именно такие рядовые граждане и превратились в неотъемлемую часть ***криминальной экосистемы***.

Трудно не согласиться с Мойзесом Наимом и в том, что современные правоохранительные органы пока еще не могут состязаться с преступными организациями – те не только богаты,

---

[3] Measuring the Mafia-State Menace / Foreign Affairs (http://www.foreignaffairs. com/articles/137692/peter-andreas-moises-naim/measuring-the-mafia-state-menace).

[4] Foreign Affairs, № 3, 2012.

[5] Там же.

жестки и безжалостны, но и пользуются огромным преимуществом в виде безоговорочной поддержки со стороны национальных правительств, дипломатов, судей, спецслужб, генералов, шефов полиции. Мафиозные государства могут позволить себе лучших юристов и экономистов, а также доступ к самым продвинутым технологиям. Страдающие от недофинансирования правоохранительные ведомства, заваленные по уши работой суды и неповоротливый бюрократический аппарат все чаще просто не поспевают за столь щедро финансируемым и маневренным заклятым врагом.

«Мафиозные государства сводят воедино скорость и гибкость транснациональных криминальных сетей и юридическую защиту и дипломатические привилегии, по определению дарованные только государству, создавая в итоге некий ***гибрид интернациональной структуры***, против которой в арсеналах национальных правоохранительных органов практически нет средств»[6].

В рамках XVI Апрельской международной научной конференции, проходящей в Высшей школе экономики (2015 г.), венгерским политологом Балинтом Мадьяр была прочитана лекция «Посткоммунистические государства на примере Венгрии», которая практически полностью была посвящена теории «мафиозного государства»[7].

Балинт Мадьяр полагает, что термин «мафиозное государство» не является публицистическим и не наделен какой-либо эмоционально-оценочной окраской; его выбор обусловлен тем, что он позволяет емко охарактеризовать основные черты правящей элиты, особенности ее организации и иерархии.

Характеристики этой относительно небольшой верхушки нового авторитарного общества и обусловливают принципиальное отличие мафиозного государства от аналогичных режимов, где элита наделена авторитарной властью. Прежде всего стоит упомянуть, что в основе системы – что свойственно любой мафии – совместные предприятия, создателями которых являются собственно члены «семьи», а также другие представители политической элиты, принятые в «семью» благодаря существующей системе взаимоотношений. Членов организации соединяют кровные и партнерские узы, охватывающие большее и большее число «семей», управляемых одним главой, который подчиняет себе пирамидальную иерархию власти. В мафиозном государстве (преступной элите) под контролем главы «семьи» оказывается вся страна. Управление осуществляется под прикрытием демократических институтов путем обретения власти и постоянного поиска новых средств для ее укрепления.

В мафиозном государстве имеет место одновременная концентрация политической власти и экономического благосостояния. Эти два понятия находятся в неразрывной связке. Далее ротация политических и экономических элит происходит не на демократической основе или вследствие рыночных механизмов, но является управляемым процессом, в котором ключевую роль занимает место того или иного человека в созданной иерархии правящей «семьи». В силу такого прошлого новые владельцы предприятий становятся не бизнесменами в деловом смысле слова, но сборщиками налогов для «семьи». Общее благо становится подчинено частным интересам на постоянной основе.

Реальные задачи социальной и экономической политики остаются в тени, и решения принимаются на основе других соображений, например, отмывания денег. Точно так же, как и реальная мафия, мафиозное государство стремится ликвидировать бытовую, неподконтрольную «семье» коррупцию, и заменить ее централизованным и формально законным механизмом перераспределения средств.

Точно так же незаконное «принуждение к сотрудничеству» заменяется на формально законные государственные требования, целью которых является закрепление благосостояния

---

[6] Там же.

[7] Мафиозное государство: «отец семьи», полигархи и все остальные / https://lenta.ru/articles/2015/04/12/mafiastate/.

политической семьи, находящейся у власти. В то время как классическая мафия опирается на шантаж, угрозы, а иногда и физическое насилие, в мафиозном государстве сферы интересов могут корректироваться *псевдозаконным государственным принуждением*»[8].

«С точки зрения социальных структур мафиозное государство создает систему патерналистско-клиентских отношений, которые строятся в иерархичной форме, с главой «семьи», находящимся на вершине пирамиды. Под прикрытием государственных институтов демократическое общество с его множеством слабых горизонтальных связей заменяется на иерархичное общество с низким числом прочных социальных связей. Отношения «патрон-клиент» ведут в перспективе к уничтожению автономии индивида и появлению цепочки зависимостей, особенно в политической сфере»[9].

Еще одно оригинальное объяснение современной организованной преступности дает Антонио Де Бонис. Он полагает, что современный мир порождает преступные сообщества качественно нового типа – ***системную мафиозную модель***. Мафия опирается на ресурсы государства и капиталистической экономики, оставляя за собой право на насилие[10].

Отсталость экономики и слабость государственных институтов, по мнению Антонио Де Бонис, – питательная среда для появления и развития мафии. Сама мафия вполне может опираться на передовые способы управления, комбинируя горизонтальные и вертикальные схемы, но при этом загоняя государство и общество в еще более периферийное положение.

Демократизация сама по себе не является гарантией уничтожения мафии. Организованная преступность успешно использует как демократические, так и автократические институты для отстаивания своих интересов. Переход к демократии должен сопровождаться созданием эффективных государственных институтов. Сущностная черта мафии – попытка слияния с государством, использования его властных возможностей, а не борьба с ним.

Корпоративный сектор – важная составляющая современной мафиозной системы. Стратегическая парадигма мафии – переход от преступления или их совокупности к преступной бизнес-модели.

По мнению Антонио Де Бониса, современная эпоха привнесла ряд серьезных новшеств во взаимоотношение государства и мафии. Уровень организации и рационализации преступности существенно вырос, иногда даже обгоняя государство – в силу возможности смешивать вертикальную и горизонтальную систему управления.

Еще более важно то, что организованная преступность, существовавшая веками, переросла в качественно новое явление. Речь о так называемой системной мафиозной модели. Ее суть – в последовательном проникновении в систему экономики и государственного управления при сохранении собственных инструментов насилия. Современная мафия невозможна без государства и капиталистической экономики. Она использует их возможности в своих интересах[11].

Зарубежные исследователи еще в начале 80-х годов пришли к выводу, что криминальная экспансия охватывает все сферы цивилизации, что международная, транснациональная преступность всегда политизирована, имеет свои модели решения противоречий, возникающих как внутри отдельных стран, так и в межгосударственных отношениях, выступает «спонсором» отдельных типов социально-экономических реформ.

---

[8] Там же.

[9] Там же.

[10] Мафия, государство и капиталистическая экономика: конкуренция или конвергенция? 12.11.2015. Россия в глобальной политике / http://www. globalaffairs.ru/valday/Mafiya-gosudarstvo-i-kapitalisticheskay-ekonomika-konkurenciya-ili-konvergentciya-17804.

[11] Там же.

Начало XXI века было ознаменовано принятием ***Конвенции ООН против транснациональной организованной преступности***[12]. В следующем году созданная в 2004 г. в рамках ООН. Группа высокого уровня по угрозам, вызовам и переменам назвала транснациональную организованную преступность одним из «шести блоков угроз, которыми мир должен заниматься сейчас и в предстоящие десятилетия». В феврале 2010 года Совет Безопасности ООН отметил «с озабоченностью серьезные угрозы, создаваемые в некоторых случаях незаконным оборотом наркотиков и транснациональной организованной преступностью для международной безопасности в различных районах мира» и предложил Генеральному секретарю Организации Объединенных Наций «рассматривать эти угрозы в качестве одного из факторов в стратегии предотвращения конфликтов и при анализе конфликтов и оценке и планировании комплексных миссий». Пресечение деятельности организованной преступности превратилось, таким образом, в приоритетный вопрос международной важности.

В список, причем не исчерпывающий, связанных с организованной преступностью проблем, которые предстоит решать, несомненно, входят торговля людьми, незаконный ввоз мигрантов, незаконный оборот наркотиков, незаконный оборот оружия, незаконный оборот природных ресурсов, незаконная торговля контрафактной продукцией, морское пиратство и киберпреступность.

В документах ООН неоднократно отмечалось, что борьба с организованной преступностью осложняется тем, что сама природа организованной преступности постоянно изменяется. Эпидемии наркомании возникают и прекращаются и вновь возникают в новой среде. Потоки торговли людьми и незаконного оборота огнестрельного оружия резко возрастают в районах конфликтов и также резко сокращаются. Конец холодной войны, сокращение числа и снижение остроты гражданских войн, поступательное движение глобализации, глобальный экономический кризис[13] – все эти факторы оказали непредсказуемое воздействие на организованную преступность.

Мировые тенденции формируются под влиянием глобальных изменений в таких областях, как демография, миграция, урбанизация, конфликты и экономика.

Эксперты ООН считают, что существует общий консенсус в вопросе о том, что в организованной преступности участвуют как высокоструктурированные, так и слабоструктурированные организации, причем, по мнению ряда специалистов, первые проигрывают последним. Согласно приводимым доводам, традиционные иерархически организованные преступные группы в условиях давления со стороны правоохранительных органов выработали «клеточную структуру», аналогичную той, которая наблюдается у террористических групп, и состоящую из небольших сетей, проводящих работу, которую ранее выполняли более жесткие структуры.

Представляется, что эти сети, состоящие из ориентирующихся на рынок отдельных преступников, были сформированы не как ответная реакция со стороны традиционных групп, а всегда существовали в сфере транснационального незаконного оборота, хотя и были менее заметными для правоохранительных органов, уделявших основное внимание проблеме преступности на местном уровне. Здесь, по всей вероятности, можно было бы с наибольшей уверенностью говорить о том, что сами традиционные группы потеряли свое значение по сравнению с рынками, на которых они осуществляют свои операции. По мнению экспертов ООН, в современном мире организованная преступность – это не столько феномен группы отдельных лиц, занимающихся различными видами незаконной деятельности, сколько вопрос группы незаконных видов деятельности, которыми практически занимаются определенные отдельные лица и группы. В случае ареста и изоляции этих отдельных лиц соответствующая деятель-

[12] См.: Овчинский В.С. XXI век против мафии. М., 2001.

[13] См.: Овчинский В.С. Криминология кризиса. М., 2009.

ность продолжается, поскольку по-прежнему остаются незаконный рынок и создаваемые им стимулы.

Эксперты Совета Европы – авторы «Белой книги о транснациональной организованной преступности»[14] выделяют перечень ключевых характеристик современной организованной преступности:

• каждое преступное деяние ложится бременем на общество. Но когда дело доходит до организованной преступности, которая обладает способностью проникать в экономические и социальные ткани общества и представляет собой серьезную угрозу для прав и свобод личности, верховенства права, надежности финансовой системы и демократии, ущерб становится гораздо больше, чем от любых других видов преступлений;

• организованные преступные группы имеют как местное, так и трансграничное измерение, не только в отношении их состава и методов деятельности, но также в отношении деятельности, которую они осуществляют, и ее последствий. Кроме того, эти группы демонстрируют высокую способность к быстрой адаптации своих преступных схем и методов деятельности за счет их гибкости;

• технологические достижения не только способствуют организованной преступности, но также прокладывают путь новым видам преступлений. Например, противодействие в отношении онлайнового мошенничества с целью хищения личных данных (фишинга), банковского мошенничества и кибератак на информационные системы, базы данных и персональные компьютеры стали частью повседневной работы правоохранительных органов[15];

• хотя террористические группы и организованные преступные сообщества имеют разные цели в долгосрочной перспективе, непрерывность их преступных действий зависит от их финансовых возможностей. В частности, незаконный оборот наркотиков выделяется в категорию наркотерроризма из-за высокой финансовой выгоды, которую он приносит;

• организованные преступные группы, как правило, специализируются на предоставлении конкретных услуг, даже если они работают в составе сети. К ним относятся поставка, сокрытие и распространение наркотиков, операции с поддельными документами или вымогательство;

• некоторые организованные преступные группы напоминают преступные предприятия с высокой степенью профессионализма, сложной структурой и людскими ресурсами, тогда как другие очень гибкие и простые;

• с точки зрения преступников, вид товаров, с которым они имеют дело, не имеет столь важного значения. Что их мотивирует, так это способность осуществлять свою деятельность с минимальным риском обнаружения, извлекая при этом максимально возможные прибыли;

• доходы от преступлений, полученных в результате криминальной деятельности, являются основой прочности преступных организаций. Преступные группы проникают в легальную экономику с целью узаконить свои доходы и используют юридических лиц в качестве щита и посредника для осуществления незаконной деятельности. Среди секторов, уязвимых для проникновения организованных преступных групп, – это «ночная жизнь», недвижимость, торговля ювелирными изделиями, пункты обмена валюты, финансовый сектор, туризм, казино, закупки и строительство. Путем реинвестирования незаконной прибыли в законные экономические средства такие группы подрывают законную коммерческую деятельность, противодействуя развитию свободного рынка и справедливой конкуренции;

• преступные группы поддерживаются широким кругом специалистов, например юристов, бухгалтеров, финансовых консультантов, коррумпированных чиновников, судей, полити-

[14] См.: Белая книга о транснациональной организованной преступности. М., 2015.

[15] См.: Ларина Е., Овчинский В. Кибервойны в XXI веке. М., 2014.

ков и химиков. Без поддержки этих профессионалов организованная преступность оказалась бы несостоятельна;

• коррумпирование властей путем подкупа или покупки услуг государственных должностных лиц является общей чертой деятельности организованной преступности, которая позволяет добиться безнаказанности или проникновения в легальную экономику и общественные институты для осуществления общего незаконного бизнеса: политики, чиновники, сотрудники органов безопасности и разведки, армейские офицеры, менеджеры финансового сектора, юристы, адвокаты, промышленники, банковские работники, журналисты и владельцы средств массовой информации или члены их семей и близкие родственники являются лучшими целями для такой практики. Как правило, это процесс, в котором каждая сторона приглядывает за другой.

В настоящей книге публикуются основные положения рабочих документов XIII Конгресса ООН по предупреждению преступности и уголовному правосудию (апрель 2015 года, Доха), докладов Европола, резолюции ПАСЕ, исследований международных организаций о новых мировых тенденциях и формах проявления организованной преступности – мафии, подготовленные в 2014–2016 годах. Причем основное внимание уделено организованной преступности, связанной с новыми информационными технологиями; формированию мафиозно-террористических государств; влиянию мафии на миграционный кризис в Европе; экологической и фармацевтической мафии.

В. Овчинский, доктор юридических наук

Часть I
Новая организованная преступность

От традиционного криминала к кибермафии: всеобъемлющие и сбалансированные подходы в целях предупреждения новых и появляющихся форм транснациональной преступности и надлежащего реагирования на них[16]

Задача предупреждения новых и появляющихся форм организованной преступности и борьбы с ними, а также способность предвидеть процессы изменения преступной деятельности является серьезным вызовом. Еще несколько десятилетий назад мошенничество с кредитными картами было почти немыслимым. За последние несколько лет в результате быстрого технического прогресса, появления новых форм преступности, растущей глобализации и экспоненциального роста мировых рынков открылись сопоставимые по масштабам возможности для активизации противоправной деятельности. Эти возможности стали генератором новых форм ценностей и создания новых каналов связи между правонарушителями и их потенциальными жертвами и снизили для преступников уровень риска быть пойманными с поличным благодаря появлению новых форм анонимности. Широкое использование таких возможностей способствовало не только распространению новых форм преступности, но и активизации тех видов преступности, которые, как считалось, уже в основном ушли в историю. Одним из примеров такого перерождения преступности является современное пиратство.

Выделить новые и появляющиеся формы преступности в отдельную категорию в системе криминологической типологизации зачастую удается благодаря их соотнесению с похожими видами преступности, такими как киберпреступность, экологическая преступность и пиратство. Однако помимо разработки определений целого ряда различных категорий преступности проблема заключается в том, что необходимо усилить инструментарий статистического анализа, в целях лучшей оценки и описания данной отдельной категории криминологической типологизации путем выявления общих особенностей и различий между подобными новыми формами противоправной деятельности. В этой связи опираться лишь на показатель тенденции преступности или ее динамики как на определяющий фактор при включении этой категории в систему классификации, возможно, недостаточно. Многие новые формы преступности распространяются действительно быстро. Однако за последние годы в некоторых регионах также выросли показатели по ряду других уже давно сложившихся видов противоправной деятельности, в частности по убийствам. Описание новых категорий преступлений требует, скорее всего, учета таких основополагающих признаков преступности, как ее коренные причины и способствующие факторы, способы совершения преступлений, характеристики потерпевших и преступников, степень участия в преступлениях и структура организованных преступных групп.

[16] Рабочий документ, представленный Секретариатом XIII Конгресса ООН по предупреждению преступности и уголовному правосудию (Доха, 12–19 апреля 2015 г., A/CONF.222/8) (Извлечение)

Характеристика новых и появляющихся форм преступности

Процесс определения общих знаменателей новых форм преступности наталкивается на целый ряд препятствий. Во-первых, существует *проблема терминологии*. Государства, органы системы ООН и научное сообщество оперируют несколькими близкими по значению терминами и категориями. В контексте ООН к ним относятся такие понятия, как «новые аспекты преступности», «появление политических проблем» и «новые формы и аспекты транснациональной организованной преступности». Каждое из них отражает различные аспекты развития противоправной деятельности. Хотя внимание настоящего документа сосредоточено на понятии «новые и появляющиеся формы преступности», в нем признаются элементы и других связанных с этим понятием категорий. Новые формы преступности могут также считаться «комплексными», например, в тех случаях, когда уголовно-правовые деяния представляют собой взаимосвязанную последовательность событий и/или когда они распределяются среди множества действующих лиц.

Во-вторых, многие новые категории преступлений сами по себе служат зонтиком для целой серии отдельных правонарушений. Так, например, понятие «экологическая преступность» включает в себя такие деяния, которые существуют уже многие десятилетия, в частности браконьерство, а также правонарушения, которые появились лишь в последние годы, в частности преступления, связанные с торговлей квотами на выбросы углерода и управлением водохозяйственной деятельностью. Аналогичным образом, термин «киберпреступность», как правило, включает как правонарушения, объектом которых являются компьютерные системы или компьютерные данные, так и правонарушения, при которых компьютерные системы или компьютерные данные служат средством преступления, как например, большинство форм преступлений, связанных с хищением личных данных.

В-третьих, новые формы преступности отнюдь не распространяются во всех странах с равной быстротой или достигают равной остроты… Некоторые формы преступности, как представляется, могут иметь лишь национальное воздействие, прежде чем произойдет их постепенное признание в качестве транснациональной угрозы.

Наконец, новые формы преступности могут не только порождать новые коренные причины, способствующие факторы или приемы для совершения противоправной деятельности, но и могут быть направлены также против новых категорий жертв, которые, возможно, будет труднее выявлять. От киберпреступности, в частности от распространения вредоносных компьютерных программ, может пострадать очень значительное число людей. Системы уголовного правосудия, требующие, чтобы в ходе судебного разбирательства в качестве потерпевшего было предъявлено конкретное лицо, может в этой связи столкнуться с особыми трудностями…

Коренные причины и способствующие факторы

Хотя не все новые и появляющиеся формы преступности приводятся в действие одними и теми же социально-экономическими факторами, можно установить целый ряд общих явлений, содействующих распространению преступности, или коренных причин и способствующих факторов. К их числу относятся глобализация; близость нищеты, конфликтов и слабых правоохранительных систем к рынкам высокостоимостных товаров; и темпы возникновения новых форм современных технологий и глобальные средства связи.

Благодаря *глобализации* национальные экономики все активнее интегрируются в систему международной экономики через торговлю, инвестиции, потоки капиталов, перемещение людских ресурсов, а также развитие и распространение технологий. Стремительный процесс гло-

бализации может оказывать давление на существующую структуру управления, расширяя роль негосударственных игроков в структуре все усложняющихся межгосударственных связей.

Этот процесс интеграции и экспансии экономик формирует контекст для перерастания некоторых проблем, имевших когда-то преимущественно локальный характер, в глобальные явления. Например, сфера пиратской деятельности, договорных матчей и противоправных тотализаторов выросла до масштабов транснациональной преступности, а такие направления, как морская торговля и спорт превратились в транснациональные многомиллиардные индустрии, привлекающие широкие инвестиции и интерес почти всех мировых экономик.

Глобализация все шире вовлекает в свободный оборот трудовые ресурсы, товары и финансовые потоки, да к тому же ее темпы в ряде случаев опережают индивидуальные и коллективные действия государств-членов по налаживанию регулирования таких перемещений. Например, объектом мер национального регулирования могут быть растущие транснациональные рынки для отдельных видов дикой фауны и флоры, человеческих органов, медицинских препаратов и культурных ценностей, однако на глобальном уровне может ощущаться дефицит общих определений и стандартов для регулирования, равно как и разнонаправленность тенденций в области преступности.

Этот разрыв создает особые возможности для криминала, поскольку правонарушители пользуются «безопасными убежищами» и брешами в регулирующих режимах, для того чтобы извлекать выгоду из стоимостного роста, обусловленного расхождениями в национальных системах контроля за предложением. Таким путем нелегальные или «серые» рынки растут параллельно и внутри легальных рынков. Эти рынки могут отличаться от незаконного оборота, ассоциируемого с рынками с установленным контролем, в частности с теми рынками, которые связаны с наркотиками, в силу того обстоятельства, что часто трудно отделить легальные рынки от нелегальных. На новых транснациональных рынках противоправная деятельность может начинаться у источника, например в ходе запрещенной браконьерской деятельности или хищения культурных ценностей, или в любой последующей точке цепочки предложения, например, в результате утечки товара и или уклонения от налогообложения в процессе экспорта или незаконного предпродажного переклеивания маркировок.

Если незаконно полученные или похищенные товары вновь всплывают на легальных рынках по поддельным документам или в результате коррупции, то отслеживание преступных деяний в таком случае может быть чрезвычайно затруднено. Легальный рынок служит эффективным средством сокрытия незаконного происхождения участвующего в обороте продукта. Например, транснациональные преступные сети, занимающиеся незаконным оборотом отдельных видов дикой природы и древесины, а также контрабандой электронных отходов и озоноразрушающих веществ часто используют те же самые маршруты, что и легальные импортеры, но по подложным правоустанавливающим документам, через лазейки в законодательстве или по подлинным документам, приобретенным с помощью подкупа.

Преступные возможности могут и далее расширяться по мере устранения торговых барьеров, создания зон свободной торговли и подписания для этого соответствующих соглашений, а также появления высоких уровней потребительского спроса. Например, высокий спрос на основные медицинские препараты в таких регионах, как Африка, в сочетании с ограниченностью возможностей местных систем здравоохранения и национальных механизмов контроля способствует появлению значительного транснационального рынка торговли контрафактными лекарствами. Недавно проведенная проверка показывала, что 35 процентов лекарств, приобретенных для борьбы с малярией в районе Африки к югу от Сахары и в Юго-Восточной Азии, не прошли тест на химический анализ. Из всех препаратов, не прошедших химический анализ, 36 процентов, относившихся к региону Юго-Восточной Азии, и 20 процентов – к региону Африки, расположенному к югу от Сахары, оказались контрафактом.

Аналогичным образом, незаконный рынок человеческих органов стимулируется в огромной мере благодаря глобальному разрыву между предложением человеческих органов и спросом на них. Это особенно актуально в отношении почек как следствие растущего разрыва между участившимися случаями почечной недостаточности и уровнями донорства органов умерших. Что касается предложения таких органов, то нерегулируемое или незаконное изъятие органов часто провоцируется нищетой как социально-экономической первопричиной и усугубляется дефицитом адекватных мер регулирования медицинских услуг. Жертв из числа представителей уязвимых групп могут привлекать незаконные агенты под фальшивыми предлогами и обещаниями, а затем таких доноров просто уговаривают или заставляют продавать свои органы.

Там, где появляются подпольные рынки, они способны быстро переплетаться с местными и транснациональными экономиками. Хотя деятельность морских пиратов у берегов Африканского Рога, например, за последние два года существенно сократилась, но пираты, выбирающие в качестве целей крупные суда международных компаний и действующие на удалении нескольких сот километров от берега, заявляют о том, что за период с апреля 2005 года по декабрь 2012 года их доходы в виде выкупов составили от 339 до 413 млн. долл. США. Было установлено, что эти преступные доходы перетекают не только к самим пиратам и финансирующим их лицам, но и в местные общины.

Еще одной отличительной чертой процессов глобализации является их *неразрывная связь с современными технологиями*. По мере того, как растут и ширятся взаимные связи национальных экономик, развивается процесс интеграции знаний и установления связей, основанных на нерыночных механизмах, в том числе информационного, культурного, идеологического и технологического обмена. Продвигать этот процесс со столь ошеломляющей скоростью продолжает глобальная Интернет-связь… Компьютерные технологии и Интернет стали источником множества социально-экономических выгод. Однако, такие технологии, равно как и другие средства активизации человеческого общения, могут направляться и на цели преступной деятельности, а с ростом глобальных сетей связи неразрывно связано распространение современной киберпреступности. По мере того, как растет киберпространство, все труднее представляется, что компьютерное преступление, а, возможно, и любое другое преступление, происходит без подключения к сети Интернет с помощью соответствующего протокола (IP).

В плане криминогенной перспективы один из основных постулатов состоит в том, что с появлением «киберпространства» формируются новые преступные явления, отличные от тех возможностей, которые напрямую доступны для преступной деятельности через компьютер. Например, некоторые лица в силу своего статуса и положения могут пойти на преступления в киберпространстве, хотя в условиях физического пространства они вряд ли отважились бы на нечто подобное. Возможность использовать гибкую идентичность, анонимность и отсутствие сдерживающего фактора также могут служить побудительными мотивами для преступного поведения в киберпространстве.

В случае киберпреступности правонарушители могут получить доступ к огромному количеству целей путем активного использования онлайновых услуг, таких как банковское обслуживание, шопинг, социальное взаимодействие и обмен файлами, превращающих пользователей в возможные объекты «фишинга» или мошенничества. Те охранные меры, которые существуют на самом деле, такие как защитные программные средства и относительно небольшой риск правоохранительных мер, недостаточны для того, чтобы остановить преступника, мотивированного соблазном значительно обогатиться.

Через глобальную связь расширяется действие фактора, способствующего укреплению преступного сообщества и обмену опытом между теми индивидами, которые в ином случае, возможно, никогда бы и не соединились. «*Социализация» уголовных элементов* через сети может привести к появлению различных форм криминальных «контактов» и установлению

связей между преступными группировками. Например, онлайновый «кардинг» или форумы «кардеров» содействуют обмену данными о похищенных кредитных картах. Места проведения онлайновых законных рынков, а также связанные с ними онлайновые дискуссионные советы обеспечивают проведение форумов не только с целью продажи полученных преступным путем товаров, но обмена информацией о поддержании режима анонимности и ухода от внимания правоохранительных органов.

В вопросах сексуального надругательства и сексуальной эксплуатации детей сеть Интернет предлагает сейчас правонарушителям беспрецедентный доступ к социальным сетям для оправдания своих поступков. Если в доцифровую эпоху правонарушители, открыто осмелившиеся обсуждать тему сексуального надругательства над детьми, подверглись бы остракизму со стороны большинства членов общества, теперь же возникли онлайновые сообщества, целью которых является нормализация отношений и создание ложного представления о приемлемости преступных деяний для общества. Такая социальная поддержка может быть особенно сильной в силу ее незамедлительного действия и интерактивного характера.

Таким образом, *информационно-коммуникационные технологии способны стимулировать новые и появляющиеся формы преступности по многим направлениям.* С одной стороны они вводят новые объекты криминальных деяний (иначе говоря, лица, предметы или ценности, против которых направлено правонарушение), такие как компьютерные данные и компьютерные системы. С другой стороны, они также привнесли с собой радикальные изменения в характер, уровни и способы совершения преступлений, считающихся устоявшимися.

Например, финансовое мошенничество в потребительской сфере стало транснациональным и обыденным в силу использования пластиковых кредитных и банковских карт для онлайновых платежей. Подстрекательство к насилию и терроризму в глобальных сетях, в том числе через социальные медийные средства, значительно расширяет сферу охвата и влияния террористических групп, ранее считавшихся локальными. Высокие уровни анонимности, предлагаемые системой «даркнет», включая серверную услугу в виде так называемой «*луковой маршрутизации*» (Tor), способны радикально влиять на торговлю запрещенными наркотическими средствами и другой продукцией, поскольку они сведут вместе транснациональных покупателей и продавцов в одном онлайновом рынке, на котором расчеты совершаются анонимно с помощью виртуальных платежных средств, а покупки доставляются почтой.

В этом смысле новые информационные технологии создают для преступлений эффект «*глокализации*» и анонимности, в силу которого имманентные связи между глобальными и локальными процессами привносят в данное локальное пространство новые категории виктимизации. С точки зрения правоохранительной практики, глобальная связь не только влияет на локальную криминальную практику, но и меняет характер взаимоотношений между глобальным и локальным поведениями. Технологии анонимизации, такие как Tor, могут стать соблазном для тех правонарушителей, которые раньше могли и не заниматься криминальной деятельностью, а также создавать значительные трудности для правоохранительных органов при выявлении правонарушителей.

Новые способы совершения преступлений

Новые и появляющиеся формы организованной преступности можно также классифицировать путем идентификации не только их коренных причин и способствующих факторов, но и по использованию существующих новых и особых преступных методов. Последние включают изменения в структуре организованных преступных групп и повышение активности взаимодействия между преступниками, а также использование коррупции для оказания содействия совершаемым правонарушениям.

Сегодня появилась гораздо более широкая разновидность организованных преступных групп, действующих в ряде случаев совместно с новыми формами транснациональной преступности. Например, в опубликованном в 2012 году издании УНП ООН *Digest of Organized Crime Cases* была представлена информация о возможном существовании различных по структуре криминальных группировок, в том числе групп, действующих по типу организованных банд, смешанных по составу групп, об участии в преступных операциях приглашаемых членов и о связях между преступными группами и группами террористов или полувоенных формирований, а также о сетях, действующих на основе создаваемых ячеек, и о комплексных сетях. Представление о повышении текучести структурных образований можно составить также на основе событий, происходящих в других регионах, в частности на примере того, как жесткая конкуренция между преступными группами сменяется договоренностями между ними по типу контрактных соглашений, достигаемых с помощью неформальных межличностных связей и общности экономических интересов.

В частности, Интернет предоставляет хорошие возможности для налаживания координации усилий отдельных исполнителей, разбросанных по данному географическому региону, открывая возможности для создания преступных сообществ с целью «концентрации» сил на кратковременном отрезке времени. В киберпреступной среде «черные» рынки, создаваемые для торговли данными о банковских и кредитных картах, характеризуются как социальные сети индивидов, участвующих в организованной преступной деятельности, а не как предприятие одной преступной группы[18]. На таких рынках группы и индивиды играют разные, а нередко и множественные, роли, в том числе роли программистов, распространителей информации, технических экспертов, хакеров, мошенников, провайдеров услуг в режиме онлайн, кассиров, курьеров для перевозки денег и лидеров.

Вместо того чтобы полагаться на установленные долговременные сети, преступные группы, участвующие в новых формах преступной деятельности, могут нанимать специалистов для выполнения задач, решение которых недоступно знаниям и навыкам членов существующей группы. Таким путем профессиональная, постоянно развивающаяся, опирающаяся на сервис преступная индустрия стимулирует появление инновационных орудий и методов, применяемых преступниками. Традиционные организованные преступные группы, включая те из них, которые организованы по типу мафии, начинают, например, прибегать к услугам киберпреступного рынка, являющегося по своему характеру сервисной структурой, с тем чтобы подготовиться к реализации технически более сложных преступных схем, покупая доступ к техническому опыту, в котором они нуждаются. Эта тенденция на приобретение черт киберпреступности в рамках более переходной, транзакционной и менее структурированной организационной модели может служить примером того, как в будущем будет осуществляться организация всех серьезных преступлений.

Действительно возросшая способность групп обеспечивать организацию и мобилизацию криминальных ресурсов, а также нанимать специалистов на краткосрочной основе в кратчайший срок ведет к появлению новых взаимосвязей между установившимися и появляющимися формами преступной деятельности. Например, что касается транснационального оборота наркотических средств, то было установлено, как одна преступная группа наняла на двухлетний срок, начиная с середины 2011 года, специальных хакеров для обеспечения оборота запрещенных наркотических средств через один европейский порт. Путем проникновения в компьютерные системы порта с помощью вредоносных компьютерных программ, засланных через электронную почту сотрудников порта, злоумышленники помогли организованной преступной группе получить доступ к информации о месте нахождения и системе охраны контейнеров порта, а также закамуфлировать свою противоправную деятельность.

Хотя роль современных технологий в преступной деятельности, несомненно, повышается, тем не менее, использование таких устоявшихся методов, как *подкуп и коррупция*,

по-прежнему придает особый характер способам совершения преступлений, относящихся к новым и появляющимся формам преступности. В частности, незаконный оборот и передвижение через границу нередко осуществляется с помощью подкупа местных должностных лиц. Так, например, при незаконном трансграничном перемещении токсичных или электронных отходов факт коррупции может происходить в момент выдачи уведомлений об отгрузке или сопроводительных документов, когда государство импорта соглашается на отгрузку, или в ряде контрольно-пропускных пунктов на границе.

Оборот человеческих органов во многих случаях зависит от того, удалось ли преступным группам наладить взаимодействие со специалистами в области медицины, готовыми заниматься пересадкой органов или подделывать медицинские сведения в обмен на незаконное вознаграждение. Как представляется, в данном случае ни один из способов совершения преступлений не является доминирующим. Скорее всего, различные формы коррупции могут существовать по всей цепочке донорства и трансплантации органов и действовать по-разному по отношению к живущим и умершим донорам. Коррупция может способствовать преступному замыслу, например, в процессе получения и распределения органов, нерегулируемого или нелегального удаления органов или при трансграничном перемещении реципиентов донорских органов или даже самих органов, предназначенных для пересадки.

В других случаях коррупция может не только оказывать воздействие на новые формы преступности, но и получать от них содействие. Например, в случае преступлений, связанных с использованием личных данных, коррупция может способствовать хищению персональных данных путем активного или пассивного подкупа должностных лиц с целью получения подлинных идентификационных документов, принадлежащих другому лицу, или путем изменения информации для того, чтобы создать или узаконить вымышленное лицо. С другой стороны, преступление, связанное с хищением личных данных, может использоваться в качестве средства, помогающего избежать опознания при коррупционных деяниях. Фальшивые личные данные могут использоваться, например, для того, чтобы воспрепятствовать проведению расследований таких правонарушений, как хищение активов или отмывание доходов от новых и появляющихся форм преступности.

Преобразование факторов, способствующих появлению новых форм преступности, в новые меры противодействия

Хотя глобализация считается, например, одним из стимуляторов новых и появляющихся форм преступности, вместе с тем она предлагает множество возможностей для усиления на транснациональном уровне мер противодействия со стороны правоохранительной системы и системы уголовного правосудия. Так, например, скоростные средства транспорта и связи могут способствовать развитию сетей формального и неформального международного сотрудничества между правоохранительными органами, прокурорами и центральными органами власти. Основными платформами для обмена информацией о появлении новых форм преступности и подготовке кадров по мерам предупреждения и ответного реагирования служат такие новые сети сотрудничества, как Прокурорская сеть стран Центральной Америки по борьбе с организованной преступностью и Сеть центральных органов и органов прокуратуры стран Западной Африки по борьбе с организованной преступностью.

Аналогичным образом, если в процессе появления новых рынков и расширения межрыночных связей могут возникнуть бреши в системе регулирующих режимов и сформироваться подпольные экономики, то одновременное углубление понимания этого процесса поможет созданию особых возможностей для мер противодействия. Так, например, *Международные руководящие принципы принятия мер в области предупреждения преступности и уголовного правосудия в отношении незаконного оборота культурных ценностей и других, связанных с*

ним преступлений считают важной борьбу с незаконной торговлей культурными ценностями с помощью рыночных мер, таких как введение или улучшение статистического учета ввоза и вывоза культурных ценностей, создание механизмов, позволяющих сообщать о подозрительных сделках или торговых операциях в сети Интернет; введения или разработки инвентарных описей и баз данных по культурным ценностям и поощрение учреждений культуры и частного сектора в отношении сообщений о подозрительном обороте культурных ценностей. Такие инициативы, как разработанная УНП ООН/Всемирной таможенной организацией (ВТО) *Программа по контролю за контейнерными перевозками*, дополнительно призваны минимизировать использование морских контейнеров для незаконного оборота с помощью анализа рисков и характеристики контейнеров, направленного на противодействие незаконному обороту в условиях крупносерийного, высокоинтенсивного грузооборота.

Точно так же и в области технологий современные достижения, которые открывают перед преступниками новые возможности, в свою очередь предлагают и новые средства для ведения расследований. Тот огромный объем информации, которая доступна как на открытых сайтах социальных сетей и чат-форумах или которая хранится на переносных электронных устройствах, таких как смартфоны, и которая может быть изъята правоохранительными органами при проведении специальных операций, служит новым источником данных, а зачастую и важным отправным моментом для проведения следственных действий. Хотя правонарушители смогут использовать такие методы, как шифрование информации, система Tor или анонимные виртуальные платежные средства для проведения незаконных сделок, эти технологии эффективны лишь тогда, когда за ними стоит «человеческий фактор». Многие проводимые правоохранительными органами расследования в конечном итоге завершаются успешно благодаря обнаружению непредумышленно оставленных преступниками улик, указывающих на наличие связей между «анонимной» информацией, ассоциируемой с уголовно-правовым правонарушениями, и идентифицирующей информацией в виде адресов IP или адресов электронной почты. Правоохранительные органы могут также воспользоваться современными технологиями для гарантированного обмена информацией и упреждающего перехвата данных или для использования технических средств наблюдения с санкции суда или дистанционно управляемых летательных систем при проведении таких операций, как противодействие браконьерству.

Инновационные методологии сбора данных

Эффективность мер, проводимых в отношении любой категории преступлений, в огромной степени зависит от доказательной базы. Это же верно и в отношении новых и появляющихся форм преступности. Однако когда речь идет о новых преступлениях, сложный характер таких преступлений в сочетании с разным набором способов совершения преступлений чрезвычайно затрудняет применение традиционных источников данных, таких как полицейские сводки. *Многие новые формы преступности часто не попадают в поле зрения полиции*, тем самым увеличивая показатель «темной статистики преступлений», и затрудняя полицейской учет, требующий увязки деяний, попавших в поле зрения полиции, с такими явлениями, как новые и появляющиеся формы преступности.

Подходы к восполнению этого пробела могут включать такие меры, как использование той или иной комбинации источников данных, включая политическую статистику, промежуточные показатели, в частности изъятые данные о запрещенных товарах, результаты опросов ключевых осведомителей и пользователей рынков и новые источники информации, такие как системы географической информации и продукты компьютерной безопасности.

Вполне возможно, что в будущих работах такие концепции, как «*большие данные*» и «*информационный выхлоп*» будут представлять собой критически важные информационные источники для отображения характера и масштабов новых форм преступности. Эти концепции

опираются на идею мониторинга информационных моделей, которые генерируются в рабочем порядке, но которые могут меняться в зависимости от необходимости реагирования на некоторые уголовно-правовые события. Например, в области морского пиратства отклонение того или иного судна от запланированного курса, определяемое с помощью географических информационных систем, будут служить одним из ранних свидетельств, указывающих на попытку угона или ограбления. Что касается преступлений против дикой природы и лесных угодий, то изменения в привычных географических схемах кормления или миграции редких и исчезающих видов могут указывать на нарушение запрета на браконьерскую деятельность или операции по установке ловушек на животных. В сфере киберпреступности с помощью данных автоматического реагирования, генерируемых программными средствами обеспечения компьютерной защиты, можно получать информацию о характере и возможных географических источниках компьютерных атак.

В основе всех усилий по сбору данных лежит идея создания эффективного потенциала для статистического учета данных и их анализа, причем в первую очередь на национальном уровне, а затем на региональном и глобальном уровнях. В самом деле, транснациональный характер многих новых преступлений требует, чтобы сбор данных не ограничивался только наиболее затронутыми в этой связи странами. На примере незаконного оборота редких и исчезающих видов дикой природы видно, что хотя основной вред может причиняться в стране происхождения, любые всеобъемлющие и сбалансированные меры противодействия требуют понимания всей цепочки незаконного оборота, характера участвующих в нем рынков и применяемых данными преступными группами способов для совершения преступлений, а также детальных сведений о связанных с ним финансовых потоках во всех задействованных странах, включая страны происхождения, транзита и назначения. Для принятия эффективных мер по предупреждению, перехвату и противодействию для борьбы с новыми формами преступности чрезвычайно важно обеспечить обмен собираемыми данными между всеми участвующими секторами и странами.

Укрепление национального законодательства, международного сотрудничества и правоохранительного потенциала

…Во многих странах новые и появляющиеся формы преступности, возможно, недостаточно охватываются существующим уголовным законодательством, или же во многих случаях они могут быть кодифицированы как противозаконные деяния, но фрагментарно или же могут регулироваться исключительно административным правом. Например, в совместном исследовании по проблеме договорных матчей и незаконной букмекерской деятельности, проведенном УНП ООН и Международным олимпийским комитетом, было установлено, что законодательное регулирование мер борьбы с новыми преступными явлениями может быть достигнуто либо путем применения или адаптации существующих норм права, либо путем принятия новых нормативных актов…

…Что касается национальных подходов к криминализации киберпреступной деятельности, то в рамках *Всеобъемлющего исследования по киберпреступности* было установлено, что для этого используется несколько правовых подходов. Например, в отношении деяний, совершаемых против компьютерных систем и данных, существует тенденция ставить их под запрет в рамках кодификации конкретных правонарушений, таких как неправомерный доступ или неправомерное вмешательство в компьютерные системы или данные, в то время как в отношении деяний, связанных с функционированием компьютерных систем, таких как компьютерные правонарушения, относящиеся к махинациям с личными данными, существует тенденция объявлять их вне закона через правовые нормы об общих правонарушениях…

…На глобальном уровне гармонизация законодательства по предупреждению появляющихся форм преступности и борьбе с ними может быть достигнута несколькими путями. Некоторые конкретные области регулируются посредством международных договоров. Примерами таких договоров, касающихся причинения вреда окружающей среде, являются Конвенция 1973 года о международной торговле видами дикой фауны и флоры, находящимися под угрозой уничтожения, и Базельская конвенция 1989 года по контролю за трансграничной перевозкой опасных отходов и их удалением. Договорами, касающимися незаконного оборота культурных ценностей, являются Конвенция 1954 года о защите культурных ценностей в случае вооруженного конфликта и два протокола к ней, а также Конвенция 1970 года о мерах, направленных на запрещение и предупреждение незаконного ввоза, вывоза и передачи права собственности на культурные ценности. Однако такие инструменты, возможно, не всегда требуют принятия законодательства по всем аспектам указанного явления. Например, стороны Конвенции о международной торговле видами дикой фауны и флоры, находящимися под угрозой исчезновения, обязаны в законодательном порядке ввести уголовные наказания в отношении нелегальной трансграничной торговли видами дикой природы, но отнюдь не в отношении внутренней торговли. Стороны Конвенции о мерах, направленных на запрещение и предупреждение незаконного ввоза, вывоза и передачи прав собственности на культурные ценности, обязались «ввести уголовные или административные санкции» в отношении лиц, нарушающих запрет на вывоз культурных ценностей без специального свидетельства на экспорт, а также на ввоз культурных ценностей, похищенных из музея или религиозного и светского исторического памятника или подобного учреждения другого государства-участника, при условии, что имеется документальное подтверждение того, что такие ценности принадлежат данному учреждению. Другие виды преступлений, такие как киберпреступность, подделка лекарственных средств и оборот человеческих органов, не регулируются юридически обязательными международными нормами права, но могут подпадать под действие некоторых региональных международно-правовых документов[17].

В тех случаях, когда юридически обязательных правовых стандартов не существует, гармонизация законодательства все-таки возможна через реализацию ряда мер, включая принятие юридически необязательных руководящих принципов, стандартов, рекомендаций или типовых законов, а также путем установления примеров оптимальной законодательной практики и оказания технической помощи. Так, например, в Международных руководящих принципах принятия мер в области предупреждения преступности и уголовного правосудия в отношении незаконного оборота культурных ценностей и других, связанных с ними преступлений предусматривается, что государствам следует рассмотреть вопрос о кодификации в качестве серьезных правонарушений целый ряд конкретных деяний, включая незаконный оборот культурных ценностей, хищение культурных ценностей и разграбление археологических и культурных памятников. В рамках своих усилий по борьбе с незаконным оборотом поддельных лекарственных препаратов УНП ООН приступило к разработке типовых законодательных положений. Аналогичным образом, разработка типового законодательства по преступлениям с использованием личных данных могла бы дополнительно помочь тем государствам-членам, которые хотели бы руководствоваться сводом типовых положений при подготовке эффективных мер противодействия.

В целом, применение уголовно-правовых мер для противодействия новым и появляющимся формам преступности может быть наиболее эффективным в том случае, если такие меры сохраняют баланс между конкретными законодательными положениями, которые имеют своей целью преступное поведение и/или на участвующие в обороте товары или рынки (в слу-

[17] См., например, Конвенцию Совета Европы против торговли человеческими органами, Конвенцию Совета Европы о манипуляции спортивных соревнований и Конвенцию Совета Европы по борьбе с преступлениями в киберпространстве.

чае незаконного оборота), и достаточно уверенной правовой определенностью, сохраняя при этом гибкость, достаточную для учета возможных будущих явлений. Если в государстве за подобные преступления существует наказание в виде лишения свободы на срок не менее четырех лет и если такие государства являются участниками Конвенции Организации Объединенных Наций против транснациональной организованной преступности, то проведению транснациональных расследований подобных преступлений могут помочь положения этой Конвенции, при условии, что расследуемое преступление является транснациональным по характеру и совершено с участием организованной преступной группы.

Но даже в тех случаях, когда гармонизация законодательства была проведена и когда международное сотрудничество может опираться на такие документы, как Конвенция против организованной преступности, все еще могут оставаться значительные трудности. Например, в области киберпреступности тот факт, что данные и онлайновые сделки все шире переходят на модель подключения двух абонентов через распределенные по цепочке промежуточные компьютеры, означает, что, прежде всего, невозможно будет определить одно государство или группу государств, к которым можно было бы обратиться с запросом о помощи в рамках международного сотрудничества. В таких случаях может все больше возникать потребность в новых формах сотрудничества, в том числе и в таких инновационных начинаниях, как взаимное признание следственных действий, а также меры по изменению концепции о роли традиционных, основанных на территориальном признаке понятиях суверенитета в контексте все расширяющихся глобальных электронных сетей.

С точки зрения потенциала правоохранительных органов расследование многих серьезных дел, относящихся к новым и появляющимся формам преступности, сопряжено с определенными техническими сложностями, создающими трудности даже для наиболее развитых и технически оснащенных государств, и представляет еще большие трудности для развивающихся стран и международного сотрудничества. Для проведения расследований, сбора и хранения доказательств необходимо проводить экспертно-криминалистический анализ информационно-коммуникационных технологий. Также важно хорошо знать, как функционируют законные финансово-экономические системы, бухгалтерский учет, методы отмывания денег и системы идентификации. Быстрое развитие методов криминалистики требует регулярного обновления учебных материалов и переподготовки должностных лиц.

Предупреждение

Одним из основных компонентов мер по предупреждению преступности является повышение уровня *разъяснительной работы среди потенциальных жертв* и других заинтересованных сторон. Появляющиеся формы преступности, как правило, гораздо сложнее многих обычных видов преступлений и порой могут иметь менее заметную клиентуру, которой должны быть адресованы разъяснительные меры. Тем не менее, этот принцип одинаково важен для всех. Информацию о характерных признаках, указывающих на возможность незаконного происхождения видов дикой природы и поддельных лекарственных препаратов можно доводить до сведения, например, торговцев и потребителей. Правительства и предприятия должны шире распространять информацию о принимаемых основных мерах по предупреждению преступности, таких как введение надежных паролей и осторожное отношение к приложениям, получаемым с электронной почтой – мерах, принимаемых с целью уменьшения угрозы киберпреступности. Не так давно УНП ООН, Всемирная туристическая организация и Организация Объединенных Наций по вопросам образования, науки и культуры провели совместную информационно-разъяснительную компанию, целью которой было убедить международных туристов не принимать участия в преступлениях, совершаемых против дикой природы, в обороте культурных ценностей, и изготовлении поддельных продуктов, в обороте людей и

незаконном обороте наркотических средств. Многие подобные информационно-разъяснительные инициативы, включая механизмы сообщения о возможных преступлениях или потерпевших, могут возникать как следствие партнерских отношений между государством и бизнесом.

Сообщения также могут рассылаться *лицам, подвергающимся риску стать участниками появляющихся форм преступности*. В Сомали инициативы по предотвращению преступности были адресованы молодым людям, с тем чтобы отговорить их от поступков, толкающих их на путь пиратства. Через общинных лидеров, политиков и религиозных деятелей в Пунтленде антипиратские послания распространялись в медийных средствах и на общих собраниях жителей, а сами акции дополнялись усилиями по организации для жителей района возможностей для получения альтернативных средств жизнеобеспечения. Информацию о добросовестной практике, которая может способствовать предотвращению преступлений, важно распространять среди потребителей даже на базовом уровне. Например, в Китае в рамках одной из инициатив используются программные обеспечения на основе сети Web с целью в зародыше пресечь нелегальную утилизацию и последующую реализацию сдаваемой в утиль электронной техники. С помощью этой компьютерной программы пользователи могут загружать фотографии своих старых электронных устройств и получать за них деньги по расчетной цене. После этого организуется сбор таких электронных средств покупателем, который гарантирует их правильную утилизацию.

В сфере усилий по профилактике преступлений одинаково важно разрабатывать политику, направленную на устранение уязвимых проблем, заставляющих отдельных лиц и группы населения совершать деяния, относящиеся, прежде всего, к новым формам преступности. Например, деяния преступного характера в отношении окружающей среды и пиратство могут совершаться исключительно ради получения средств жизнеобеспечения для правонарушителей и их семей. Целью таких подходов может быть расширение доступа населения к альтернативным источникам доходов для лиц, находящихся в зоне риска, и лишение преступных синдикатов возможности вербовать местных жителей; что в результате позволит сократить расходы на содержание системы уголовного правосудия и избежать серьезных последствий в виде тюремного заключения для отдельных лиц, их семей и общества в целом.

Наконец, новые технологии могут также играть особую роль в связи с использованием их в ходе профилактики, в частности для организации визуального наблюдения и принятия дополнительных мер защиты возможных целей. Например, на американском континенте и Ближнем Востоке некоторые страны используют *пилотируемые системы с дистанционным управлением для картирования, мониторинга и охраны археологических памятников, помогая предотвращать риски разграбления культурных ценностей*. Новые технологии могут также играть решающую роль в предотвращении производства и распространения поддельных медицинских препаратов. Законным изготовителям, оптовикам, аптекам и логистическим компаниям предоставляется возможность еще шире использовать технологии отслеживания и контроля по цепочке движения продукции, снабжаемой для этого защитной маркировкой и средствами идентификации. Эта система позволяет заинтересованным сторонам во всех точках вдоль цепи распределения идентифицировать медицинские препараты и устанавливать их подлинность, равно как и легитимность торговых партнеров, а также облегчает проведение расследований и изъятие препаратов, попавших под подозрение.

Следующее поколение появляющихся форм преступности и глобальная повестка дня в области развития

С уверенностью можно сказать, что *появляющиеся сегодня формы преступности уже не будут таковыми завтра*. Вполне вероятно, что процессы глобализации и технологического развития будут и далее ускоряться и продолжать играть определенную роль в части стимули-

рования криминальных инноваций. Вместе с тем, и другие явления, в том числе изменение климата, развитие биоинженерии, нехватка водных ресурсов, виртуальные платежные средства, широкое распространение «краудсорсинга» и децентрализация общественных ценностей и услуг, новые формы энергетики, такие как термоядерная реакция, достижения в области робототехники, создания автономных систем и искусственного интеллекта, могут в общем и целом стимулировать появление новых рынков, возможностей, коренных причин и факторов, способствующих росту масштабов преступности, а также использованию новых приемов противоправной деятельности, влияющих на ее распространение.

Для того чтобы противостоять этому вызову, потребуется постоянно уделять пристальное внимание общечеловеческим факторам, лежащим в основе многих форм противоправной деятельности, включая необходимость постоянно прилагать усилия для борьбы с коррупцией и сокращения ее масштабов, для обеспечения населения стабильными средствами на жизнь и решения проблемы нищеты и социального неравенства. Вместе с тем, вполне вероятно, что *инновации в социально-экономической сфере необходимо будет дополнять своевременным применением надлежащих мер регулирования, а также предусмотреть включение в них «специальных мер по предотвращению»*, с тем чтобы уменьшить возможности для преступных проявлений. В общем и целом, завтра потребуются всеобъемлющие и сбалансированные меры противодействия новым и появляющимся формам преступности, с тем чтобы с помощью глобальных, новаторских, системных и координируемых инициатив в области предотвращения преступности и уголовного правосудия пресекать появление преступных инноваций…

Укрепление мер реагирования систем предупреждения преступности и уголовного правосудия на появляющиеся формы преступности, такие как киберпреступность[18]

Киберпреступность. Определение проблемы

В 1994 году в *Руководстве Организации Объединенных Наций по предупреждению преступности, связанной с применением компьютеров, и борьбе с ней* было отмечено, что «потенциальная сфера охвата компьютерной преступности так же широка, как и сфера охвата международных телекоммуникационных систем». Хотя в Руководстве слово «Интернет» употребляется только один раз, что, возможно, не вызывает удивления, а слово «киберпреступность» вообще не употребляется, содержащиеся в нем выводы являются весьма дальновидными. Хотя основное внимание в Руководстве уделяется понятию «компьютерное преступление», уже широко признано, что сегодняшняя киберпреступность действительно опирается на глобальные информационно-коммуникационные технологии, в частности на Интернет, которые используются для совершения преступных деяний транснационального масштаба.

Помимо развития терминологии предпринимались научные усилия, с тем чтобы сформулировать определение термина «киберпреступность». Современный подход заключается в признании того факта, что *киберпреступность является не исключительно техническим юридическим термином, а скорее сводным термином для указания на все деяния, совершенные против компьютерных данных или систем или с помощью их использования*. В рамках других подходов основное внимание уделяется преступлениям против компьютерной информации или использованию информационных ресурсов в незаконных целях.

Деяния, которые обычно относят к категории «киберпреступности», включают такие деяния, при которых объектом преступления являются компьютерные данные или системы, а также деяния, при которых использование компьютерных или информационных систем является неотъемлемой частью способа совершения преступления. Примеры первых включают преступления против конфиденциальности, целостности и доступности компьютерных данных и систем, такие как получение незаконного доступа к компьютерным данным или системам (иногда именуемые «основными» киберпреступлениями). Примеры последних включают использование компьютерных данных или систем для мошенничества, хищения или причинения вреда другим лицам и преступления, связанные с использованием компьютеров и интернет-контента, включая пропаганду ненависти, детскую порнографию, преступления с использованием личных данных и продажу запрещенных товаров в режиме онлайн[16].

Однако в целом граница между киберпреступностью и обычной преступностью становится все более размытой. По мере все более широкого применения в повседневной жизни электронных устройств и систем подключения к глобальным сетям использование электронных доказательств, таких как текстовые сообщения, сообщения по электронной почте, данные просмотра сети Интернет и данные социальных сетей, становятся обычным делом при проведении многих обычных уголовных расследований. Используемые в таких случаях цифровые средства судебной экспертизы и запросы к поставщикам электронных услуг, а также многие трудности и эффективные методы расследований часто такие же, как и при расследовании

[18] Справочный документ XIII Конгресса ООН по предупреждению преступности и уголовному правосудию (Доха, 12–19 апреля 2015 г., A/CONF.222/12) (Извлечение)

дел, связанных с киберпреступлениями. Таким образом, хотя в настоящем документе основное внимание уделяется деяниям, которые принято относить к киберпреступности, многие положения и выводы имеют более широкое применение в отношении электронных доказательств в целом.

Основным фактором, способствующим как повышению уровня современной киберпреступности, так и более активному использованию электронных доказательств, является развитие систем подключения к глобальным сетям. В настоящее время насчитывается почти 3 миллиарда пользователей Интернета, на долю которых приходится около 40 процентов всего населения мира.

Хотя такой быстрый рост числа пользователей Интернета и компьютерных технологий способствовал экономическому росту и расширил доступ к таким жизненно важным услугам, как образование, здравоохранение и электронное управление, он также открыл новые возможности для преступной деятельности. Такие инструменты киберпреступности, как «ботнеты» (производный термин от английских слов «robot» (робот) и «network» (сеть)), например, могут состоять из глобальных сетей, включающих десятки или сотни тысяч устройств потерпевших, каждое из которых инфицировано вредоносной программой, которая может дистанционно контролироваться преступниками. Сайты социальных сетей могут в течение нескольких секунд задействоваться на глобальном уровне для преступных домогательств, пропаганды ненависти, угроз насилием, вымогательства или распространения частной информации, принадлежащей отдельным лицам. Поскольку преступники стремятся также сделать своей мишенью «интернет-вещи», мировой потенциал преступной деятельности может еще больше увеличиться.

Помимо глобального характера проблемы в последнее десятилетие происходило циклическое повышение степени анонимности, предлагаемой Интернетом, в результате чего его стали использовать при совершении преступных деяний. Первые годы своего существования Интернет, согласно широко распространенному мнению, был в значительной мере анонимным, по крайней мере в той степени, в какой пользователи не понимали технических возможностей отслеживания онлайновой активности на уровне отдельных лиц. Однако в последние годы системы уголовного правосудия стали более привычными к таким понятиям, как IP-адреса и журналы соединений, а также использование судебных приказов для получения данных от поставщиков электронных услуг. В результате этого электронные следы, оставляемые пользователями Интернета, стали все более доступными для следователей, хотя получение данных может потребовать значительного времени и усилий. Кроме того, прогресс в разработке цифровых средств судебной экспертизы, включая устройства судебной экспертизы, которые работают в режиме автоматической настройки и просты в использовании, облегчил рутинный анализ данных, хранящихся в таких цифровых устройствах, как компьютеры и смартфоны.

Технологии постоянно совершенствуются, и при использовании современных средств судебной экспертизы и методов расследования киберпреступлений возникают проблемы, которые нельзя было предвидеть еще десять лет назад. Например, бесплатное и широко доступное программное обеспечение позволяет осуществлять 256-битное шифрование отдельных файлов и целых устройств хранения данных. Без пароля или кода зашифрованные таким образом данные практически недоступны для правоохранительных органов. Еще более совершенное 2048-битное шифрование представляет собой сегодня теоретически непреодолимую преграду. Наряду с обычным Интернетом функционируют новые децентрализованные сети обеспечения анонимности, часто называемые «темной паутиной». Такие услуги, как «луковый» маршрутизатор (Tor), крайне затрудняют возможность определения многими правоохранительными органами источника электронных сообщений или идентификацию веб-сайтов, оказывающих «скрытые услуги». Такие скрытые услуги могут использоваться для анонимного размещения незаконных онлайновых рынков сбыта наркотиков, оружия или детской порнографии. Неко-

торые из этих сетей предлагают также возможность децентрализованного хранения зашифрованных данных в участвующих сетевых «узлах». Электронные документы или изображения, хранящиеся таким образом, опять-таки практически недоступны для правоохранительных органов. Последствия таких технологий для деятельности правоохранительных органов носят серьезный характер и затрагивают вопрос о том, каким образом можно лучше всего обеспечить соответствие правоохранительных мер реагирования динамике появления новых форм киберпреступности.

Оценка уровня киберпреступности

Один из подходов к оценке новых форм и масштабов преступности, включая киберпреступность, требует использовать сочетание таких мер, как получение информации о преступниках, информации о движении средств на незаконных рынках и информации о количестве преступных событий, причиненном вреде и убытках и обусловленных этим незаконных финансовых потоках. Применительно к киберпреступности в этих целях можно использовать ряд источников данных. К ним относятся полицейские статистические данные о зарегистрированных преступлениях, обследования населения и предприятий, инициативные сообщения потерпевших и информация об использовании технологий по обеспечению кибербезопасности. К дополнительным источникам относятся также такие методы, как краулинг URL-адресов и поглощение «ботнетов».

Хотя статистические данные о зарегистрированных полицией киберпреступлениях нельзя не учитывать, ясно, что они в значительной степени носят ограниченный характер, поскольку большинство случаев виктимизации не доводятся до сведения полиции. В глобальном плане правоохранительные органы могут использовать разные статистические методы и подходы, что затрудняет международное сопоставление данных. Кроме того, общий уровень зарегистрированных полицией киберпреступлений в существенной степени зависит от численности личного состава специальных полицейских подразделений, в связи с чем статистические данные могут указывать на масштабы полицейских расследований, а не на лежащий в их основе уровень виктимизации, связанной с киберпреступностью.

Важными альтернативными источниками информации являются обследования по вопросам виктимизации физических лиц и предприятий. Обследования показывают, что для населения в целом уровень виктимизации в результате киберпреступности существенно выше, чем уровень виктимизации в результате «обычных» форм преступности. Показатели виктимизации в результате мошенничества с кредитными картами в режиме онлайн, хищения личных данных, ответов на попытку фишинга и несанкционированного доступа к учетным записям электронной почты составляют от 1 до 17 процентов среди пользователей Интернета в 21 стране мира, в то время как типичные показатели в отношении краж со взломом, ограблений и угонов автомобилей составляют для этих же стран не более 5 процентов. Предприятия частного сектора в Европе сообщают об аналогичных показателях виктимизации. Например, в Европе предприятия сообщают о показателях виктимизации в размере от 2 до 16 процентов в отношении таких деяний, как нарушение данных в результате несанкционированного доступа или фишинга.

Данные обследований, которые включают информацию о финансовых потерях в результате киберпреступности, можно использовать для составления оценок последствий киберпреступности. В ходе одного исследования потерпевшие потребители в 24 странах сообщили о том, что за один год средние прямые потери в результате киберпреступлений составили от 50 до 850 долларов. В рамках еще одного исследования на основании данных ряда обследований была сделана оценка, что мировые прямые и косвенные издержки, связанные с совершением нескольких видов киберпреступлений, а также издержки по защите от них, включая такие пре-

ступления, как банковское мошенничество в режиме онлайн, мошенничество с платежными картами в режиме онлайн и мошенничество с авансовыми платежами, составляют ежегодно сотни, если не тысячи миллионов долларов.

Анализ рынков киберпреступности также позволяет оценить характер и масштабы некоторых форм киберпреступности. В рамках одного из таких подходов основное внимание уделяется анализу онлайновых форумов, которые функционируют как преступные «социальные сети» в целях сбыта и покупки социальных товаров и обмена информацией преступного характера.

В ходе проведенного в 2011 году исследования использовались данные, полученные на шести подпольных интернет-форумах, содержащих свыше 2500000 постов и 900000 частных сообщений от более чем 100 000 пользователей. В числе наиболее распространенных объектов торговли были кредитные карты, данные о банковских счетах и инструменты, используемые при совершении мошенничества. Анализ потока сообщений на 13 веб-форумах показывает, что списки данных об украденных картах предлагаются в режиме онлайн по средней цене 100 долл. США, а такие запрещенные устройства, как сканеры кредитных карт можно приобрести по средней цене в 2 400 долларов США. Новые исследовательские технологии также позволяют осуществлять вебкраулинг скрытых услуг «тор». Это может облегчить систематическое выявление и категоризацию количества и видов «темных» веб-сайтов, посвященных таким темам, как незаконная продажа наркотиков, детская порнография, продажа оружия или орудий совершения киберпреступлений.

И наконец, определение категорий преступников способствует пониманию характера и методов деятельности основных преступных организаций. Весьма вероятно, что соответствующего стандартного «профиля» не существует. Сравнительно небольшое число высококвалифицированных программистов и хакеров могут способствовать появлению новых видов киберпреступности и предлагать свои услуги в преступных целях. Вместе с тем широкая доступность эксплойтов и вредоносных программ означает, что многие преступники уже больше не нуждаются в глубоких знаниях. Для совершения различных видов киберпреступлений также требуется большое количество рядовых «пехотинцев». В рамках недавней схемы мошенничества с предоплаченными дебетовыми картами, одна организованная преступная группа наняла сотни людей в 26 странах, благодаря чему в двух отдельных случаях было произведено свыше 40000 одновременных снятий денежных средств в банкоматах. Согласно оценкам, было похищено 45 млн. долларов США[29]. Хотя *свыше 80 процентов киберпреступлений могут быть связаны с организованной преступностью*, ясно, что широкая типология групповой структуры, в том числе наличие преступных объединений с произвольной структурой, затрудняет любую прямую характеризацию лиц, совершающих киберпреступления.

Предупреждение киберпреступности и борьба с ней

Важным компонентом при разработке эффективных стратегий предупреждения и расследования киберпреступлений является информация об их характере и масштабах.

Национальная политика, стратегия и законодательство, касающиеся киберпреступности, являются важным отправным пунктом определения основ и приоритетов в области борьбы с киберпреступностью. Онлайновое хранилище данных о киберпреступности УНП ООН, которое начнет функционировать в 2015 году, будет содержать подробные данные о национальных стратегиях в 50 странах, охватывающих такие области, как повышение осведомленности о киберпреступности, международное сотрудничество, потенциал правоохранительных органов, законодательство, предупреждение и публично-частное партнерство. Внутреннее законодательство о киберпреступности часто охватывает целый ряд областей, включая криминализацию, следственные полномочия, юрисдикцию, электронные доказательства и международное

сотрудничество. Обзор внутреннего законодательства о киберпреступности свидетельствует о том, что уголовная ответственность за совершение киберпреступлений устанавливается на основе сочетания положений, касающихся как только киберпреступлений, так и в целом общеуголовных преступлений. Уголовная ответственность за совершение «основных» киберпреступлений, таких как получение незаконного доступа к компьютерным данным и системам, может устанавливаться путем принятия специального законодательного положения, в то время как деяния, связанные с применением компьютеров для получения личной или финансовой помощи или причинения личного или финансового вреда, чаще всего могут признаваться уголовно наказуемыми на основе положений, касающихся совершения общеуголовных (не связанных с применением компьютеров) преступлений.

В некоторых случаях внутренние нормативно-правовые основы принимаются во исполнение или с учетом многосторонних документов, которые могут быть обязательными или необязательными для сторон. К таким документам относятся Конвенция о кибербезопасности и защите личных данных Африканского союза, Соглашение о сотрудничестве государств – членов Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации, Конвенция Совета Европы о киберпреступности, Директива 2013/40/EU Европейского парламента и Совета Европейского союза об атаках на информационные системы, Конвенция о борьбе с преступлениями в области информационных технологий арабских государств и Соглашение о сотрудничестве в области обеспечения международной информационной безопасности Шанхайской организации сотрудничества.

Помимо положений, касающихся криминализации и процессуальных полномочий, существующие документы могут также содержать положения о механизмах международного сотрудничества при трансграничном расследовании киберпреступлений и преследовании за их совершение. В этой области правоохранительные органы сталкиваются с растущими проблемами. Появление технологий «облачных» вычислений и децентрализованных сетей обмена информацией и средств хранения означает, что, несмотря на теоретическую невозможность идентификации местонахождения конкретного компьютера в конкретный момент времени, соответствующие данные могут существовать в нескольких копиях, распространяться между многими устройствами и местами нахождения и переноситься в другое географическое местоположение в течение нескольких секунд.

Некоторые поставщики услуг по хранению данных, например частные поставщики электронных услуг или услуг, связанных с «облачными» технологиями, могут быть по закону обязаны хранить копии данных в течение определенного срока и будут, как правило, предоставлять данные правоохранительным органам на основании судебного приказа или другой соответствующей юридической процедуры. Однако если поставщик услуг или данные находятся за пределами юрисдикции, в которой проводится расследование, то такие юридические процедуры часто связаны с использованием государствами официальных и длительных процедур оказания взаимной правовой помощи. В случае использования других методов хранения данных, например при хранении данных физическими лицами в децентрализованных компьютерных сетях, выявление данных в исходном месте может быть затруднено, при этом нередко данные хранятся в зашифрованном виде. Для обеспечения сохранности данных и их получения, возможно, потребуются меры принуждения в отношении соответствующего физического лица.

В настоящее время на международном уровне ведутся дискуссии относительно современной и основанной главным образом на принципе территориальности модели транснациональных расследований киберпреступлений и доступа к данным. В некоторых существующих многосторонних документах предусмотрены механизмы, направленные на облегчение доступа к данным для правоохранительных органов, таких как круглосуточные контактные центры по обеспечению помощи в расследовании киберпреступлений, оперативное обеспечение сохран-

ности данных, трансграничный доступ к хранящимся компьютерным данным с соответствующего согласия или к общедоступным данным и срочные просьбы об оказании взаимной помощи. На практике очевидно, что даже при наличии таких механизмов многие правоохранительные органы сталкиваются со значительными трудностями при получении своевременного доступа к экстерриториальным данным в ходе расследования киберпреступлений. В то же время необходимо в достаточной степени обеспечить соблюдение прав человека, принципа верховенства права и гарантий неприкосновенности частной жизни, с тем чтобы доступ правоохранительных органов к данным был определенным, предсказуемым, пропорциональным и находящимся под надлежащим контролем.

Оптимизации процессов оказания взаимной правовой помощи, касающихся электронных доказательств, могут способствовать такие нововведения, как включение модуля по электронным доказательствам в переработанную Программу составления просьб об оказании взаимной правовой помощи Управления Организации Объединенных Наций по наркотикам и преступности (УНП ООН). Вместе с тем одновременно с этим правоохранительные органы могут испытывать растущую потребность в нахождении новаторских методов сотрудничества в области проведения транснациональных расследований киберпреступлений. Особенно важным в этом отношении может оказаться участие в координации поддержки транснациональных расследований таких структур, как *Глобальный инновационный комплекс Интерпола и Европейский центр по борьбе с киберпреступностью (ЕЦК) Европейского полицейского управления (Европол)*.

Участники партнерских отношений в области предупреждения киберпреступности и борьбы с ней, будь то на многостороннем или национальном уровне, должны также включать *частный сектор*. Ключевую роль в предупреждении киберпреступности могут также играть поставщики интернет-услуг и хостинговых услуг. Они могут хранить учетные журналы, которые можно использовать для расследования преступной деятельности, оказания помощи потребителям в применении безопасных онлайновых методов и выявлении взломанных компьютеров, блокирования некоторых видов вредоносного контента и в целом для обеспечения в интересах потребителей защищенной коммуникационной среды. Существует ряд моделей публично-частного партнерства, например, между правоохранительными органами и поставщиками электронных услуг. Многие из них базируются на обмене информацией на основе четких правил, доверия, ограниченного членства и поощрения взаимной выгоды и ответной реакции. В некоторых случаях отраслевые коллективные органы, такие как Исследовательский альянс кибербезопасности, служат платформой для взаимодействия промышленности с правительствами в области кибербезопасности и борьбы с киберпреступностью.

И наконец, важнейшую роль играет наращивание потенциала на уровне национальных правоохранительных органов и систем уголовного правосудия. Хотя большинство стран приступили к созданию специализированных структур для расследования киберпреступлений и преступлений, связанных с электронными доказательствами, во многих странах эти структуры не получают достаточного финансирования и страдают от отсутствия достаточных возможностей. Поскольку цифровые доказательства все шире используются при расследовании «обычных» преступлений, правоохранительным органам, возможно, необходимо проводить четкое различие между возможностями следователей по киберпреступлениям и возможностями лабораторий по судебной экспертизе цифровых доказательств, а также установить для них четкую сферу ответственности. Оперативные сотрудники правоохранительных органов, возможно, также испытывают растущую потребность в приобретении и использовании базисных навыков, таких, которые используются для составления обоснованного экспертно-криминалистического описания устройств для электронного хранения данных.

Поскольку при совершении киберпреступлений широко используются новые технические достижения, такие как анонимные сети, высокая степень шифрования и виртуальные

валюты, следователям придется также руководствоваться новыми стратегическими подходами. Например, правоохранительным органам, возможно, следует активизировать партнерские отношения с научно-исследовательскими группами, которые уделяют основное внимание разработке технических методологий в таких областях, как характеристика и анализ операций с виртуальной валютой. Следовательно, возможно, также необходимо рассмотреть вопрос о том, каким образом специальные методы расследования, такие как слежка, тайные операции, использование осведомителей и проведение контролируемых поставок в случае продажи запрещенных товаров в режиме онлайн, могут использоваться вместе с интернет-расследованиями и методами цифровой судебной экспертизы. В целом очевидно, что расширение возможностей правоохранительных органов и учреждений уголовного правосудия в области борьбы с киберпреступностью будет постоянно развивающимся процессом в силу стремительного появления технических инноваций и новых форм преступности.

Анализ перспектив организованной преступности[19]

ВВЕДЕНИЕ

Основные тенденции развития тяжкой и организованной преступности

Упадок традиционных иерархических преступных группировок и сетей будет сопровождаться расширением **виртуального преступного мира, включающего индивидуальных криминальных предпринимателей**, которые используют свой опыт и знания в рамках в различных незаконных схемах. Такой динамичный криминальный рынок уже действует в сфере киберпреступности, но в будущем также будет распространяться на области «традиционной» организованной преступности, такие как оборот наркотиков, организация нелегальной иммиграции или подделка товаров. На этом **раздробленном и глобальной** криминальном рынке преступники-конкуренты будут сотрудничать в рамках отдельных операций.

Преступники будут меньше полагаться на стабильные иерархические группировки, которые легко могут стать мишенью для правоохранительных органов. Они будут стремиться диверсифицировать свою преступную деятельность, специализируясь при этом выбранных направлениях. Преступники, как объединенные в группы, так и одиночки будут организовывать свою преступную деятельность **наподобие сферы услуг**, что облегчается существованием социальных сетей, обеспечивающих достаточно безопасную и анонимную среду общения. В погоне за новыми клиентами, организованная преступность будет неизменно стремиться изменить ассортимент предоставляемых товаров и услуг, переходя от традиционных к более новым.

Почти все виды организованной преступной деятельности будет опираться на **цифровые инфраструктуры**. Торговля незаконными товарами и обмен денег будут происходить в виртуальном пространстве, требующем минимального личного взаимодействия между торговыми партнерами и снижающем риск обнаружения и пресечения. Виртуальные валюты позволят организованным преступным группировкам анонимно обмениваться средствами и использовать финансовые ресурсы в беспрецедентных масштабах, без необходимости использования сложных и дорогостоящих схем отмывания денег. Некоторые преступники будут оказывать узкоспециализированные услуги поставок для относительно небольших групп клиентов. Эти услуги могут включать в себя **проникновение** в системы управления или физическое проникновение в компании с помощью сложного мошенничества с личными данными и использования перехваченной в сети информации.

Тяжкая и организованная преступность будет ориентироваться на наиболее уязвимые общественные группы с целью эксплуатации и нахождения новых потребителей незаконных товаров и услуг. Тем не менее, в ближайшее десятилетие **методы преступной деятельности и целевые группы, выбираемые в качестве жертв и клиентов, будут меняться**. Сильнее всего это затронет пожилых людей, число которых растет. Преступники стремятся эксплуатировать пожилых людей и предлагают им специально подобранные услуги. Изменение маршрутов миграционных потоков может повлечь рост вывоза граждан ЕС на развивающиеся рынки для трудовой и сексуальной эксплуатации. **Гораздо активнее, чем раньше, преступники будут стремиться использовать легальные коммерческие структуры**, как в

[19] Доклад Европола. Exploring tomorrow's organized crime. Report Europol, 2 March 2015 (Извлечение)

качестве жертв преступлений и в качестве инструментов для обеспечения своей преступной деятельности.

Факторы	Перспективы тяжкой и организованной преступности:
• Транспорт и логистика • Нанотехнологии и роботехника • Данные как товар • Электронные отходы • Рост соперничества за природные ресурсы • Распространение виртуальных валют • Демографические изменения в ЕС	• Глобальная виртуальная криминальная среда, в которой действуют независимые преступники • Организация преступной деятельности как сферы услуг и диверсификация товаров и услуг • Использование цифровых инфраструктур, виртуальных валют и проникновения в легальные организации • Ориентация на новые целевые группы потенциальных жертвы: пожилые люди и легальные коммерческие структуры

Ключевые факторы изменений

• Инновации в **транспорте и логистике** позволят ОПГ совершать преступления анонимно через Интернет в любое время и в любом месте без необходимости физического присутствия

• **Нанотехнологии и роботехника** открывают новые рынки для организованной преступности и обеспечивают новые инструменты для сложных криминальных схем.

• Более активное использование **Больших данных** и личных данных позволит ОПГ осуществлять сложные мошенничества с личными данными в беспрецедентных масштабах.

• **Электронные отходы** могут стать ключевым незаконным товаром для европейских ОПГ

• **Экономическое неравенство** в Европе повышает социальную толерантность к ОПГ, которые все глубже проникают в экономику ослабленных стран, выставляя себя в качестве провайдеров работы и услуг.

• ОПГ будут все активнее пытаться проникнуть в сектора экономики, связанные с **природными ресурсами**, выступая в качестве брокеров и торговых агентов.

• **Виртуальные валюты** облегчают преступникам деятельность в качестве независимых предпринимателей, организующих свою преступную деятельность по принципу сферы услуг и не нуждающихся в сложных криминальных инфраструктурах для получения и отмывания доходов.

• ОПГ будут все более ориентироваться на эксплуатацию **пожилых людей**, число которых растет и предоставление им незаконных товаров и услуг.

1. НЕОБХОДИМО НОВОЕ ОПРЕДЕЛЕНИЕ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ

Изменение криминальной ситуации в Европе

Организованная преступность остается одним из вызовов для правоохранительных органов, отвечающих за защиту граждан Европейского Союза. ОПГ так же разнообразны, как

и рынки, на которых они работают, и деятельность, которую они осуществляют. Во многих случаях они отражают общество, культуру и систему ценностей, из которых они возникли. Поскольку общества в Европе становятся все более взаимосвязанными и интернациональными по характеру, современная организованная преступность также является взаимосвязанной и действует в международном масштабе. Структурированные группировки, с которыми обычно ассоциируется организованная преступность, размываются, уступая место свободно организованным криминальным сетям, состоящим из отдельных криминальных предпринимателей, ведущих свой бизнес в общей и часто цифровой криминальной среде. Во введении показывается перспектива развития организованной преступности в ЕС, на фоне которой следующих главах будут обсуждаться ключевые факторы ее развития.

Экономические и социальные перемены, обусловленные миграцией, различиями, становлением мультикультурного общества, демографическими изменениями, а также технологическими инновациями, влияют на характер ОПГ и отдельных преступников. Беспрецедентные социально-экономические перемены в Европе за последние 70 лет поставили под вопрос традиционные системы ценностей. Это особенно заметно на примере утраты чувства коллективизма у европейцев и росте и развитии индивидуализма.

ОПГ действуют на рынке криминальной экономики, регулируемом законами спроса и предложения, и используют толерантное отношение общества к таким типам преступлений как торговля контрафактными товарами и мошенничество в отношении государственных органов и крупных компаний. Эти факторы продолжают оказывать влияние на характер организованной преступности. Границы между законной и незаконной деятельностью становятся более размытыми, и дать определение организованной преступности становится все сложнее. Отдельные преступники и преступные группировки проявляют гибкость и быстро приспосабливаются к ситуации, выбирая новые жертвы, нейтрализуя принимаемые в отношении них меры или находя новые криминальные возможности. Политические и законодательные перемены, такие как заключение новых соглашений о свободной торговле и дальнейшее расширение ЕС несомненно влияют на организованную преступность в ЕС. Однако, вступление в ЕС новых стран открывает правоохранительным органам новые возможности для сотрудничества и обмена информацией.

Ориентированный на услуги криминальный мир

Прогнозируемое развитие криминальных сетей, занятых «традиционной» организованной преступностью деятельностью, такой как оборот наркотиков или организация нелегальной иммиграции отражает эволюцию преступников и криминальных сетей, вовлеченных в киберпреступность. Компьютерные преступники уже действуют как развитая и очень динамичная, хотя и разобщенная часть онлайн сообщества.

В европейской организованной преступности все больше будут доминировать свободные, неоформленные и гибкие сети, состоящие из самостоятельных криминальных предпринимателей. Преступники работают в свободном режиме и больше не входят в крупные сети или группы. Объединяясь как провайдеры услуг для поддержки преступной деятельности в рамках проектов, они принадлежат к обширному преступному миру, деятельность которого сильно облегчается Интернетом.

Такие преступники все чаще будут образовывать сетевые объединения для планирования конкретной преступной деятельности или координации своего участия в осуществляемых криминальных проектах. До настоящего времени это относилось к киберпреступности, однако в дальнейшем рост рынков в сети с криминальными предложениями услуг будет распространяться и на традиционные формы преступности.

Анонимные рынки криминальных услуг в Интернете угрожают способствовать слиянию организованной преступности терроризма. Преступные деятели, не связанные с конкретной группировкой, предоставляющие услуги исключительно для получения прибыли, будут иметь меньше препятствий для сотрудничества с террористическими группировками. Радикализация и возвращение иностранных боевиков в ЕС также может повлиять на характер организованной преступности. Вернувшиеся и радикализованные экстремисты часто будут действовать в том же широком криминальном мире, что и преступные сети.

Организационная (корпоративная) преступность

В ряде случаев преступная деятельность считается социально-приемлемой, особенно когда она направлена на нарушение нормативных положений, которые считаются «чрезмерными» и направлена на повышение доходов от в остальном легальной деятельности.

Традиционно, корпоративные преступления не так активно преследовались правоохранительными органами, как другие виды преступной деятельности. Некоторые виды корпоративной преступности считались допустимыми как неизбежное условие ведения бизнеса, и не вызывали беспокойства, поскольку компании-нарушители обеспечивали занятость и вносили свой вклад в развитие национальной экономики. На организационную или корпоративную преступность обращали мало внимания и ее недооценивали. Однако, серия скандалов, включая корпоративные преступления, опубликованные в прессе в начале 2000-х гг., высветили масштабы и издержки подобной деятельности. Криминальная деятельность корпораций имеет место ничуть не реже других видов преступности. Борьба с организационной преступностью по-прежнему сопряжена с большими сложностями: компании и их руководство не хотят негативной известности, и поэтому подобные преступления часто остаются скрытыми от общества и от правоохранительных органов. Если бы не было инсайдеров-информаторов, многие случаи корпоративных преступлений выявлялись бы только при наличии большого числа потерпевших. Экономический кризис выявил серьезные и, в ряде случаев, преступные нарушения банков и предприятий, которые нанесли значительный экономический ущерб миллионам потерпевших. Хотя этот экономический ущерб обычно не был преднамеренным, умышленная недобросовестность и игнорирование финансовых правил в ряде случаев можно было квалифицировать как преступную деятельность. В результате суды США и Европы в ряде случаев наложили на нарушителей штрафы.

Расследование организованной преступности по-прежнему сопряжено со значительными трудностями. В настоящее время ведутся споры по поводу масштабов и точного характера организованной преступности, что требует дополнительных исследований и целевых расследований. Обсуждение проблем оценки корпоративной преступности с правовой и политической точек зрения осложняется необходимостью согласовывать потребности бизнеса с действующими нормативами. Во многих юрисдикциях роль правоохранительных органов в расследовании корпоративной преступности определена недостаточно четко.

Глобализация бизнеса, сопровождаемая экспоненциальным ростом прямых иностранных инвестиций и появлением действительно международных корпораций, еще сильнее затрудняет расследование корпоративных преступлений. Уже сейчас корпорации выбирают место регистрации с целью свести к минимуму налоги, и некоторые из них могут выбирать страны с более свободными нормами и социальной терпимостью к некоторым видам криминальной деятельности, что способствует принятой ими модели ведения бизнеса, предусматривающей использование определенных преступных схем.

Использование законодательства

Законодательство было и останется ключевым фактором, определяющим характер и масштабы организованной преступной деятельности в Европе. Законы, регулирующие иммиграцию, организацию системы социального обеспечения, налоги, торговлю, конкуренцию, защиту окружающей среды и многие другие области, определяют направления и характер деятельности ОПГ. Хотя в ЕС достигнут значительный прогресс в гармонизации некоторых сфер законодательства, влияющих на тяжкую и организованную преступность в некоторых государствах-членах, во многих областях права в разных государствах-членах действуют сильно различающиеся положения. Такие различия в законодательстве и распространение законодательства на всю территорию ЕС создает ниши и возможности для организованной преступности. ОПГ уже научились использовать специальные знания и опыт для организации сложных криминальных предприятий, занимающихся мошенничеством с НДС или нелегальным оборотом отходов. В перспективе ОПГ будут еще активнее изучать возможности использования несоответствий в законодательстве различных юрисдикций ЕС. Гармонизация системы уголовного правосудия не позволит преступникам скрываться от правосудия в той или иной юрисдикции. Определенная унификация на уровне ЕС уже осуществляется.

Однако, распространение различного законодательства в государствах-членах ЕС облегчает для преступников использование лазеек в законодательстве. Организационная преступность имеет возможность прибегать к услугам самых опытных юристов на коммерческом рынке, что создает все более серьезные проблемы для правоохранительных органов.

2. ОСНОВНЫЕ ФАКТОРЫ ПЕРЕМЕН И ИХ ВЛИЯНИЕ НА ТЯЖКУЮ И ОРГАНИЗОВАННУЮ ПРЕСТУПНОСТЬ

В ближайшие десятилетия организованная преступность претерпит глубокие и существенные изменения, вызванные доступностью новых технологий, экономических и социальных перемен, а также принимаемых правоохранительными органами мер. Эти изменения произойдут независимо от того, дадут ли эксперты новое определения организованной преступности, и правоохранительные органы должны серьезно рассматривать факторы и условия, определяющие развитие тяжкой и организованной преступности в ближайшем будущем.

Транспорт и логистика

Инновации в области транспорта и логистики позволят преступникам сохранять анонимность, совершая преступления в Интернете в любое время и в любом месте без физического присутствия.

ОПГ найдут новые и инновационные способы использования изменения организации транспорта, новых маршрутов и технологий. Новые технологии позволят быстро и часто незаметно перемещать крупные партии незаконных товаров. Поскольку транспорт и логистическая инфраструктура в большей степени полагаются на онлайн-системы и автоматизированные системы дистанционного управления, ОПГ, будут все больше зависеть от возможности проникновения в эти системы для манипулирования маршрутами перевозок, внедрения в цепочки поставок и сбора ценных и конфиденциальных данных.

Эти далеко идущие изменения в транспорте и логистике будут иметь значительное влияние на серьезную и организованную преступность. ОПГ будут искать возможности атаковать транспортные и логистические инфраструктуры и хабы или проникнуть в них для облегчения

своей преступной деятельности. Транспорт и логистика будет все больше зависеть от использования Больших данных и облачных сервисов, что сделает эти сектора мишенью для киберпреступности. Кибератаки уже угрожают цифровым системам частного и государственного сектора, а в перспективе станут реальной опасностью для физического существования коммерческих инфраструктур и активов. ОПГ, занимающиеся хищением грузов, станут использовать уязвимые места автоматизированных транспортных систем. Эти группы будут пытаться установить контроль над системами управления воздушным, железнодорожным или другими видами транспорта с целью изменить маршрут автоматичебских транспортных средств и похитить их груз. Это позволит преступникам совершать хищения дорогостоящих товаров без необходимости присутствия на месте преступления.

ОПГ будет все шире торговать данными, связанными с перевозками и логистикой, предоставляя ценную информацию другим преступникам или конкурирующим компаниям. Эти данные могут быть получены путем взлома и социальной техники, а также посредством физического проникновения компаний в сектор транспорта и логистики. Эти данные будет включать в себя конфиденциальную коммерческую информацию, персональные данные и интеллектуальную собственность, имебющую решающее значение для бизнеса компании. Аутсорсинг и предоставление услуг компаний в глобальном масштабе даст ОПГ еще больше возможностей проникать дальше в логистические цепочки, облегчая и маскируя деятельность, связанную с незаконным оборотом.

Изменения в транспортной и логистической инфраструктуре скажутся и на обороте нелегальных товаров, таких как наркотики, огнестрельное оружие, контрафакт, запрещенные отходы или охраняемые виды дикой природы. Некоторые криминальные рынки сместятся, уступая место новым маршрутам, центрам и новым криминальным рынкам. Также как и для легальных товаров, 3D-печать вызовет перемещение производства запрещенных товаров ближе к потребительским рынкам. Это особенно вероятно для контрафактных товаров, оружия и наркотиков, и может повысить значение оборота сырья, включая незаконных прекурсоров.

Направление и типы потоков незаконных товаров будут меняться. Использование ранее недоступных маршрутов через Арктику будет влиять на глобальные потоки контрабанды путем в глобальном масштабе, таких как наркотики или исчезающие виды дикой природы. Благодаря хорошо развитой транспортной инфраструктуре и появлению новых рынков в Азии, ЕС, скорее всего, станет ключевым транзитным регионом для различных нелегальных товаров, соединяя места происхождения и назначения по всему миру. Экспоненциальное расширение электронной торговли приведет к дальнейшей активизации оборота и торговли незаконными товарами на глобальном уровне. Использование беспилотных автоматизированных транспортных средств для незаконного оборота товаров позволит преступникам поддерживать лишь виртуальную связь со своей преступной деятельностью. Установление или даже простое выявление подозреваемых станет серьезной проблемой для правоохранительных органов.

ОПГ, организующие незаконную миграцию и торговлю людьми, будут стремиться использовать в своих интересах изменения в системе транспорта и логистики. Преступники и жертвы воспользуются диверсификацией транспортных возможностей. Незаконных мигрантов, возможно, будут перевозить на автоматических беспилотных транспортных средствах сухопутным путем, по воде или по воздуху, так что мигранты не будут непосредственно контактировать с преступниками. Преступники будут стремиться научиться или нанимать специалистов для взлома систем управления транспортом, чтобы установить контроль над перевозками. Основные горячие точки, а также маршруты нелегального въезда в ЕС изменятся в результате перемен в демографии и экономической ситуации стран происхождения и транзита. По мере роста привлекательности стран Азии для мигрантов ЕС может превратиться для них в транзитный регион или даже регион происхождения. Эти процессы могут также затронуть

торговлю людьми ее жертвы. Аутсорсинг и краудсорсинг в секторе логистики с целью уменьшения расходов может открыть новые возможности для эксплуатации рабочей силы.

Крупные суммы денег, связанные с транспортными и логистическими проектами в области исследований и развития, инфраструктуры и производства, будут, скорее всего, активно привлекать финансовую и экономическую преступность. ОПГ будет искать возможности развернуть мошенничество и коррупцию в тендерах, государственно-частном партнерстве и в инфраструктурных проектах. Контролировать сложные цепочки поставок с участием нескольких видов транспорта станет сложнее. Повышенные меры безопасности, как в отношении цепочки поставок, так и таможни, скорее всего, приведут к задержкам в обработке транзитных грузов, которые могут спровоцировать рост попыток коррупции, с целью ускорения процедуры оформления. Логистические компании будут предоставлять дополнительные консультации по таможенным процедурам и возможностям обойти правила. Некоторые ОПГ будет специализироваться на предоставлении услуг, связанных с упрощением транспортных операций и разработки бизнес-моделей для получения значительной прибыли от обхода процедур.

Фундаментальные изменения в области транспорта и логистики в мировом масштабе также изменят характер ОПГ эксплуатирующих эти отрасли. Большая мобильность позволит преступникам совершать преступления в любом месте, в любое время, быстро и незаметно. Краудсорсинговые приложения будут способствовать преступной деятельности. Например, навигационные приложения, использующие данные пользователей в реальном времени для поиска наиболее эффективных маршрутов, облегчат преступникам уклонение от правоохранительных внимание. Такие технологии, как использование Больших данных, дистанционный взлом, взлом роботов и автоматизированных систем могут обеспечить ОПГ поистине глобальный охват при использовании ограниченного числа технических специалистов и поддержании низкого профиля на месте преступления.

ОПГ, как правило, требуют более высокого уровня знаний для незаконного использования полученных данных в целях своей преступной деятельности. Они должны будут привлекать людей, имеющих опыт в области информационных технологий или использования ресурсов посредством аутсорсинга внешних экспертов для конкретных видов деятельности. Переход к проникновению в системы управления перевозками и логистикой, скорее всего, сделает насилие нехарактерным инструментом для действующих в этой сфере ОПГ, за исключением случаев выяснения отношений с сообщниками и конкурентами.

Данные как товар

Более широкое использование Больших данных и личных данных позволит ОПГ проводить сложные мошенничества с личными данными на беспрецедентном уровне.

На продажу: ваши данные

Расширение Больших данных и появление Интернета, связывающего устройства, процессы и данные привело к резкому увеличению качества и количеств личных данных, собираемых частными компаниями, государственными органами и преступниками. Ожидается, что личные данные будут становиться все более важным товаром, они будут повсеместно собираться и использоваться при получении услуг в коммерческом секторе. Преступники также будут их использовать при оказании своих услуг, а также для совершения мошенничества. Все более распространенные беспроводные соединения различных изделий, таких как автомобили, бытовые приборы и одежда, получившие название «Всеохватывающий Интернет» создают гораздо более широкие возможности для сбора данных о пользователях. Предпочтительные продукты, режим дня, состояние здоровья и местонахождение будут, скорее всего, постоянно

регистрироваться при использовании таких изделий. Кроме того, современное использование Интернета и смартфонов показывает, что пользователи уже готовы делиться своими персональными данными, такими как знакомства, трудовая деятельность и фотографии с третьими лицами. Ожидается, что их публикация станет все более частой по мере распространения устройств, требующих ввода личных данных от своих пользователей. Законодатели столкнуться с проблемой обеспечения права пользователей на конфиденциальность и, скорее всего, сосредоточатся не на профилактике, а на регулировании вопросов сбора, распространения и коммерциализации информации.

Данные, пассивно собираемые потребительскими товарами и активно вводимые пользователями, используются производителями товаров и часто продаются рекламным агентствам. Помимо распространения информации через подключенные к сети устройства, ожидается также расширение сбора биометрических данных. Процесс сбора и обработки биометрических данных станет менее дорогостоящим. Государственные органы и частные компании будут использовать биометрическую информацию в самых разных целях, в том числе в технологиях идентификациях, формировании социальных сетей на основании генетического сходства, использовании генетической информации для определения склонности к определенным заболеваниям и установления стоимости медицинской страховки.

Скимминг частных данных

Расширение сбора и повышение значимости биометрических и личных данных создаст много возможностей для серьезной и организованной преступности. Киберпреступники уже сейчас могут получать большие объемы информации о своих потенциальных жертвах. Личные данные получают главным образом путем проникновения в сети или перехвата коммуникаций. Однако преступники могут целенаправленно атаковать базы данных, принадлежащие производителям и рекламным агентствам. Похищенные из этих источников данные могут продаваться другим преступным группировкам, специализирующимся на различном мошенничестве. Для них будут представлять интерес сведения об интересах, структуре социальных сетей и финансовые данные. Более того, растущая взаимосвязанность позволит преступникам создавать шпионские программы для наиболее распространенных товаров, таких как автомобили, холодильники или нагреватели.

Также подвержены хищениям данные, связанные с дистанционным банкингом и кредитными картами. Технология радиочастотной идентификации, позволяющая совершать покупки, прикладывая карту к радиочастотному считывающему устройству, уже используется в Европе, чаще всего в магазинах и кафе, поскольку облегчает и ускоряет совершение платежа. Это создает возможности для нового вида мошенничества с использованием считывающих устройств для копирования данных с карт. При этом карта не обязательно должна использоваться и даже может быть скопирована через кошелек или одежду. Члены ОПГ могут посещать людные места, такие как транспортные узлы или крупные магазины и использовать скрытые считывающие устройства для сбора данных о картах, принадлежащих проходящим мимо людям. Затем эти данные будет использоваться или продаваться другим группировкам. Ожидается, что финансовый сектор примет меры для предупреждения такой кражи данных, хотя масштабы принятия этих мер могут различаться. Если бесконтактные платежи получат большее распространение, ожидается использование таких мер, как противоскимминговое покрытие карт или кошельков.

Хотя современные технологии не позволяют эффективный мобильных кошельков, преступники могут разработать коммуникационные технологии, считывающие финансовые данные с мобильных телефонов. Затем эти данные будут использоваться так же, как и полученные в результате бесконтактного скимминга.

Мошенничество с использованием личных данных станет более сложным в результате развития технологий сбора личных и биометрической информации. Поскольку использование биометрических данных становится широко распространенным, вполне вероятно, что базы данных, хранящие эту информацию, станут мишенью для преступников. Распространение биометрических данных в качестве средства аутентификации в перспективе может сделать онлайн-сервисы более безопасным. Тем не менее, взломанные биометрические данные могут также представлять дополнительные риски. Традиционные механизмы аутентификации, такие как пароли или фразы, могут быть изменены пользователями, если они подозревают, их счета были скомпрометированы. Биометрические данные неизменны по своей природе, и их попадание к киберпреступникам может быть гораздо более серьезные последствия, чем взлом паролей. Биометрические данные часто считается исключительно надежными для аутентификации. Их хищение может предоставить преступникам доступ к физическим структурам, а также к конфиденциальной информации.

Опытные группы киберпреступников уже предоставляют полный набор похищенных личных данных для заинтересованных покупателей, как правило, для использования при совершении различных махинаций. В будущем, этот пакет данных будет содержать еще более полную информацию, включая биографические данные, личные данные, фотографии, информацию о кредитных картах и биометрические данные человека. Ожидается, что торговля незаконно полученной информации будет расширяться по мере роста заинтересованности преступников в таких данных. ОПГ смогут извлечь выгоду в различных областях преступности из этих более полных похищенных личных данных. ОПГ, занимающиеся организацией нелегальной иммиграции и торговлей людьми, смогут использовать эти данные, чтобы обеспечить нелегальных мигрантов и жертв торговли людьми новыми личными данными в комплекте со всей необходимой информацией, чтобы избежать рисков или обойти правоохранительные контрмеры при проникновении в ЕС или во время последующих перемещений. Точно так же, ОПГ, занимающиеся оборотом наркотиков с риска. Некоторые ОПГ будет предоставлять специализированные пакеты личных данных на заказ, с учетом конкретных методов ОПГ в различных областях преступности. Например, ОПГ, занимающиеся торговлей исчезающими видами дикой природы, могут заказать личные данные, связанные с научно-исследовательскими учреждениями для того чтобы перевозить исчезающие виды, используя специальные разрешения, выдаваемые только для научно-исследовательских целей.

Нанотехнологии и роботехника

Нанотехнологии и роботехника откроют новые рынки для организованной преступности и создадут новые инструменты для сложных криминальных схем.

Нанотехнологии и преступность

Роботехника и нанотехнологии влияют также на тяжкую и организованную преступность. Растущая зависимость производства и здравоохранения от роботов создает уязвимость, которая может быть использована преступниками. Способность осуществлять хакерские атаки рабочей силы фабрики или больницы открывает новые возможности для компьютерного вымогательства. Однако необходимый для этого высокий уровень технической компетентности делает маловероятным широкое использование таких схем ОПГ. Ожидается, что подобные преступления будут совершаться в политических целях, и заниматься этим будет небольшое число высококвалифицированных специалистов-одиночек. Роботы-исполнители могут также использоваться правоохранительными органами во всех сферах их деятельности, например при контроле дорожного движения, наблюдении или обезвреживании взрывных устройств.

Сложность и дороговизна нанотехнологий создают серьезный барьер как для правоохранительных органов, так и для ОПГ. Жизненно важно, чтобы правоохранительные органы выделили необходимые средства и врем для получения знаний, необходимых для ответа на угрозы, связанные с нанотехнологиями, а также для использования возможностей, открывающихся в этой сфере. Поскольку ожидается, что нанотехнологии станут такими же распространенными, как и персональные компьютеры, отсутствие внимания правоохранительных органов к данной новой проблеме создаст «белое пятно», которое используют ОПГ.

ОПГ, имея необходимые средства, могут использовать нанотехнологии для разработки или модификации психоактивных веществ. Они могут воспользоваться преимуществами растущего рынка нанотехнологий для изготовления контрафактных наркотиков или устройств. Нанотехнологии могут также помочь правоохранительным органом, повышая чувствительность и эффективность специальных технических устройств. Эффективность и быстрота криминалистического анализа места преступления и оставленных преступниками следов резко возрастут, поскольку нанотехнологии ускорят анализ ДНК и повышают возможности исследования отпечатков пальцев и следов крови.

Электронные отходы

В отсутствие необходимых законодательных и правоохранительных мер незаконная торговля электронными отходами резко вырастет в ближайшем будущем, как в отношении объемов, так и в отношении качества методов, используемых преступниками, занятых в этой сфере.

Золотые отходы

За последние 30 лет объем отходов в Европе резко вырос. В то время, как количество бытовых и промышленных отходов быстро растет и вызвало развитие крупной и сложной индустрии утилизации отходов, один из видов отходов сочетает в себе беспрецедентный потенциал роста с товарной ценностью – речь идет об электронных отходах.

Все более широкое использование техники в самых различных сферах жизни ведет ко все большему распространению электронных устройств в домашнем хозяйстве, на работе и в общественных местах. Технический прогресс, с которым связано устаревание и частая замена потребительских товаров, сокращает срок жизни электронных устройств, обусловливает экспоненциальный рост электронных отходов в виде выброшенных устройств и их частей. Проблеме роста числа устаревших электронных приборов посвящены многочисленные статьи; поскольку растущие рынки Китая, Индии, Бразилии предъявляют все больший спрос при неуклонном сокращении срока службы электронных устройств. Даже по осторожным оценкам общее число устаревших компьютеров и телефонов в развивающихся регионах станет больше, чем в развитых к 2017 г. В 2012 г. объем электронных отходов оценивается в 48,9 млн. т.[7] Это на 15,2 % больше по сравнению с объемом мировых электронных отходов в 2011 г.[8] Даже если темпы роста объема электронных отходов сохранятся на нынешнем уровне, к 2017 г. объем электронных отходов может достичь от 65,49 до 93,510 млн. т.

При этом такие оценки не могут учитывать появление новых технологий. Например, еще 10 лет назад трудно было предположить, что спрос на смартфоны и планшеты превысит спрос на стационарные компьютеры. В результате в будущем это может привести к еще более активному образованию электронных отходов.

Возможно, за последние 50 лет технический прогресс больше, чем любой другой фактор поддерживал экономический рост, формировал индустриальное общество и оказывал сильное

влияние на окружающую среду. Электронные отходы являются одним из побочных продуктов такого развития и в перспективе угрожают стать одним из ключевых криминальных товаров.

Ключевой нелегальный товар будущего

Торговля отходами – не новое явление. Такие преступные группировки как итальянская мафия и восточноевропейские ОПГ давно вовлечены в незаконный бизнес по «утилизации отходов». Традиционно, оборот отходов включал утилизацию бытовых и промышленных отходов по ценам, ниже чем у легальных операторов, с нарушением законодательства, по защите окружающей среды и обеспечению добросовестной конкуренции.

Объем электронных отходов в следующем десятилетии должен увеличиться и ОПГ будут все более активно пытаться использовать этот ресурс. Распространение электронных приборов, содержащих драгоценные металлы и такие материалы как золото, серебро, никель и палладий уже превратило электронные отходы в ценный товар, торговля, бартер и оборот которого уже осуществляются в мировом масштабе, подобно другим незаконным товарам – таким как наркотики, огнестрельное оружие и исчезающие виды дикой природы. Основными факторами, превращающими электронные отходы в ключевой незаконный товар, являются объем и доходность. Эти два элемента создают динамический цикл, связанный с дефицитом материалов, необходимых для производства электронных товаров повседневного спроса, спрос на которые растет во всем мире, и с изобилием электронных отходов, содержащих эти драгоценные ресурсы.

ОПГ уже глубоко вовлечены в оборот и торговлю электронными отходами, которые обещают значительные прибыли, а в случае разоблачения грозят лишь довольно умеренными штрафами. При этом, экспоненциальный рост объема электронных отходов может превратить их в основной криминальный товар, соперничающий с наркотиками по объему оборота и прибыли.

В настоящее время электронные отходы из ЕС часто переправляются в Западную Африку и в Индию. Расширение рынка электронных отходов может сопровождаться диверсификацией регионов их переработки. Это может привести к незаконной переработке некоторой части электронных отходов в Европе. Подобно тому, как сейчас синтетические наркотики незаконно производятся в подпольных лабораториях, ОПГ могут создать предприятия по переработке электронных отходов, нанося серьезный ущерб окружающей среде и создавая риск для местного населения.

Африка и Азия, в частности, сами становятся крупными источниками электронных отходов, и переработка этих отходов может стать важной отраслью местной промышленности. Влияние развитой глобальной транспортной инфраструктуры на организованную преступность уже было описано в отдельной главе настоящего доклада. Очевидно, однако, что поставки через континенты все более крупных партий отходов привлечет внимание организованной преступности.

ОПГ могут также пытаться извлекать доходы из электронных отходов, получаемых из других источников, помимо бытовых электронных приборов. Солнечные батареи получают все большее распространение в качестве источника энергии и либо изначально предусматриваются в проектах новых сооружений, либо добавляются в ходе осуществления проектов модернизации. Несмотря на широкое распространение солнечных батарей в ЕС, цикл их переработки и утилизации должным образом не организован[11]. Организованная преступность уже вложила значительные средства в производство «зеленой энергии» и организовала различные схемы мошеннического получения субсидий, имея прямой доступ к предприятиям зеленой энергетики через различные легальные коммерческие структуры. ОПГ, скорее всего, попытаются извлекать доходы от торговли отработанными элементами инфраструктуры зеленой энер-

гетики, поскольку многие из этих установок содержат те же самые металлы и ресурсы, которые можно найти в других электронных изделиях.

Торговля и оборот электронных отходов будут все больше привлекать ОПГ в ЕС и за его пределами. Без необходимых законодательных и правоохранительных мер незаконная торговля электронными отходами может резко вырасти в ближайшем будущем как с точки зрения объемов, так и в отношении методов, используемых преступниками, вовлеченными в этот бизнес. Незаконная переработка электронных отходов опасна для окружающей среды и уже нанесла ей существенный ущерб. Она также вредит здоровью населения, подвергающегося воздействию токсических побочных продуктов переработки. Организованная преступная деятельность по торговле электронными отходами представляет серьезную криминальную угрозу и вызов для государств-членов ЕС, которые должны развивать партнерство в глобальном масштабе, чтобы предотвратить превращение электронных отходов ключевой криминальный товар будущего.

Экономическое неравенство в ЕС

Экономическое неравенство в Европе повышает толерантность общества к организованной преступности, поскольку ОПГ активно действуют в экономически отсталых регионах и выступают как работодатели и провайдеры услуг.

Влияние на организованную преступность

ОПГ будущего смогут приспосабливаться и быстро использовать происходящие изменения, особенно в экономике, находя новые рынки, предлагая новые услуги или разрабатывая новые способы действия. Рост среднего класса в странах с развивающейся экономикой, таких как Китай, Индия, Бразилия и Россия, создаст новые возможности для серьезной и организованной преступностью. Этот средний класс представляет собой обширный рынок для незаконных товаров, а также является потенциальным объектом как легальных, так и нелегальных инвестиций и мишенью для профессиональных мошенников. Средний класс развивающихся стран будет представлять собой рынок до 2 млрд. дополнительных потребителей к 2030 г. В настоящее время на менее чем 1 миллиард человек приходится три четверти мирового потребления. Ожидаемое массивное расширение глобальной потребительской базы вызовет значительное увеличение спроса на все виды товаров и услуг, как легальные, так и нелегальные. ОПГ смогут извлечь из этого выгоду в целом ряде различных областей преступности, включая торговлю наркотиками, торговлю контрафактной продукцией, мошенничество с НДС, акцизное налоговое мошенничество, мошенничество с предоплатой и мошенничество с платежными картами.

Между тем, снижение благосостояния в некоторых частях Европы может заставить ОПГ адаптироваться к потребительской базе, которая способна тратить меньше на незаконные товары, которые они предлагают. Рынок наркотиков по-прежнему будет обусловлен динамикой соотношения между стоимостью и оценкой потребителей, а также наличием наркотиков у поставщиков. Тем не менее, доля на рынке разных наркотиков существенно изменится, так как будет преобладать спрос на более дешевые и «эффективные» наркотики. Спрос на синтетические наркотики, включая новые психоактивные вещества (NPS), как ожидается, значительно возрастет, в то время как кокаин и героин станут менее популярными. Спрос на контрафактные товары может значительно увеличится, так как доходы все большей части населения будет уменьшаться. Экономические трудности могут сделать потребление незаконных продуктов, таких как контрафакт товаров повседневного спроса, более социально приемлемым и услуги и товары, предлагаемые ОПГ будут воспринимается в качестве оправданной альтернативы. ОПГ,

производящие контрафактную продукцию также смогут больше полагаться на эксплуатацию нелегального труда, чтобы поддержать производительность на уровне, необходимом для удовлетворения растущего спроса на их продукцию.

Экономический спад во многих государствах-членах ЕС может изменить структуру организованной преступной деятельности. Вместо ориентации на страны Западной Европы, мобильные организованные преступные группировки могут больше внимания уделять Восточной Европе, где экономическое развитие и рост благосостояния предоставляют много возможностей для квартирных краж и угонов автотранспорта.

Бедность и прекращение процветание создают благоприятную почву для криминальной эксплуатации. Экономическое неравенство в ЕС может привести к росту нелегальной иммиграции и торговли людьми в целях эксплуатации труда, принуждения к проституции и преступности. Спрос на дешевую рабочую силу существенно возрастет в результате быстрого расширения глобальной потребительской базы, и вызовет усиление трудовой эксплуатации в традиционно уязвимых отраслях, таких как гостиничный бизнес, строительство или уборка. Отрасли, обычно не связанные с этим явлением, также могут быть затронуты. В будущем, эксплуатация труда может иметь место в контексте новых и возникающих бизнес-моделей, таких как краудсорсинг или быстро расширяющаяся электронная торговля. Жертвами экономического спада могут стать и другие профессиональные и социальные группы. Например, масштабный аутсорсинг в сфере администрации может сопровождаться эксплуатацией опытных и квалифицированных сотрудников в области бухгалтерского учета, ввода данных или любых других услуг, которые могут предоставляться дистанционно в режиме онлайн.

Модели эксплуатации в ЕС уже меняются в результате экономического давления. Жертв сексуальной эксплуатации все чаще перемещают в пределах ЕС и не исключено, что имеющиеся или возникающие экономические диспропорции внутри ЕС могут спровоцировать подобные перемещения с целью трудовой эксплуатации или принуждения к преступности. Граждане ЕС с очень низкими доходами или столкнувшиеся с существенным снижением уровня жизни, будет становиться все более уязвимыми для таких форм эксплуатации, в том числе мошенничества с предоплатой, предоставлением занятости и условиями труда, которые выглядят более благоприятными, чем на легальном рынке труда. Снижение уровня жизни в Европе и рост богатства в странах с развивающейся экономикой также могут подтолкнуть граждан ЕС к эмиграции. Вполне возможно, что ОПГ начнет предлагать комплексные услуги по содействию гражданам ЕС, стремящимся нелегально выехать в страны в Азии или Южной Америки. Европа может по-прежнему оставаться регион назначения для нелегальных мигрантов из менее благополучных стран, но при этом перестанет быть наиболее притягательным местом.

Экономический спад, вероятно, повлечет за собой рост мелких, неорганизованных форм преступности, включая мошенничество с социальными пособиями или кражи. Эти преступления будут также совершать ОПГ, маскируя свою деятельность как по организации крупных уголовных предприятий со сложными структурами. Рост недоверия в обществе представляется особенно опасным и может оказаться выгодным для ОПГ, подрывая доверие граждан к власти и повышая привлекательность организованной преступности в качестве поставщика товаров и работодателя.

Социально-экономические диспропорции служат решающим фактором в распространении социальных волнений и беспорядков. Исторические примеры связи между неравенством и возникновением беспорядков включают так называемые «массовые МВФ-беспорядки» в 1980-х и 90-х гг. Жесткие меры, такие как сокращение социальных выплат или снижение субсидий на основные товары, такие, как продукты питания[22] или вода[23], глубоко подорвали доверие граждан к своим правительствам. Неспособность государств обеспечить минимальные стандарты жизни породила множество общественных движений и инициировала волну общественных протестов. Ряд аналогичных событий может быть отмечен в сегодняшней Европе.

Экономический кризис породил социальные движения, ставящие под вопрос авторитет государственной власти и требующие открытой демократии в том числе такие движения, как «Индинядос» и «Окупай». Технический прогресс позволил организовывать такие движения в виртуальном режиме. Инструменты, разработанные некоторыми из наиболее радикальных сторонников этих движений, могут причинить существенный ущерб уже в ближайшее время. Методы крипто-анархистских групп могут оказаться весьма полезным для ОПГ, особенно после дальнейшей доработки. Инновации в области самовоспроизводящихся 3D принтеров сделают 3D-печать широко доступной и открыть новые возможности для ОПГ, занимающихся оборотом огнестрельного оружия или торговлей контрафактными товарами. Альтернативные криптовалюты основной функции которых является анонимность, такие как Дарккойн и различных Биткойн-услуг по отмыванию денег, таких как «туман» или «темный кошелек», сделает отслеживание сделок практически невозможным, в значительной степени содействуя торговле незаконными товарами в Интернете.

Насильственные радикализация и организованная преступность пересекаются и взаимодействуют в широком спектре криминальной экономики. Инструменты, разработанные под предлогом социального сопротивления, используются также в преступной деятельности, иногда в переработанном виде. Некоторые склонные к насилию радикальные группы и одиночки используют эту идеологию, чтобы скрыть преступные умыслы и придать более организованный характер своей деятельности. В условиях экономического кризиса и снижения уровня жизни эти группы стали более заметны и получили возможность рекрутировать новых членов, что усиливает представляемую ими угрозу.

Сложные экономические условия будут вовлекать некоторых людей к тяжкую или организованную преступность. Ухудшение экономической ситуации и отсутствие альтернативных источников доходов обеспечивает ОПГ большой приток новых членов. Долгосрочные экономические проблемы могут сделать организованную преступность и ОПГ более социально приемлемыми и создать среду, которая способствует коррупции.

Усиление соперничества за природные ресурсы

ОПГ будут все активнее проникать в отрасли промышленности, зависящие от природных ресурсов, чтобы действовать в качестве брокеров или агентов при торговле этими ресурсами.

Обеспечивая будущее организованной преступности

С учетом значительной скорости роста численности населения и роста подушевого потребления электроэнергии, продовольствия и товаров многие страны столкнутся с дефицитом природных ресурсов. Инфильтрация в мультинациональные компании может позволить ОПГ контролировать доступ к природным ресурсам и получать беспрецедентные доходы. На некоторых рынках основных природных ресурсов доминируют монополии или олигополии, что усиливает потенциальную угрозу инфильтрации ОПГ в эти глобальные корпорации. Большинство природных ресурсов находятся за пределами ЕС, поэтому европейские ОПГ не могут непосредственно контролировать их добычу, но они способны найти свои ниши и все чаще выступают в качестве брокеров или агентов, например, для компаний, стремящихся получить права на буровые работы или доступ к трубопроводам.

Нефть

Началось соперничество за контроль над ресурсами Северного Ледовитого океана и Антарктиды. Доступ в антарктический регион в настоящее время регулируется Договором об Антарктике, который вступил в силу в 1961 г. и защищает континент как научный заповедник. Договор истекает в 2048 г., и вполне возможно, что бедные энергоресурсами страны предпочтут не продлевать его и начнут конкурировать в добыче прогнозируемых 200 млрд. баррелей нефти. Доступ к запасам нефти в Южно-Китайском море в настоящее время также остро оспаривается между китайским и вьетнамским правительствами, и этот спор, как ожидается, продолжится.

ОПГ будут искать различные возможности проникнуть в этот сектор. Повышение цен на нефть сделает откачку нефти из трубопроводов, фильтрацию или промывку промышленного дизельного топлива для использования в качестве автомобильного, мошенничество с НДС и акцизами прибыльной деятельностью для ОПГ. Они также будут активнее заниматься киберпреступностью в попытках получить контроль над критическими инфраструктурами. Некоторые ОПГ уже занимаются этим. Тем не менее, в будущем, ожидается, что многие другие ОПГ будут стремиться активизировать свое участие в этом секторе в результате усиления конкуренции между группами.

Международные нефтяные компании уже изучают запасы нефти на Балканах и глубокие залежи, окружающие африканский континент. Высокий уровень коррупции в обоих регионах создает благоприятную почву для проникновения ОПГ в сферу поставки и технического обслуживания трубопроводов и других видов инфраструктуры.

Газ

Подобно нефти, газ является весьма ценным товаром. В настоящее время запасы природного газа извлекаются с помощью новой технологии ректификации, что привело к перенасыщению рынка и снижению цены, особенно в США. Транспортировка сжиженного природного газа не является легкой задачей; крупные инфраструктурные проекты в США направлены на решение этой проблемы с использованием железнодорожного и морского транспорта. ОПГ могут участвовать в строительстве и обслуживании этой инфраструктуры в целях получения доступа и контроля за поставками критических ресурсов. Особенно высок риск проникновения ОПГ в портах, примером чего служит установление каморрой контроля в порту Джоя Тауро в Калабрии, Италия.

Энергетическая безопасность стала предметом серьезной озабоченности ЕС и его государств-членов, которые ищут альтернативные источники энергии. Соединенные Штаты взяли на себя обязательство по скорейшему созданию инфраструктуры, необходимой для экспорта сжиженного природного газа в случае полного прекращения поставок по трубопроводам.

Высокий уровень проникновения ОПГ в энергетические компании по-прежнему вызывает серьезную озабоченность государств-членов ЕС. ОПГ также все чаще стремятся осуществлять преступную деятельность, связанную с установлением цен и поставками нефти и газа на черный рынок.

Вода

Вода становится все более дефицитным ресурсом, который уже стал серьезной проблемой в Южной Азии. Население региона, по прогнозам, вырастет на 32 % в течение следующих

30 лет. Конкурентная борьба за ресурсы, как ожидается, усилится и станет основным вопросом национальной политики страны и международных отношений в регионе. Изменение климата может вызвать нехватку воды во многих регионах мира.

ОПГ, вероятно, попытаются получить прибыль от дефицита ценных ресурсов, таких как вода, с помощью незаконного забора или кражи воды и продажи ее по завышенной цене. ОПГ уже осуществляют незаконный забор нефти и газа непосредственно из трубопроводов и легко могут расширить эту деятельность, занявшись также водой. Для получения доступа к водным ресурсам ОПГ могут коррумпировать служащих водораспределительных компаний.

Продовольствие

Цены на продукты питания неразрывно связаны с ценами на нефть. Тем не менее, на цены эти цены также влияют засуха и наводнения. Глобальные изменения климата, скорее всего, приведут к более частым засухам и наводнениям, которые также оказывают существенное влияние на колебания цен на продовольствие.

Считается, что рост цен на продовольствие в 2008 г. стал одним из факторов, вызвавших социальные волнения на Ближнем Востоке. Во время арабской весны в 2011 г. цены резко выросли снова, что спровоцировало беспорядки в Алжире, Бахрейне, Египте, Ираке, Ливии, Мавритании, Омане, Сирии, Саудовской Аравии и Уганде. ОПГ могут попытаться извлечь выгоду из нехватки продовольствия и роста цен на него. Вполне возможно, что ОПГ с большими ресурсами начнут накапливать запасы продовольствия, чтобы продать их на черном рынке в будущем. ОПГ, вероятно, будут более активно участвовать в хищении грузов, содержащих продукты питания и другие ценные материалы. В прошлом грузовики ООН с продовольственной помощью уже становились мишенью вооруженных нападений. Такие инциденты могут в будущем могут участиться и затрагивать регулярные маршруты поставок, а не только помощь в зонах конфликтов.

Нехватка продуктов питания, скорее всего, повлечет за собой ухудшение общего качества пищевых продуктов для потребителей в Европе. В ЕС ОПГ смогут использовать растущий спрос на качественные продукты для совершения мошенничества, связанного с переупаковкой или переименованием низкокачественных продуктов. ОПГ также сами производить и распространять продуктов питания низкого качества.

Земля для сельскохозяйственного использования будет становиться все более ценным ресурсом. ОПГ могут попытаться получить контроль над продовольствием и цепочками поставок продуктов питания путем скупки сельскохозяйственных земель. Эта деятельность позволит им получать значительные прибыли и оказывать давление на граждан и государственные учреждения. Продовольственная безопасность является важным условием для функционирования общества и ее подрыв представляется особенно опасным сценарием.

Распространение виртуальной валюты

Виртуальные валюты дают все больше возможностей действовать в качестве независимых криминальных предпринимателей, работающих по принципу криминального предоставления услуг, без необходимости прибегать к сложной криминальной инфраструктуре для получения и отмывания денег.

Платежи в битах

Появление виртуальных валют вызвало интенсивные дебаты в средствах массовой информации и среди правоохранительных органов. В настоящее время, многочисленные виртуальные валюты позволяют выполнять скрытые платежи в Интернете. В то время как Биткойн является самой популярной на сегодняшний день криптовалютой, общепризнанной виртуальной валюты не существует. Тем не менее, виртуальные валюты создаются, чтобы обеспечить больше удобств для все более широкого круга потенциальных клиентов. Это развитие может привести к появлению одной или нескольких ключевых виртуальных валют, принимаемых на разных платформах и сайтах электронной торговли. Распространение платежных операторов, выполняющих автоматическую обработку сделок, совершаемых с использованием различных валют, также способствует диверсификации.

Виртуальные валюты предлагают определенный набор функций, которые делают их привлекательными для преступников: анонимность или использование псевдонима и быстрые безвозвратные переводы средств. Хотя виртуальные валюты предназначены для законного использования, их также широко используют преступники. Преступники часто отдают предпочтение централизованным схемам (особенно в расчетах между собой), которые по своей природе более стабильны по сравнению с криптовалютами, стоимость которых очень изменчива.

Виртуальные валюты являются идеальным инструментом для отмывания денег. Вход и выход из системы осуществляется через обменник. Обмен услугами представляет собой еще одну нишу услуг в теневой цифровой экономике. Тем не менее, используются также легальные обменники, особенно те, в которых не применяется принцип «Знай своего клиента» и предлагаются несколько методов обналичивания, в том числе платежи через предоплаченные или виртуальные кредитные карты и бюро платежных услуг.

Получив контроль над цифровыми финансовыми средствами, пользователь может легко создавать электронные кошельки, отказываясь от уже скомпрометированных. В дополнение к традиционным методам «расслоения», криптовалюты предлагают специализированные услуги по отмыванию денег, известные как «переключатели» или «смесители», которые скрывают сделки до того этапа, с которого отследить их очень затруднительно.

Нерегламентированные или ненадлежащим образом регламентированные азартные игры используются в целях отмывания денег в течение многих лет. Однако появление возможности осуществлять платежи, играть и обналичивать деньги с помощью виртуальных валют добавили новый уровень анонимности.

Виртуальные валюты для реальных преступлений

Виртуальные валюты уже оказали значительное влияние на различные виды преступной деятельности, облегчая обмен средств между преступниками и порождая процветающей черный рыночной обмен в сети (Даркнет). Тем не менее, ожидается, что виртуальные валюты будут расширять базу пользователей и будут использоваться для совершения сделок за пределами виртуальной реальности. Виртуальные валюты имеют потенциал стать предпочтительным способом оплаты в различных областях преступности, включая традиционные, такие как оборот наркотиков, продажа контрафактных товаров или незаконный оборот оружия.

В то время как децентрализованные виртуальные валюты или криптовалюты были менее популярны среди киберпреступников, их предпочитают преступники, занимающиеся в Даркнете традиционными видами преступной деятельности с помощью Интернета. На рынках Даркнета в качестве платежного средства, как правило, используется Биткойн.

По мере того, как виртуальные валюты продолжают развиваться, есть вероятность появления новых валют, ориентированных на незаконную деятельность и обеспечивающих большую безопасность и подлинную анонимность. Именно для этих целей были созданы такие схемы, как MUSD, Объединенная платежная система и UAPS. Распространение этих схем обеспечит процветание криминальной экономики, оставляя правоохранительным органам мало возможностей для вмешательства.

Роль фрилансеров в организованной преступности должна стать более заметной благодаря этому процветающему анонимному рынку. Специалисты по компьютерам и в других областях, представляющих интерес для преступных организаций, станут рекламировать свои услуги за оплату в криптовалюте. Если фрилансер будет задержан правоохранительными органами, анонимность платежа не позволит выйти на крупную организацию. Таким образом, преступные группировки смогут прибегать к специализированным услугам по принципу аутсорсинга с минимальным риском для себя.

Группировки, занимающиеся торговлей людьми, оружием и наркотиками будет шире предлагать свои услуги и товары на незаконных рынках. Ожидается, что наиболее распространенными видами деятельности будет сексуальная эксплуатация и сбыт наркотиков. Анонимность, обеспечиваемая для покупателей при использовании криптовалюты, может снизить барьеры для широких слоев общества в онлайн покупке незаконных материалов.

Ряд вредоносных программ на ПК и мобильных телефонах собирают с зараженных устройств данные об электронных кошельках. Другие программы заставляют зараженные устройства вырабатывать электронные деньги для преступников. Можно ожидать, что это явление станет все более распространенным.

Демографические изменения в ЕС

ОПГ все чаще будут выбирать пожилых людей в качестве жертв, а также специализироваться на предоставлении им незаконных товаров и услуг, используя новые возможности.

Старая Европа – новые криминальные рынки

На тяжкую и организованную преступность также оказывают влияние масштабные демографические перемены. Пожилые люди, вследствие их уязвимости, всегда были мишенями для преступников, и эта тенденция усилится за счет роста доли лиц старше 60-ти лет. Мошенничество, совершаемое ОПГ в отношении пожилых людей, в настоящее время затрагивает все государства-члены ЕС и с ростом числа пожилых людей, вероятно, еще более расширится. Однако, расширение этой возрастной группы не только увеличивает число потенциальных жертв, но и значительно увеличивает потребительскую группу нелегальных товаров и услуг.

ОПГ уже ориентируются на пожилых людей при выработке определенных мошеннических схем. При этом, поскольку жизнь пожилых людей сильно зависит от пенсионного и социального обеспечения, ОПГ все активнее занимаются мошенничеством в этой сфере. Такое мошенничество подразумевает либо незаконное получение средств за счет пожилых людей, либо нелегальные консалтинговые услуги по увеличению получаемых пенсионных и социальных выплат.

Экономический кризис показал, что ОПГ, занимающиеся контрафактом товаров, отличаются большой гибкостью и приспособляемостью. До кризиса большую часть контрафакта составляли подделки предметов роскоши, таких как сумки, очки или другие дорогих товаров. Но в связи со снижением доходов населения ОПГ перешли на подделку преимущественно товаров повседневного спроса, такие как чистящие порошки или зубная паста. В перспективе при

подделке товаров ОПГ могут ориентироваться специально на потребности растущего числа пожилых потребителей.

С возрастом люди все сильнее зависят от лекарств и медицинских приборов. Распространение поддельных лекарств уже сегодня представляет серьезную угрозу здоровью граждан ЕС, и ОПГ, вероятно, расширят спектр контрафакта медикаментов и медицинского оборудования, чтобы получать прибыль в сегменте, ориентированном на пожилых людей.

Некоторые ОПГ активно пытаются проникнуть в прибыльные отрасли экономики и добиться доминирующего положения. В качестве примера можно привести гостиничный бизнес, транспорт, строительство или утилизация отходов. Предоставление медицинских услуг становится все более прибыльной отраслью, которая будет расти в ближайшие годы, частично в результате демографических изменений.

Медицинские услуги, для пожилых людей представляют растущий сектор, и ОПГ будут пытаться проникнуть в этот прибыльный бизнес. Проникновение организованной преступности в эту отрасль здравоохранения влечет риск оказания некачественной медицинской помощи уязвимым членам общества, а также предоставляет дополнительные возможности для преступной деятельности, такие как распространение фальсифицированных лекарственных средств или различных мошенничества в отношении пациентов и страховых компаний. Это станет результатом ожидаемого движения ОПГ в сферу услуг, которая обещает значительные прибыли, более низкий риск обнаружения и значительно более мягкие наказания по сравнению с традиционной преступной деятельностью.

Старение населения Европы будет оказывать влияние на характер преступности в ЕС. Пожилые люди будут все чаще будут становиться объектом мошенничества, а также потребителями контрафактных товаров. но может возникнуть и в значительной группы потребителей запрещенных товаров. ОПГ можете воспользоваться возможностями в секторе здравоохранения, расширяя свою деятельность в различных аспектах оказания медицинской помощи и активизировать свое участие в производстве и распределении контрафактных фармацевтических препаратов. В целом, демографические изменения, вероятно, не окажут влияния на уровень тяжкой и организованной преступности в ЕС, но они вызовут изменения на рынках товаров и откроют новые возможности для ОПГ, которые будут стремиться приспособиться к меняющейся структуре населения Европы.

3. ЭВОЛЮЦИЯ КРИМИНАЛЬНЫХ РЫНКОВ

С точки зрения общей эволюции тяжкой и организованной преступности и влияния ключевых факторов современные криминальные рынки можно разделить на три категории:

Наиболее динамичные криминальные рынки

Преступность в Европе включает разнообразных отдельных преступников, свободные сети и ОПГ, действующие в различных областях, начиная от традиционной преступной деятельности, такой, как торговля наркотиками, до новых, быстро развивающихся направлений, таких как киберпреступность. Европол внимательно отслеживает эти области преступности и регулярно составляет свой основной отчет – Оценка угроз тяжкой и организованной преступности (SOCTA). Хотя все виды преступности, отмеченные в SOCTA, оказывают серьезное влияние на ЕС, его государства-члены и граждан, некоторые криминальные рынки, как ожидается, будет отличаться особенно динамичным характером.

Наиболее динамичные рынки не всегда являются самыми крупными. Темнее менее, они представляют проблему для правоохранительных органов, поскольку быстро меняются и используют новые, неизвестные ранее методы, материалы и технологии. Цель этого раздела

состоит в том, чтобы выделить те области преступности, которые, как ожидается, претерпят самые значительные изменения, не пытаясь дать оценку их влияния, опасности или общей значимости по отношению к другим криминальным угрозам.

Синтетические наркотики и новые психоактивные вещества

Синтетические наркотики по-прежнему будут представлять серьезную проблему в ЕС. Традиционные синтетические наркотики, такие как амфетамин, метамфетамин, МДМА и другие вещества будут доступны на европейском рынке наркотиков, и ОПГ будет продолжать производить эти препараты в ЕС. Тем не менее, правоохранительные меры и изменения в законодательстве подтолкнут ОПГ, занимающиеся производством этих препаратов, к инновациям, в результате чего технологии и организация производства будут совершенствоваться. Недавние события показали, что преступные группировки способны быстро приспособиться к запрету прекурсоров, перейдя на альтернативные неконтролируемые вещества.

Новые психоактивные вещества (NPS), скорее всего, превратится в наиболее серьезную проблему, связанную с наркотиками в ЕС в ближайшем будущем. Их производство и продажа во многих случаях юридически представляет собой «серую зону», что стимулирует дистрибьюторов и потребителей и не препятствует производству и торговле. Неконтролируемые NPS легко импортировать и распространять в ЕС, удовлетворяя быстро растущий спрос во всех государствах-членах. Эти вещества уже захватили часть рынка наркотиков, имитируя традиционные препараты, такие как кокаин и героин.

Интернет-магазины и глобальная инфраструктура сбыта облегчают заказ и получение новых психоактивных и других веществ. Открытая онлайн-торговля новыми психоактивными веществами, вероятно, расширит их сбыт. Этот рынок имеет потенциал быстрого роста и даже сможет конкурировать с каннабисом. Социальная толерантность к новым психоактивным веществам в настоящее время относительно высока и может даже увеличиться с появлением на рынке широко потребляемых и популярных веществ. Миллионы потребителей смогут заказать новые психоактивные вещества анонимно из своего дома. Их новые разновидности будут продолжать появляться в значительных количествах каждый год, что потенциально делает эту проблему ключевой для правоохранительных органов и органов здравоохранения ЕС.

Контрафактные товары

Контрафактные товары будут продаваться в будущем исключительно через Интернет. Рынки электронной торговли контрафактными товарами станут еще более сложным, вследствие копирования сайтов правообладателей потребителям станет еще труднее отличать подлинные товары от подделки. Повышение осведомленности и защита прав интеллектуальной собственности в Китае, вероятно, приведет к смещению производственных зон в Африку.

3D-печать будет иметь далеко идущие правовые последствия для защиты прав интеллектуальной собственности, а правоохранительные органы столкнутся с новыми формами контрафакта, которые будет очень трудно доказать. Вполне возможно, что преступные группировки будут заниматься поставками контрафактного сырья для 3D принтеров, а также подделка 3D принтеров и их компонентов. 3D принтеры могут привести увеличению производства контрафактной продукции в ЕС.

С учетом ограниченного доступа к ресурсам, таким как вода и земли сельскохозяйственного назначения, вполне вероятно, что фальсификация продуктов питания с использованием генетически модифицированных продуктов, а также фальсификация или контрафакт семенного фонда получат большее распространение для удовлетворения потребительского спроса.

Старение населения в ЕС приведет к росту производства и оборота контрафактной фармацевтической продукции, медицинских приборов, протезов, а также подделки вакцин. Эпидемия ожирения в Европе может также вызвать рост оборота поддельных таблеток для похудения, лечения диабета, связанного с ними оборудования и сердечных препаратов. Электронные аптеки уже действуют весьма успешно, и данная бизнес-модель может быть распространена для сбыта других контрафактных товаров.

В ЕС уже отмечались случаи подделки подушек безопасности и тормозных колодок. Как правило, они продаются через Интернет. В ряде случаев мошенники сбывали уже использованные подушки безопасности, что создает серьезные проблемы для здоровья и безопасности потребителей.

Киберпреступность

Технологические инновации происходят быстро и во многих случаях непредсказуемо. Не ограничиваясь виртуальным пространством, киберпреступность расширяется и оказывает влияние практически все другие виды преступных действий. Появление преступности в виде онлайн услуг сделало киберпреступность горизонтальной по своей природе, также как отмывание денег и подделка документов. Изменение характера киберпреступности непосредственно влияет методы, используемые в других видах преступной деятельности, таких как оборот наркотиков, содействие незаконной иммиграции или сбыт контрафактных товаров. Темпы технического развития и быстрое принятие ОПГ новых методов и техники делают невозможным детальное прогнозирование этой области преступности. Тем не менее, ряд важных тенденций проявляются уже сейчас и будут иметь долгосрочные последствия.

Общие тенденции развития киберпреступности предполагают значительное увеличение масштабов, сложности, количества и типов атак, числа жертв и экономического ущерба. Киберпреступность использует основанную на услугах и торговле криминальную индустрию, используя ряд легальных инструментов и услуг, таких как анонимность и кодирование. Это позволяет традиционным ОПГ осуществлять более сложные преступления, нанимая специалистов с необходимыми техническими навыками и опытом.

Следует ожидать, что разработчики вредоносных программ все чаще будут ориентироваться на различные терминалы Интернета и новые формы критических инфраструктур. Вредоносные программы будет больше использовать кодирование и становиться все более «умными».

Можно ожидать использование новых и более сложных методов социальной инженерии, например, достижений в области искусственного интеллекта. Поскольку все больше людей выбирают социальные сети в качестве средства общения, можно предположить, что эти сети будут использоваться для загрузки и распространения вредоносных программ.

Мошенничество без предъявления карты будет расширяться пропорционально росту количества платежных операций онлайн. Распространение бесконтактных платежных систем неизбежно сделает их предметом для атак.

Поскольку виртуальные валюты предлагают функции, которые делают их привлекательными для киберпреступников, легальные схемы по-прежнему будут использоваться, в том числе и в противоправных целях. Ожидается, что виртуальные валюты будет продолжать развиваться, обеспечивая нишу для киберпреступников.

Создание угроз критическим инфраструктурам и людям будет все более размывать грань между кибератаками и физическим нападением, поскольку они приводят к одинаковым результатам: разрушениям и травмам людей. Кроме того, усиление проникновения виртуальной реальности в повседневную жизнь имеет может привести к тому, что киберпреступления будут влечь за собой сильный психологический ущерб.

Различие между законной и незаконной деятельностью может также становятся все более размытым, поскольку такая практика, как сбор и перехват данных и манипуляции с целью оказания влияния на репутацию будут еще более тесно связаны с получением прибыли. Сходство между криминальным спамом и законными методами маркетинга, такими как поведенческая реклама, уже могут служить показателем этой тенденции. Перед законодателями встает задача разграничить обстоятельства, при которых эти действия могут считаться законными, и обеспечить по возможности согласование этих норм на международном уровне. Криминализация, естественно, также потребует достаточного потенциала для расследования, пресечения и уголовного преследования.

Наконец, расширение использования беспилотных транспортных средств, роботов и автоматизированных устройств неизбежно поднимет вопрос о компьютерах как разумных агентах. Это может совершенно изменить уголовное право, которые исторически существует для регулирования отношений между людьми.

Экологическая преступность

Экологические преступления охватывает различные виды преступной деятельности и услуг. Ожидается, что в ближайшие годы экологическая преступность значительно вырастет. Это особенно касается оборота электронных отходов, который рассмотрен более подробно в другой главе настоящего доклада.

Стабильные криминальные рынки

ЕС и его государства-члены будут по-прежнему сталкиваться не только с динамичными областями преступности, описанными выше, но также с традиционной преступной деятельностью, использующей хорошо проверенные методы, дающие высокий доход. Оборот каннабиса будет по-прежнему приносить криминальным сетям миллиарды евро. Организованная преступность в сфере недвижимости будет оставаться угрозой для граждан и бизнеса в течение следующего десятилетия. ЕС останется предпочтительным местом назначения для нелегальных мигрантов и торговцев людьми. Описанные ниже области преступности по-прежнему будут создавать серьезную угрозу для ЕС. Установившиеся маршруты, отработанные методы и сохраняющийся спрос на запрещенные товары в ЕС и за его пределами означают, что эти криминальные рынки будут сохраняться и представлять проблему для правоохранительных органов. Эти рынки представляют наибольшую долю тяжкой и организованной преступностью в ЕС в настоящее время и такое положение сохранится в дальнейшем.

Каннабис

Каннабис является наиболее популярным наркотиком в государствах-членах ЕС и, вероятно, останется таковым в обозримом будущем. Помимо выращивания в ЕС, каннабис ввозится в значительных количествах из Марокко, Албании и Афганистана. В результате эффективной деятельности правоохранительных органов по пресечению каналов поставки, маршруты контрабанды могут значительно измениться. Снижение ввоза, вероятно, усилит тенденцию выращивания каннабиса организованными преступными группировками на всей территории ЕС. В некоторых государствах-членах с подходящими климатическими условиями, где выращивание каннабиса в крупных масштабах ранее не практиковалось, таких как Болгария, Румыния или Хорватия, выращивание каннабиса может значительно расшириться.

Ожидается, что дебаты вокруг легализации каннабиса усилятся в течение ближайших десяти лет, возможно, в результате его легализации или декриминализации в некоторых странах. Любые такие изменения могут оказать существенное влияние на распределение каннабиса в рамках ЕС и на ОПГ, которые в настоящее время занимаются его оборотом и сбытом.

Правоохранительные органы уже отмечают широко распространенную общественную толерантность к каннабису, которая, по всей видимости, сохранится и в обозримом будущем. Европейские правоохранительные органам необходимо готовиться к возможным изменениям в правовом статусе каннабиса в некоторых странах ЕС.

Организация нелегальной иммиграции

Основные факторы, такие, как вооруженные конфликты, засухи, нехватка продовольствия и стихийные бедствия по-прежнему будут причиной миграционных потоков в ЕС из различных регионов. Число стран происхождения расширится.

ОПГ будут сосредотачиваться на обеспечении долгосрочного пребывания в ЕС путем предоставления консультаций о том, как обойти или использовать действующее законодательство. ОПГ будет чаще прибегать к методам, которые трудно обнаружить, например, браки по расчету или злоупотребление другими правовыми статусами. Диапазон предпочтительных стран назначения в ЕС будет расширяться и включить государства-члены, которые ранее в основном использовались для транзита.

Некоторые ОПГ будут стремиться получить возможность модифицировать и подделывать чипы с биометрическими данными, такими как отпечатки пальцев. Альтернативные виды транспорта, такие как автоматизированные автомобили, будет использоваться для перевозок, не вызывая подозрений и без физического присутствия организаторов.

Организаторы или посредники регулярно используют онлайн предложения для перевозки нелегальных мигрантов внутри ЕС. Водители выкладывают свои предложения на популярных веб-сайтах по совместному использованию автомобилей, которые позволяют указывать маршруты, количество свободных мест и цену за место. Посредники связываются с такими водителями и организуют перевозки нелегальных мигрантов в ЕС. Подобные перевозки регулярно перехватываются на таких маршрутах как Венгрия – Австрия – Германия и Венгрия – Австрия – Италия – Франция.

Торговля людьми

Торговля людьми является одним из старейших видов преступной деятельности и будет оставаться важным источником дохода для ОПГ в Европе. Сохраняющаяся потребность в дешевых товарах и услугах, в сочетании с усилением конкуренции между поставщиками, приводит к снижению цен и создает новые возможности для эксплуатации. Спрос на дешевые товары приведет к усилению эксплуатации на обычном рынке труда. ОПГ будут все чаще использовать легальные бизнес-структуры и механизмы субподряда для облегчения незаконного трудоустройства и эксплуатации.

ОПГ по-прежнему будут ориентироваться на наиболее уязвимые общественные группы и организовывать их перевозку в страны с большим рынком сексуальной и трудовой эксплуатации. Вполне возможно, что в будущем эти ОПГ будут реагировать на растущий спрос на сексуальную эксплуатацию европейских женщин в странах с формирующимся классов средних, где европейские женщины могут считаться «экзотикой», что обеспечит высокие доходы. Использование онлайн услуг для организации торговли людьми в будущем будет расширяться. Интернет сделал возможным сексуальную эксплуатацию с помощью веб-камер или секс-чатов; пер-

спективные технические инновации, несомненно, вызовут появление новых, пока неизвестных форм эксплуатации.

Организованная преступность имущественного характера

ОПГ, специализирующиеся на имущественных преступлениях, быстро адаптируются к изменению ситуации и постоянно ищут новые возможности. Преступники могут уделять больше внимания электромобилям.

Похитители грузов также приспосабливаются к новым условиям. Цепочки поставок, скорее всего, станут полностью автоматизированными, где участие человека будет ограничиваться дистанционным контролем и заданием исходных пунктов и пунктов назначения. С учетом этого преступники могут вмешиваться в автоматизированные системы управления и перенаправлять грузы в свой адрес.

Онлайн платформы станут основным рынком для краденых товаров, особенно для передачи данных и ценностей. Краденные товары уже торгуются как в открытой сети, так и в Даркнете. Эта тенденция будет продолжаться и предлагаемые услуги, скорее всего, станут более профессиональным и охватывать более широкую сферу. Например, вместо того, чтобы полагаться на криминальные связи, потребители смогут купить угнанный автомобиль на заказ, анонимно и с минимальными усилиями. Торговля похищенными культурными ценностями в настоящее время представляет собой маргинальное явление. Однако, с развитием таких огромных рынков, как Китай, Бразилия и Индия может резко вырасти спрос на культурные ценности, которые рассматриваются как символы высокого статуса.

Мошенничество

Развитие схем мошенничества будет определяться повсеместным подключением к Интернету через стационарные и мобильные устройства и распространением онлайн услуг. Широкое распространение обмена личными данными между отдельными лицами, а также между гражданами и государственными органами, привлекает внимание ОПГ, которые способны получать значительные прибыли от мошенничества, используя краденые личные данные. ОПГ будет развивать мошеннические схемы, эксплуатирующие дистанционное предоставление услуг и образование через Интернет. Рост электронной торговли породил множество новых видов мошенничества в отношении индивидуальных потребителей, онлайн поставщиков и предприятий, предоставляющих услуги по переводу денег.

В ЕС и его государствах-членах субсидии и другие финансовые стимулы являются неотъемлемой частью экономической политики, направленной на стимулирование экономического восстановления и поддержки секторов с высоким потенциалом роста. ОПГ продемонстрировали свою способность получать доступ к государственным фондам, часто предназначенные для приоритетных секторов, таких как возобновляемые источники энергии, и злоупотреблять ими. ОПГ будет стремиться расширить свою деятельность в других секторах экономики, где появляются возможности для мошеннического получения субсидий, коррумпируя для этого государственных служащих.

Оборот огнестрельного оружия

В оборот оружия будут вовлечены новые регионы происхождения и новые ОПГ. Ряд конфликтов в Европе и около нее, скорее всего, повысит доступность огнестрельного оружия на нелегальном международном рынке и увеличит его незаконный оборота в ЕС через морские и

сухопутные границы. Огнестрельное оружие из Сирии, Ливии и Мали уже доступно на европейском черном рынке, и эти страны могут превратиться в основных поставщиков такого оружия в ЕС.

Оборот незаконного огнестрельного оружия будет осуществляться преимущественно через Интернет. Технические инновации сделают платформы и рынки Даркнета значительно более доступными в будущем.

Огнестрельное оружие, выведенное из легального оборота, останется важным источником пополнения черного рынка. Несмотря на внимание средств массовой информации к презентации первого пистолета, полученного методом 3D-печати в мае 2013 г., технология 3D-печати вряд ли станет основным источником распространения огнестрельного оружия из-за технической сложности изготовления огнестрельного оружия таким путем и легкости доступа и относительно низких ценна огнестрельное оружие на черном рынке в ЕС.

Сокращающиеся криминальные рынки?

Ожидается сокращение некоторых криминальных рынков в связи с тем, что предлагаемые на них товары и используемые ими методы становятся менее актуальными в век цифровых технологий.

Фальшивомонетничество

Наличные деньги будут необходимы и в будущем, и не будут полностью вытеснены электронными средствами платежа. Преимущества анонимных денежных переводов с использованием наличных денег перевешивают их недостатки. Денежные останется ценным и стабильным средством платежа, особенно в конфликтных зонах, после крупных стихийных бедствий или в любой другой ситуации, где инфраструктура неспособна обеспечивать электронные денежные переводы.

Преступники также продолжат подделывать банкноты, которые, вероятно, будут иметь полимерную основу. Полимерные банкноты могут иметь больше степеней защиты. Сырье для подделки денег, например, бумага, полимеры, краски и голограммы, станет еще более доступным. Даркнет останется важным посредником в торговле сырьем и поддельными деньгами. Цифровые принтеры будут совершенствоваться и станут еще доступнее, что позволит отдельным лицам, а не только ОПГ, изготавливать фальшивые деньги высокого качества.

Кокаин и героин

Новые психотропные средства, имитирующие эффект традиционных наркотиков, таких как кокаин и героин, могут снизить долю этих наркотиков на европейском рынке. Тем не менее, торговля кокаином приносит ОПГ огромные прибыли, и останется такой в ближайшие годы. Хотя ожидается, что выращивание в странах происхождения будет снижаться, методы генетической модификации и новые технологии, скорее всего, компенсируют это снижение. ОПГ будут диверсифицировать свои маршруты и организацию, используя политическую нестабильность и слабость правоохранительных органов в некоторых регионах. Расширение Панамского канала приведет к значительному увеличению грузовых перевозок, что представляет большую экономическую выгоду для ЕС, но также может создать дополнительные возможности для торговли кокаином.

Балканский маршрут останется самым значительным маршрутом ввоза в ЕС героина, даже с учетом возможной диверсификации поставок.

4. ПЕРСПЕКТИВЫ ПРАВООХРАНИТЕЛЬНОЙ РАБОТЫ ПРАВООХРАНИТЕЛЬНАЯ РАБОТА: ВЫЗОВЫ И ВОЗМОЖНОСТИ

Серьезная и организованная преступность сохранит свой динамизм и способность приспосабливаться к меняющимся условиям. Правоохранительные органы на всей территории ЕС должны идти в ногу с технологическим прогрессом и возрастающей сложностью криминальных схем, пронизывающих все секторы экономики и общества – при этом ограничивая свои расходы с учетом сокращения бюджета. Отражая тенденции преступности, полиция становится все более сложной и борьбы с преступностью в настоящее время требует беспрецедентной степени специализации и экспертных знаний.

Анализ данных и Большие данные

Распространение и повсеместная доступность Интернета обещает стать ключевым элементом качественного скачка в работе полиции, но также представляет вызов для нее и требует выработки технических решений, привлекать экспертные знания и финансовые ресурсы, необходимые для полного использования этих возможностей.

Повышение Больших данных и появление повсеместного Интернета предоставит неоценимые возможности для правоохранительных органов в разработке, расследовании, выявлении и наблюдении за подозреваемыми. Такие устройства как телефоны и персональные компьютеры в настоящее время позволяют правоохранительным органам определить местонахождение человека. Учитывая возможность подключения через такие продукты как одежда, ювелирные изделия и обувь, станет легче определить местоположение человека в определенный момент времени. Например, обувь, которая автоматически подключается к ближайшей беспроводной сети для обновления онлайн фитнес-профиля, может позволить выявить закономерности движения человека. Преступники могут оставить свой мобильный телефон дома, но внедрение цифровой техники во все более широкий ассортимент товаров сделает затруднительной полную изоляцию от нее.

Правоохранительные органы также смогут использовать анализ Больших данных для прогнозирования и изучения общественного мнения. Большие данные обещают революционные изменения в борьбе с тяжкой и организованной преступностью. Расширенный анализ данных может помочь определить приоритеты усилий и эффективнее использовать оперативные данные. Анализ Больших данных может выявить закономерности в преступной деятельности и связи между якобы несвязанными между собой событиями или преступниками и пресечь деятельность децентрализованных криминальных сетей.

Тем не менее, потенциал использования этих технологий также поднимает серьезные вопросы, связанные с защитой данных. Недавние утечки информации, связанные с масштабным перехватом личных сообщений в рамках контртеррористических усилий, показали, что граждане многих государств-членов выражают все большее беспокойство в связи с использованием этих технологий. Эффективная правоохранительная работа невозможна без доверия и сотрудничества со стороны граждан и потребует разъяснения характера и пределов использования Больших данных. Надежная защита данных, а также прозрачность являются ключевыми ценностями, которые будут определять, удастся ли правоохранительным органам сохранить доверие граждан.

Подготовка кадров

Использование Больших данных и передовых методов анализа информации требует исключительно высокого уровня знаний и специальных навыков, которых в настоящее время не имеет большинство правоохранительных органов на всей территории ЕС. Вместо того чтобы полагаться на специалистов общего профиля, полицейские должны будут овладеть специализациями, необходимыми для выполнения сложных и специфических задач. С учетом необходимости рекрутирования специалистов, правоохранительным органам придется пересмотреть приоритеты и по-новому оценить, что им следует делать самим, а что можно поручить частному сектору.

Правоохранительные органы вряд ли смогут конкурировать с частным сектором в борьбе за наиболее квалифицированных специалистов в области анализа данных с точки зрения оплаты труда. Тем не менее, они должны найти способы вербовать людей, обладающих узкоспециализированными знаниями. Вполне возможно, что правоохранительные органы будут делегировать некоторые следственные и полицейской функции предпринимателям. Значительную часть расследований в области киберпреступности уже проводят частные компании, работающие совместно с правоохранительными органами. Эта тенденция может усилиться и распространиться на сферы, в которых частный сектор ранее не действовал.

Следователи со специализированной подготовкой уже работают в таких областях, как киберпреступность, контрафакт и финансовые расследования. Поскольку технология прогрессирует и используемые преступниками методы становятся все более сложными, полицейские должны будут получить специальные знания и опыт, чтобы противостоять криминальным вызовам. Технический прогресс потребует от полиции привлечения специалистов по нанотехнологиям и роботехнике, либо в качестве сотрудников, либо на внештатной основе.

Международное и межведомственное сотрудничество

Глобализация организованной преступности является предметом обсуждения политиков, правоохранительных органов и научных кругов в течение многих десятилетий. Тем не менее, признание этой проблемы не влечет за собой глобализацию правоохранительных органов в той степени, которая необходима для эффективного противодействия этой угрозе. Усилия в области международного сотрудничества, такие как деятельность Интерпола и Европола, убедительно показывают необходимость и эффективность международного сотрудничества в борьбе с тяжкой и организованной преступностью. В перспективе преступники будут осуществлять почти всю свою деятельность в рамках виртуальной и глобальной криминальной сети, которая не знает ни границ, ни юрисдикции. Национальные правоохранительные органы будут сталкиваться со все более сложными криминальными структурами, которые действуют не только в двух или трех странах, но действительно в глобальном масштабе.

Международное сотрудничество правоохранительных органов может обеспечить инструменты для противодействия этой угрозе. Тем не менее, подлинное сотрудничество требует приверженности стран обмену данными, опытом и ресурсами для того, чтобы каждая страна была способна бороться с новыми формами организованной преступности. Международные правоохранительные органы, такие как Европол, сохранят решающее значение в укреплении доверия между национальными правоохранительными органами, организовывая совместные оперативные мероприятия и реализуя эффективное международное полицейское сотрудничество.

Международное сотрудничество правоохранительных органов разных стран является ключевым элементом в борьбе против тяжкой и организованной преступности. Однако не

только правоохранительные органы отвечают за предупреждение и пресечение организованной преступности. Интернет превратился в весьма сложную многостороннюю среду, которая регулируется в основном частными компаниями, а не государственными органами. В перспективе правоохранительные органы должны заниматься с частным сектором даже больше, чем сегодня. Партнерство государственного и частного сектора в борьбе с киберпреступностью уже развивается, и есть некоторый прогресс в сотрудничестве с компаниями-правообладателями товарных знаков в борьбе против контрафактной продукции. Тем не менее, ожидаемое смещение организованной преступной деятельности в виртуальное пространство в течение следующего десятилетия требует от правоохранительных органов развития междисциплинарного взаимодействия с партнерами по всему миру и в различных секторах.

Частные решения государственных проблем?

Правоохранительные органы должны будут сделать важный выбор, имеющий серьезные последствия: развивать потенциал в полиции или прибегать к аутсорсингу необходимых услуг в частном секторе. Частный сектор в сфере безопасности значительно вырос в последние десятилетия. Многие функции, традиционно осуществляющиеся правоохранительными органами в настоящее время, выполняются частными службами безопасности, либо в рамках аутсорсинга государственных функций, либо частной коммерческой деятельности. Некоторые эксперты считают, что в частных службах безопасности работает больше людей во всем мире, чем в правоохранительных органах. Возникли и развиваются ряд коммерческих направлений в областях, ранее относившихся исключительно к компетенции правоохранительных органов. Банки и страховые компании имеют собственные аналитические и детективные службы Частные предприниматели, часто бывшие сотрудники полиции, все чаще предлагают консультационные услуги в этих областях. Ранее аутсорсинг был ограничен сектором логистических услуг, таких как уборка, поставки, обслуживание транспортных средств, и организационным сектором: человеческими ресурсами и информатикой. Теперь же все чаще основные правоохранительные функции, в том числе наблюдение и патрулирование, осуществляются внешними субъектами, а не правоохранительными органами. Уже многие годы частные детективы играют важную роль в проведении уголовных расследований, связанных с мошенничеством и другими видами преступной деятельности. Это привело к тому, что традиционно «полицейские задачи» входят в компетенцию не только полиции, но и большого числа организаций государственного и частного сектора.

Инвестирование в будущее

В любом случае правоохранительные органы будут нуждаться в средствах для инвестирования в новые и инновационные технологии, а также привлечения специалистов, которые могут использовать эти инструменты для борьбы с тяжкой и организованной преступностью. Политикам необходимо будет выработать модели финансирования правоохранительных органов, либо предусматривающих увеличение бюджета, либо инновационные схемы финансирования правоохранительной деятельности и инфраструктур.

В будущем, некоторые полицейские службы смогут выполняться в рамках новых форм коллективного финансирования. Краудсорсинг представляет собой новую бизнес-модель, которая хорошо зарекомендовала себя в обеспечении некоторых услуг и финансирования для многих частных предприятий. Краудсорсинг среди территориальных общин может быть использован для финансирования полицейской работы или обеспечения безопасности. Жертвы киберпреступности могут объединяться, чтобы привлекать частных экспертов по компьютерной безопасности, особенно если правоохранительные органы не в состоянии расследо-

вать большее количество инцидентов. Тем не менее, такая практика остается спорной с культурной и идеологической точки зрения.

Организованная преступность становится все более сложной и разнообразными, и правоохранительные органы не будут иметь никакого выбора, кроме как стать более гибкими и приспосабливаться к меняющейся обстановке. Большие данные и анализ данных в перспективе могут радикально изменить правоохранительные подходы к борьбе с тяжкой и организованной преступностью. Тем не менее, эти явления также представляют серьезный вызов для правоохранительных органов, которые должны стремиться в полной мере использовать их потенциал.

Комментарии Академической консультативной группы SOCTA:

– Некоторые перспективные тенденции преступности уже очевидны – изменения в различных формах употребления наркотиков и их производства, огромный рост объема контрафактных товаров, изменение характера террористической деятельности (в частности, уменьшение числа атак, изменившийся характер участия в террористических организациях и рост гибридного терроризма – частично преступная и частично террористическая деятельность), изменения в финансовой преступности и использование цифровых технологий для криминальных коммуникаций. Чтобы реагировать на эти изменения, правоохранительные органы должны принять инновационные подходы в борьбе с преступностью, привлекая партнеров из социальных и коммерческих структур. Элементом этого станет расширение базы правоохранительной работы, однако это может быть сопряжено с трудностями на национальном уровне и при двухстороннем обмене информацией. Но нынешняя тенденция привлечения правоохранительными органами внешних партнеров в качестве экспертов, несомненно, будет расширяться. Это потребует взвешенных и, возможно, сложных административных и управленческих решений. Планирование этих процессов на европейском уровне должно стать приоритетной задачей;

– В частности, можно отметить, что тенденции в области преступности являются функцией мотивации, возможностей, а также того, как государственные и частные организации, намеренно или случайно действуют, чтобы собирать информацию и пресекать эти возможности. Долгосрочные тенденции включают способы, которыми технологии воздействуют на развитие возможностей (например, позволяя приобретать простых в использовании комплектов электронного оборудования и совершать мошенничество с личными данными, что затрудняет обнаружение; финансовые переводы с использованием биткойн также помогают сохранить анонимность). Традиционные преступления, такие как оборот наркотиков и контрабанда людей по-прежнему будут предоставлять широкие финансовые возможности для лиц, располагающих сетевыми структурами или организационными навыками. Поэтому было бы неправильно ожидать, что в будущем традиционные виды преступлений будут вытеснены с рынка за счет развития средств коммуникации и электронной коммерции;

– Может, однако, появиться больше возможностей для «организованных преступных сетей» использовать электронные средства, чтобы оградить себя от риска и расширить свою преступную финансовую деятельность. Могут также открыться больше возможностей для внедрения инсайдеров в банки и другие учреждения, чтобы получать финансовую информацию и обеспечивать отмывание денег, что потребует надлежащих контрмер со стороны служб безопасности. Правоохранительным органам придется расширить сферу применения методов криминальной разведки, используемых для борьбы с незаконным оборотом наркотиков;

– Как отдельный перспективный вызов следует отметить возможный рост значения для преступного мир «распределенных неиерархических сетей», создаваемых в результате сложных глобальных заговоров. В настоящее время они наиболее заметны в Интернете, и уже

заставляют нас пересмотреть границы между реальными и виртуальными преступлениями. Традиционные иерархические сети играют в настоящее время меньшую роль в террористических организациях, что говорит об ожидаемом снижении их значения и в обычной преступности. Социальные сети и «темная паутина» уже сделали такие сложные 'плоские' сети реальным инструментом совершаемых в Интернете правонарушений, и их влияние, вероятно, будет расти. Эти тенденции будут представлять как концептуальные и организационные вызовы для правоохранительных органов. Это потребует переосмысления понятия «организованной» структуры, а мониторинг и контроль таких сетей будет крайне сложным;

– Для того, чтобы реагировать на косвенные и непреднамеренные последствия собственного производства и маркетинга, организациям частного сектора, возможно, придется разработать усовершенствованные формы регулирования и контроля. В какой-то мере это уже происходит, но управление, интеграция с государственными ресурсами обеспечения и контроля такой деятельности потребует новых решений в административной и правоохранительной сфере. Кроме того, расширение концепции общественной безопасности и включение в нее продовольственной безопасности и других аспектов создаст ряд проблем для Европола и других полицейских структур, которые должны будут работать в различных коммерческих сферах для решения подобных вопросов, чем раньше они никогда не занимались;

– Сбор и обмен информацией в Европе значительно улучшилась. Но аналитическая работа организована иногда недостаточно хорошо, что свидетельствует о необходимости увеличения инвестиций в аналитический потенциал.

Организованная интернет-преступность. Главная угроза (IOCTA)[20]

Доклад подготовлен на основе материалов Европейского Центра киберпреступности ЕВРОПОЛА. Оценка охватывает ключевые события, текущие и перспективные угрозы, а также тенденции, которые проявятся в области киберпреступности в ближайшее время. Доклад подготовлен с учетом национальных материалов государств-членов ЕС, записок экспертов ЕВРОПОЛА, а также материалов, поступивших от частного сектора, общественных движений и научных кругов.

Ключевой вывод доклада – это стремительный рост профессионализма киберпреступников, чьи практические навыки, организованность и программно-аппаратное обеспечение подчас начинают превосходить соответствующие характеристики правоохранительных органов. При этом киберпреступность с каждым годом увеличивает свой аппетит и готовность рисковать и нести жертвы в лице отдельных членов киберпреступного сообщества при сохранении развитых сетей и других форм оргпреступных организаций.

В докладе сформулирован ряд основных рекомендаций по повышению эффективности борьбы с киберпреступностью, а также выделены приоритетные темы межстранового и межведомственного взаимодействия правоохранительных органов ЕС в рамках Полицейского Цикла EMPACT.

В качестве ключевых направлений развития киберпреступности, а соответственно и межстранового и межведомственного взаимодействия, выделены такие сферы, как интернет-педофилия и сексуальная эксплуатация детей через интернет, кибератаки на финансовые учреждения, платежное мошенничество и другие виды мошенничества, связанные с кражей и присвоением персональных данных. Новой темой является использование преступниками интернета вещей, особенно в области педофилии.

Резюме

IOCTA 2015 показывает, что киберпреступность становится все более агрессивной и конфронтационной. Если в 90-е – начале нулевых годов киберпреступность в основном носила пассивный характер и была связана с кражей информации, а также с социальной инженерией, когда интернет выступал всего лишь средой общения, то в настоящее время киберпреступники готовы и открыто идут на прямую конфронтацию. Киберпреступления в значительной части, особенно в наиболее крупных синдикатах, стали приобретать характер активных кибератак. Киберпреступники все больше не просто ищут дыры в кибербезопасности, а взламывают и активно преодолевают защитные системы частного бизнеса, государственных учреждений и граждан. Вместо того чтобы прибегать к уловкам и скрытности, киберпреступные организации все активнее делают ставку на техническое, программное и кадровое превосходство над правоохранителями и службами безопасности частных и общественных сетей. Рост преступлений в области педофилии, кражи данных, вымогательства и т. п. осуществляется в основном за счет этого превосходства. Наличие такого превосходства увеличивает страх граждан и бизнеса. Он выражается в том, что согласно имеющимся данным в 2014–2015 гг. заметно упало число обращений граждан и бизнеса, пострадавших от киберпреступников. Они боятся обращаться в полицию, во-первых, потому, что не верят в ее эффективность, а во-вторых, опасаясь еще

[20] Доклад Европола. 30 сентября 2015 г. (Извлечение). The Internet Organized Crime Threat Assessment (IOCTA). Europol, 30 September 2015.

более наглых атак киберпреступников. Эта проблема без преувеличения превратилась в проблему номер один киберпреступности.

Киберпреступность превратилась в быстрорастущую индустрию. В настоящее время все более широкое развитие получает бизнес-модель CaaS или «Преступление как сервис». Эта модель предоставляет легкий доступ к наиболее технически сложным преступлениям для традиционных преступников, а также лиц и структур, склонных к девиантному поведению. Киберпреступники сегодня работают не только на себя, но и по заказу традиционных оргпреступных группировок, отдельных компаний, граждан и т. п.

Киберпреступность охватывает сегодня чрезвычайно широкий спектр разнообразных преступлений. По-прежнему наибольшее число преступлений приходится на использование вредоносных компьютерных программ. В этой связи в 2015 г., согласно оценкам, наиболее быстрорастущим видом киберпреступности является вывод из строя при помощи вредоносных программ персональных и корпоративных компьютеров, гаджетов и сетей. Вывод имеет целью вымогательство, когда при получении определенной суммы денег программы удаляются из компьютера и работа системы восстанавливается. При этом, начиная с 2015 года, вредоносные программы, используемые для вымогательства все чаще стали включать в себя модуль, позволяющий копировать данные, содержащиеся в компьютере или сетях. Тем самым даже после удаления вируса и возобновления работы преступники в качестве трофея забирают не только деньги, но и данные.

Быстрыми темпами растет финансовая киберпреступность. Во все большей степени вредоносные программы уступают место программным продуктам, позволяющим подключаться к транзакционным и платежным финансовым сетям и перенаправлять в пользу преступников все возрастающие финансовые средства.

В условиях борьбы с оффшорами киберпреступники начинают предлагать новую услугу, связанную с проведением незаметных для финансовых и правоохранительных органов транзакций в банки тех стран, где имеется более мягкое финансовое законодательство. По оценке Швейцарской банковской ассоциации доходы киберпреступности от перевода денег из швейцарских банков после принятия соглашения о разглашении банковской тайны при судебных решениях, в банки таких стран, как Гибралтар, Сингапур, Гонконг, измеряются миллиардами швейцарских франков.

Средства массовой информации называют 2015 год «годом кражи данных». В условиях, когда данные стали цифровым золотом современности, они привлекают наибольшее внимание киберпреступников. В то же время надо иметь в виду, что популярность этой темы стимулировала медиа подробно освещать все выявленные случаи кражи данных. Поэтому, хотя киберпреступления в области данных и являются наиболее динамичным видом преступности, сегодняшние масштабы этого вида преступности несколько преувеличены благодаря медийному освещению.

Еще одна проблема, которая выявилась в этом году, это – размытость между деятельностью киберпреступников и групп, формируемых компаниями частного сектора и конкурентной разведки, которые занимаются так называемым активным тестированием и поиском дыр. По сути, и преступники, и корпоративные специалисты используют в своей деятельности одни и те же приемы, один и тот же софт. Это проблема, которую предстоит решать.

Все возрастающей проблемой для правоохранительных органов становится социальная инженерия, подкрепленная эффективными программными средствами. В ЕС отсутствует какое-либо законодательство, запрещающее социальную инженерию. При этом именно социальная инженерия является распространенным и эффективным инструментом, используемым в сложных киберпреступных комбинациях и многоступенчатых мошенничествах.

Общей проблемой становится то, что современные высокотехнологичные средства одинаково используются бизнесом, государством и преступниками. Поэтому принятая полициями

стран ЕС методология, связанная с поиском преступников по признакам использования того или иного инструментария в новых условиях оказывается бессмысленной.

Сексуальная эксплуатация детей онлайн становится все более распространенной и создает все более серьезные проблемы. Наибольшее внимание в Европе привлечено к dark net, где создано большое число сайтов, демонстрирующих сцены педофилии и жестокого обращения с детьми. Это крайне опасная ситуация, поскольку, как правило, плательщики, они же абоненты подобных сервисов, требуют новых лиц и новых зрелищ. Это толкает поставщиков контента на расширение сферы сексуальной эксплуатации детей и все более изощренных видов преступности. Кроме того, нельзя не отметить, что пользователи подобных сервисов по уровню своего дохода заметно превышают средний уровень по Европе. Они относятся в своей массе либо к верхней части среднего класса, либо к богатым.

Принимая во внимание, что техническое решение darknet таково, что обладатели педофильских порталов способны достаточно легко вычислить их пользователей, возникает питательная среда не просто для шантажа, а для проникновения самых жестоких преступников в верхние эшелоны бизнеса, а иногда и государственных структур. В этой связи необходимо резко усилить межгосударственное и межведомственное сотрудничество ЕС в рамках решительного искоренения педофилии с привлечением всех доступных программных, технических и агентурных средств.

Новым видом преступности стало распространение самогенерируемого неприличного контента. С повсеместным распространением среди тинэйджеров и молодежи гаджетов, в сети стало появляться огромное количество контента, связанного с различными сексуальными действиями. Зачастую тинэйджеры не понимают последствий выкладывания подобного рода фото и видео. Киберпреступники сегодня имеют на вооружении мощные программы работы с подобного рода фото- и видеоконтентом. Они позволяют находить тех, кто выложил контент и шантажировать их и их родителей. По данным правоохранителей ряда стран-членов ЕС, темпы роста самогенерируемого неприличного видеоконтента в разы превышают объемы наращивания фотоконтента в YouTube и Instagram.

Несомненно, возможности и потенциал киберпреступников значительно укрепили последствия скандала Сноудена. Охватившая Европу паранойя, связанная с шифрованием всего и вся, начиная с трафика, заканчивая электронной почтой, заметно облегчила жизнь киберпреступникам. Если еще в 2012 г. шифрованная электронная переписка была достаточно надежным маркером, указывающим на необходимость как минимум более пристального наблюдения за тем или иным пользователем, то сегодня этот маркер уже не работает.

Также для преступников большие возможности открывают широкое распространение небанковских платежных систем, в том числе на основе блокчейна. Свою роль играет ширящееся распространение шифрованных облачных хранилищ, а также IT бизнесы, как SaaS (сервис как услуга).

Новой неожиданной проблемой для Европола становится растущий дефицит высококвалифицированных программистов и специалистов других профессий, связанных с быстроразвивающимся сектором IT. В этих условиях даже крупнейшие европейские компании активно ищут персонал, в том числе среди хакеров, чего еще несколько лет назад не происходило. Кроме того, в условиях бюджетных ограничений не только частный бизнес, но и государственные структуры все чаще используют модель аутсорсинга. Киберпреступники своевременно обнаружили эту тенденцию и создали множество легальных фирм, которые превратились в интерфейс между средним, крупным бизнесом и государственными структурами, и наиболее агрессивными и мощными киберорганизациями. Это ведет не только к утечке сведений, но и тому, что киберпреступники подчас разрабатывают системы защиты, шифрования и т. п. для крупных корпораций, т. е. производят продукцию, которая должна защищать от них. Еще пару лет назад таких проблем не было.

Европол согласен со своими американскими коллегами, что в настоящее время преступное сообщество быстрее адаптируется к таким нововведениям, как dark net, интернет вещей, искусственный интеллект и блокчейн, по сравнению с правоохранительными органами. Как показывают обследования, европейский бизнес плохо понимает подлинные масштабы киберугроз. По имеющимся данным крупные европейские компании тратят на информационную безопасность в два-три раза меньше, чем их коллеги в России, Азии, и в пять-шесть раз меньше, чем в Соединенных Штатах. При этом именно Европа, с большим числом юрисдикций, является сегодня наиболее благоприятной сферой для киберпреступников со всего мира. По неофициальным данным в Европе раскрывается лишь одно из 30 преступлений в сфере киберпреступности против корпораций. Риск быть пойманным и наказанным составляет примерно 3 %. Такой уровень риска не то, что не может остановить, а более того, привлекает в Европу киберпреступников со всего мира.

В то же время нельзя не отметить и ряд успехов в борьбе с киберпреступностью Европола и национальных полицейских организаций. Европейский континент стал первым, где создан межнациональный, в рамках ЕС, полицейский цикл EMPACT и образованы межстрановые команды тактических действий против киберпреступности (J-CAT). Кроме того, Европе удалось наладить координацию Европола, национальных полицейских структур и частных служб информационной безопасности ключевых финансовых учреждений. Количество успешных атак и совершенных киберпреступлений в финансовой сфере в Европе в результате этих мер существенно ниже, чем в Соединенных Штатах и Канаде.

Можно констатировать, что в основных своих компонентах юридическая база для борьбы с киберпреступностью создана. Сегодня главный упор необходимо сделать на повышении эффективности оперативных и тактических действий. Основными компонентами концепции отражения угроз должны стать новой программный уровень оснащения полиции, создание глобальных в рамках ЕС баз данных и сведений по основным конкретным видам киберпреступности. Наряду с повышением программного и информационного уровня, необходимо провести сплошную переподготовку полицейских кадров с тем, чтобы не только сотрудники подразделений, занятых борьбой с киберпреступностью, но и обычные полицейские знали основные приемы и методы, позволяющие им снять информацию с компьютера преступника, отследить его активность на криминальных форумах и группах в социальных сетях, факт использования биткойна и других криптовалют и т. п.

Европол исходит из того, что при всей важности наращивания и повышения эффективности подразделений по борьбе с киберпреступностью, ее можно если не победить, то хотя бы остановить. Только задействовав весь аппарат правоохранительных органов. Глупо выглядит полиция, в которой подразделения функционально разделяются на действующие в реальной и виртуальной среде, в онлайне и офлайне. Преступники этого разделения не знают. Они уже давно действуют и совершают свои антиобщественные поступки в цифровой реальности.

Основные следственные задачи являются общими для всех областей не только киберпреступности, но и вообще противодействия преступности. Это: атрибуция, собирание и установление доказательной базы, определение юрисдикции и т. п. В условиях, когда киберпреступники действуют в киберпространстве, где нет каких-либо государственных границ, единственным ответом им может стать только возрастающий уровень международного сотрудничества между отделами по борьбе с киберпреступлениями стран-членов ЕС, а также привлечение к этой работе партнеров из стран Европейского континента, которые не являются членами ЕС, а также других стран мира с высоким уровнем развития информационных технологий.

Ключевые результаты

• Киберпреступность становится все более агрессивной и конфронтационной. В дополнение к кибервымогательствам, требующим незначительных технических навыков, все большее развитие получают новые виды киберпреступности, особенно в финансовой сфере и области хранения данных, которые предполагают высокий уровень компьютерного мастерства и оказывают парализующие воздействие на жертвы насилия.

• Борьба с киберпреступностью не может вестись исключительно подразделениями полиции, ориентированными на борьбу с киберпреступностью. С киберпреступностью должна бороться вся полиция в рамках межведомственной и межнациональной координации с привлечением частного сектора, научных кругов и общественных организаций.

• Кибермошенничество по-прежнему остается главной киберугрозой для частных лиц и организаций. С каждым годом этот вид киберпреступности насыщается новыми программными продуктами, прежде всего связанными с шифрованием и многомодульными вирусами, а также соединением киберпреступности и социального инжиниринга.

• Совместными силами полиции и финансового сообщества удалось победить такие программы-трояны, как «Зевс», «Цитадель» и «Шпионский глаз». Однако это была пиррова победа, поскольку на смену программам-троянам пришли вредоносные многомодульные программы, ориентированные на финансовый сервис, такие как Dyre или Dridex.

• Объемы и частота кражи массивов данных резко возрастают и постепенно становятся магистральным направлением киберпреступности. На данные существует огромный спрос на рынке. Вокруг этого черного рынка сложилась большая сеть киберпреступников – поставщиков подобного рода данных. Нарушения, связанные с кражей данных, в том числе персональных данных, помимо того, что сами по себе являются преступной деятельностью, запускают самые разнообразные виды преступности – от мошенничества и вымогательства до финансовых краж и квартирных ограблений.

• Социальная инженерия является распространенным и эффективным инструментом, используемым самыми различными видами киберпреступности. Наиболее широко социальная инженерия применяется различного рода мошенниками и ворами. В настоящее время нет специального законодательства, которое как-либо ограничивало использование методов социальной инженерии. Опыт показывает, что для кражи сведений и данных социальная инженерия оказывается не менее, а иногда и более эффективной, чем традиционное хакерство.

• В настоящее время в финансовой сфере на смену мошенничеству с кредитными картами в качестве наиболее быстро развивающейся сферы приходят транзакционные мошенничества. Транзакционные мошенничества предполагают использование сложного программного инструментария. Транзакционное мошенничество приносит доход киберпреступникам по трем направлениям: перенаправление средств с реального счета на преступный, присоединение к основному платежу небольшой дополнительной суммы, отчисляемой на преступный счет, как правило, при регулярных платежах, типа «за коммунальные услуги» и т. п., и наконец, доход от продажи сведений о транзакциях, включая доход от шантажа лиц, допустивших незаконные транзакции.

• Стремительное повышение программно-аппаратного уровня киберпреступников. Наряду с традиционными одиночными и нестабильными группами киберпреступников, в странах ЕС все активнее действуют организованные преступные группировки с распределенными по континентам аппаратными базами, использующими самые современные программные средства и успешно сочетающими их с наиболее продвинутыми технологиями социальной инженерии. Как правило, такого рода трансконтинентальные группировки базируются за пределами ЕС, но деятельность осуществляют в странах ЕС. Это затрудняет борьбу с ними из-за неот-

работанности межгосударственных и многосторонних соглашений о юрисдикции, сотрудничестве и взаимодействии правоохранителей.

• В Европе не поставлен на должный уровень, как в корпоративном, так и особенно в частном секторе, вопрос информационной безопасности. Европейские компании тратят недостаточно средств на создание эффективной системы информационной безопасности. Они не располагают необходимыми кадрами. Крайне низок уровень компьютерной грамотности, особенно в части цифровой гигиены, жителей стран ЕС. Это способствует превращению Европы в наиболее притягательное место для киберпреступников.

• Широкое распространение Tor, биткойна, других средств анонимизации привели к беспрецедентному росту числа торговых площадок в dark net и объему торговых операций. Несмотря на разгром ряда крупнейших торговых площадок, типа Silk Road, на месте уничтоженных быстро появляются новые торговые площадки, предлагающие весь набор товаров и услуг, нарушающих все мыслимые законы.

• Наряду с Tor постепенно набирает популярность европейская сеть darknet I2P. В ближайшее время следует ожидать появления большого числа торговых площадок и незаконных финансовых бирж, базирующихся на блокчейне. При этом сам по себе блокчейн, в отличие от биткойна, является полностью законным программным средством, которое чем дальше, тем больше будет служить протоколом для финансовых и деловых взаимодействий в киберпространстве.

• Стремительный охват интернетом бедных и развивающихся стран, а также скачкообразное увеличение доступа пользователей к потоковому видео в комбинации с повышением анонимности провоцирует взрывной рост услуг, связанных с детским сексуальным насилием, садомазохизмом и использование неприличного фото- и видеоконтента для вовлечение молодежи в преступные группы.

• Не по дням, а по часам распространяется шифрование и засекречивание передачи информации в интернете между частными лицами, и частными лицами и компаниями. Хотя эти решения являются обоснованными с точки зрения неприкосновенности личного информационного пространства, они открывают простор для киберпреступников. Злоумышленники используют их для того, чтобы скрыть свою идентичность, связи, факт совершения преступлений и получения вознаграждения за преступную деятельность. Сравнивая на виртуальных весах плюсы и минусы послесноуденовской анонимности и шифрования, европейские правоохранительные органы категорически утверждают, что минусов, в том числе для граждан гораздо больше, чем плюсов. Защищая свою идентичность от правительств, граждане становятся все более незащищенными по отношению к киберпреступности.

• Биткойн позиционирует себя в качестве единой глобальной валюты в рамках всего мира. Если до недавнего времени биткойн преимущественно использовался как платежное средств в рамках сети Top, то в настоящее время платежи в биткойнах принимаются во все большем числе площадок интернета. Это также создает благоприятную питательную среду для преступников.

Ключевые рекомендации

• Расследования в области киберпреступности крайне сложны и капиталоемки. Правоохранительным органам, как в рамках отдельных стран-членов ЕС, так и на уровне межгосударственного сотрудничества должны быть выделены гораздо большие ресурсы, чем в настоящее время. Без этого не удастся не то что уничтожить, но даже сдержать рост киберпреступлений, черпающих ресурсы из поистине бездонных источников. Кроме того, специфика киберпреступности такова, что от правоохранительных органов в этой сфере нельзя ждать немедленных результаты и быстрых арестов. Их работа должна вестись без лишнего давления

в течение того срока, который необходим правоохранителям для сбора доказательств и уличении виновных.

• Правоохранительные органы в своей работе должны исходить из того, что нет киберпреступности вообще. В киберпространстве орудие преступности, жертвы, тип организованности, способы финансирования и требуемые ресурсы столь же разнообразны, как и в традиционных видах преступности. Поэтому в рамках борьбы с киберпреступностью на национальном и наднациональном уровнях должны быть созданы целевые команды, борющиеся против конкретного вида киберпреступности и общие инфраструктурные подразделения, обеспечивающие высокий программно-аппаратный уровень для кибероперативников.

• Руководителям правоохранительных ведомств и властям стран ЕС необходимо смириться с тем, что борьба с киберпреступностью, а значит, обязательная фиксация киберпреступлений неизбежно приведут к резкому ухудшению статистики раскрываемости преступлений в странах и на континенте в целом. Благоприятная тенденция общего падения уровня преступности в Европе, а также повышение уровня раскрываемости преступлений является не более чем иллюзией, поскольку хорошо известно, что низовые органы полиции многих стран-членов ЕС отказываются принимать заявления о киберпреступлениях. Хорошие европейские цифры – это следствие плохого учета. Борьба с киберпреступностью требует не благоприятных отчетов, а точной картины масштабов происходящего.

• Финансовая система является поистине кровеносной системой единого европейского хозяйства. Несмотря на достигнутые успехи в борьбе с финансовой киберпреступностью, нужно и далее усиливать взаимодействие между Европолом, правоохранительными органами отдельных стран, европейским финансовым сектором и индустрией безопасности. Следует рассмотреть вопрос о создании единого в рамках ЕС в системе Европола центра анализа вредоносного программного обеспечения и разработки методов противодействия ему. В настоящее время такой центр (EMAS) уже действует. Но он ограничивается лишь анализом. Необходимо аналитическую функцию добавить функцию разработки, а также создать в структуре центра подразделение европейской киберкриминальной разведки.

• Первостепенное значение для всей Европы имеет защита жертв жестокого обращения с детьми, как в реальном, так и в виртуальном пространстве. Поэтому едва ли не главной задачей является создание возможно на основе межстрановой кооперации системы идентификации насильников, распространителей информации в виде видео и фотоконтента и пользователей его. Это позволит сделать неотвратимым наказание за данный вид преступлений. Киберпреступность в области сексуального насилия над детьми является той редкой сферой киберпреступности, которая при должной мобилизации усилий в кратчайший период времени может быть не только остановлена, но и ликвидирована вообще.

• Правоохранительные органы должны продолжать расширять сотрудничество для обмена знаниями, опытом, практикой, передовыми технологиями по работе с биткойном и другими криптовалютами в части использования их глобальным преступным сообществом.

• Чтобы противостоять киберпреступности правоохранительные органы должны вкладывать все возрастающие средства в проведение судебной цифровой экспертизы, а также создание специальных лабораторий, позволяющих достоверно устанавливать следы киберпреступлений. Наряду с этим необходимо оснастить правоохранительные органы передовыми технологиями преодоления различного рода шифрования, которое все шире используют киберпреступники.

• Необходимо в рамках ЕС создать единую базу сетевых протоколов и форматов файлов цифровых кошельков, используемых в различных платежных системах.

• Исполнение законов предполагает овладение полицейскими новым набором инструментов и ресурсов, которые позволяют не только раскрывать, но и профилактировать сложные высокотехнологичные преступления, где наряду с информационными технологиями исполь-

зуются средства социальной инженерии. Особое внимание должно быть уделено выявлению признаков, которые позволяют в цифровой среде, также как и при традиционной преступности осуществлять профайлинг преступников. А также их специфический почерк преступлений.

• Полицейские органы должны быть оснащены программными средствами, позволяющими вести наблюдение, отслеживание, пресечение и расследование преступлений в dark net. В этих целях следовало бы организовать не только межстрановую, но и межведомственную кооперацию и на этой основе создать единый стандартный инструментарий для полицейской работы в darknet.

Перечисленные выше меры являются первоочередными с точки зрения эффективности борьбы с киберпреступностью.

• При максимальном развитии дистанционных методов борьбы с киберпреступностью, сохраняет свое значение агентурная работа среди киберпреступников. Только она может в ближайшее время обеспечить не просто повышение уровня раскрываемости компьютерных преступлений, но и пресечение компьютерных преступлений в зародыше, и их профилактику.

• Необходимо сделать максимальный акцент на предупредительную работу в сфере киберпреступности по отношению к сексуальной эксплуатации детей в интернете. Как показывает опыт ряда стран – членов ЕС, регулярное посещение школ, телепередачи и беседы с родителями позволяют заметно повысить уровень информационной гигиены семей и детей и на этой основе затруднить деятельность преступников.

• В ближайшие годы в финансовой сфере работу против киберпреступности необходимо строить на основе принятых в этом году «Руководящих указаний и рекомендаций относительно пресечения кибератак на банкоматы».

• Повышение эффективности борьбы с киберпреступностью на национальном уровне может быть обеспечено только за счет резкого повышения координации и уровня осведомленности о киберпреступности в рамках сотрудничества стран ЕС с привлечением других стран – не членов ЕС. Главными направлениями такого сотрудничества являются:

– максимальный обмен информацией и оперативными данными, создание международных банков вредоносного программного обеспечения, мошенников и компаний и персоналий «денежных мулов»;

– осуществление комплексной инициативы по пресечению деятельности «денежных мулов». В этих целях помимо координации правоохранительных органов ЕС, необходимо наладить сотрудничество с промышленностью и финансовым сектором;

– установление безопасного общего канала в рамках ЕС, через который национальные органы будут делиться информацией о скомпрометированных кредитных или дебетовых картах, а также платежных кошельках, с целью предотвращения их использования для крупномасштабных мошенничеств.

• Правоохранительным органам стран-членов ЕС наряду с межнациональным и межведомственным сотрудничеством, а также налаживанием контактов с частным сектором и обществом необходимо тесное взаимодействие с национальными и глобальными СМИ. Наряду с прочим, целью этого сотрудничества должно быть пресечение героизации киберпреступников в масс-медиа и пресечение своего рода рекламы киберпреступности за счет излишне широкого освещения отдельных ее актов.

• Основой кооперации правоохранительных органов со всеми субъектами, юридическими лицами и гражданами должны стать недавно принятые Директивы сетевой и информационной безопасности ЕС. В Директивах подробно разъяснены важнейшие принципы координации, активного партнерства и взаимоотношений между частным сектором, обществом, правоохранителями.

• Правоохранители должны резко активизировать сотрудничество с научными кругами. Взаимодействие полицейских сил с наукой в Европе имеет более низкий уровень, чем во мно-

гих других регионах. В условиях широкого использования киберпреступниками таких высоких технологий, как многомодульный вредоносный софт, блокчейн-технологии, децентрализованные рынки и искусственный интеллект, правоохранительные органы и наука должны составлять единое целое.

• Правоохранительные органы стран-членов ЕС должны развивать рабочие отношения и потенциал сотрудничества с правоохранительными органами стран, не входящих в ЕС, и в первую очередь с Китаем, странами Юго-восточной, Южной Азии и Индии. Главное внимание в этом сотрудничестве надо уделить таким видам преступности, как использование мультиплатформенного вредоносного софта, мошенничество с кредитными картами и нажива на трансляции жестокого обращения с детьми.

• Государства-члены ЕС должны предоставлять разведке Европола всю необходимую информацию об интернет-активности в стране-члене ЕС. Кроме того, необходимо ввести в практику представления Европола информации не только от полицейских, но и иных правоохранительных структур в тех случаях, когда экстремизм и оборот наркотических средств или огнестрельного оружия осуществляется через интернет.

• Как никогда ранее правоохранительные органы должны наладить с помощью Европола обмен данными о такой новейшей преступной технологии, как социальная инженерия. При этом Европол будет брать на себя не только координирующую, но и аналитическую функцию, способствуя разработке методов и методик выявления случаев применения социальной инженерии на максимально ранних стадиях.

• Правоприменители и правоохранители стран ЕС должны активизировать свою работу в рамках таких многосторонних инициатив, как План действий по безопасности на авиатранспорте и Инициативы по созданию безопасной среды электронной коммерции в ЕС.

Законодательство

• По-прежнему сохраняется необходимость в дальнейшем согласованном изменении национальных законодательств с целью унификации правовых инструментов борьбы, прежде всего, с такими направлениями киберпреступности, как финансовые кибермошенничества и отмывание преступных доходов с использованием виртуальных валют.

• С учетом необходимости резкой активизации расследовательских и оперативных мероприятий в darknet необходимо внесение изменений в национальные законодательства и законодательство ЕС, позволяющие агентам более эффективно, чем в настоящее время, работать под прикрытием.

• Национальные органы должны обеспечить оперативное выполнение директивы ЕС «О пресечении атак на информационные системы». Все страны ЕС должны ввести в соответствии с директивой более жесткие, чем в настоящее время, наказания и штрафы за кибератаки, а также значительно ужесточить уголовную ответственность за использование вредоносных программ, как основного способа совершения кибер- и иных преступлений.

• Законодатели и политики вместе с промышленными и научными кругами, а также гражданскими активистами должны в самое ближайшее время решить вопрос шифрования. При этом, защита частной жизни и собственности отдельных пользователей не должна ставить под угрозу способность государственных и правоохранительных органов к расследованию уголовных или национальных угроз безопасности. Выбирая между приватностью отдельного человека и угрозой обществу законодательство должно предоставлять непререкаемый авторитет угрозам национального и регионального масштаба, по сравнению с частной приватностью. В этой связи необходимо провести дискуссию на национальном и европейском уровнях относительно законодательного запрещения шифрования файлов, электронной почты и т. п. в тех

случаях, когда компания – владелец сервиса или платформы не передает ключи шифрования государственным органам.

Оперативные направления действий и мероприятия

• С учетом роли IOCTA 2016, как наиболее целостного источника информации о положении дел с киберпреступностью, в настоящем докладе в качестве ключевых направлений оперативных действий для правоохранительных органов ЕС на 2016 г. предлагается выделить:

Кибератаки

• Ботнет-сети, в частности развернутые для DDOS атак и атак на финансовую инфраструктуру;

• Рынок программ-вымогателей и эксплойтов, как части модели «преступность как услуга»;

• Создание и использование многомодульных вредоносных программ, способных не только проникать в частные корпоративные сети, красть из них данные, но и перенастраивать, разрушать или брать под контроль физические объекты инфраструктуры.

• Программы для кражи данных.

• Блокировка антивирусных сервисов.

Киберсексуальная эксплуатация

• Трансляция платного потокового порно.

• Платный показ сексуальных занятий по заявкам.

• Трансляция педофильных актов и жестокого обращения с детьми с созданием специальных сервисов. В основном расположенных в darknet.

• Платные садомазохистские каналы по заявкам.

Платежные мошенничества

• Кража идентификаторов кредитных карт.

• Взлом защиты платежных сервисов с целью доступа к электронным деньгам.

• Целевые акции по корыстному подключению к каналам транзакций денежных средств.

• «Беловоротничковая» преступность с использование высоких технологий.

Сквозные преступления

• Использование мошеннических сайтов принудительного перенаправления, встраивания в сайты вредоносного софта, преступное использование хостинга и т. п.

• Создание нелегальных торговых сайтов в darknet.

• Сервисы по нелегальным транзакциям и отмывания денег.

• Криминальные схемы, выстроенные с использованием биткойна и других виртуальных валют.

• Криминальное онлайн консультирование.

Насколько это возможно и реалистично, деятельность правоохранительных органов должна быть нацелена в первую очередь на арест руководителей и ключевых функциональных членов организованных киберпреступных группировок. Эта работа должна быть дополнена интенсификацией блокировки и реквизиции активов членов ОПГ, а также активизацией агентурной работы с использованием мер смягчения наказания или полного прощения в случае деятельного раскаяния.

Успешная борьба с указанными выше направлениями киберпреступности невозможна без создания после широкого общественного обсуждения и законодательного закрепления системы превентивного мониторинга компаний, а также граждан стран – членов ЕС, обладающих критически важными навыками, которые могут быть использованы киберпреступниками. Превентивный мониторинг должен быть дополнен осуществляемыми как на национальном уровне, так и на уровне ЕС мерами разъяснительной работы со специалистами в области информационных технологий, повышения их осведомленности, профилактирования и, наконец, целенаправленных мер по обеспечению их полной занятостью в государственном, частном и общественном секторах.

С учетом резкого снижения возраста компьютерной преступности подобная работа должна начинаться не в частном секторе, а еще в университетах и даже старших классах школ. Именно там, в университетах, компьютерных клубах и молодежных сетях киберпреступники вербуют свои кадры. Поэтому законодатели, политики и общественность обязаны не только предоставить правоохранителям возможность мониторить активность лиц профессий, попадающих в зону риска, но и разворачивать профилактическую работу уже на уровне школ.

ВВЕДЕНИЕ

AIM

IOCTA 2015 разработана Европейским центром борьбы с киберпреступностью Европола. Она направлена на информирование лиц, принимающих решения по борьбе с преступностью на стратегическом, политическом и тактическом уровнях. Целью документа является определение приоритетов для оперативных действий правоохранительных органов ЕС, а также стран-членов ЕС в рамках компетенций ЕВРОПОЛА. В качестве трех первоочередных направлений борьбы с киберпреступностью в 2016 г. выделяются кибератаки, сексуальная эксплуатация детей в интернете и преступления в сфере платежных систем и средств. При этом особый акцент делается на новые явления, связанные с переплетением информационных технологий с социальной инженерией, как новым методов преступности.

Основываясь на принципиальном согласии, достигнутом странами-членами ЕС, в настоящем докладе дана информация о господствующих тенденциях в области киберпреступности в рамках ЕС. В нем делается прогноз относительно будущих рисков и возникающих угроз, а также даются рекомендации о повышении эффективности противодействию киберпреступности, в том числе на основе укрепления кооперации и сотрудничества правоохранительных органов стран-членов ЕС и ЕВРОПОЛА.

В IOCTA 2015 особый акцент делается на практическом опыте и достижениях стратегических партнеров в частном секторе и в научных кругах.

IOCTA 2015 призван изменить ситуацию, когда правоохранительные органы отстают от киберпреступников в таких областях, как сложная киберпреступность, dark net, виртуальные валюты, интернет вещей, использование киберпреступниками экспертных систем и искусственного интеллекта.

SCOPE

Несмотря на многочисленные технические, юридические и оперативные проблемы национальным и общеевропейским правоохранительным органам удалось осуществить ряд успешных действий против киберпреступников, в том числе в сети Tor. В то же время, достигнутые

успехи не носят пока системного характера. Более того, дальнейшее продвижение затрудняется растущей тенденцией повсеместного использования шифрования, инструментов обеспечения анонимности, а также программ анонимизации трафика.

Доклад содержит обновленную информацию по таким темам, как интернет вещей и большие данные, которые в перспективе станут одной из главных сфер приложения киберпреступности. Каждая глава доклада содержит анализ ситуации, обзор наиболее дерзкий и крупных преступлений в конкретной области, а также предсказание тенденций. Каждая глава завершается набором конкретных рекомендация для правоохранительных органов, имеющих задачи превентивно устранить угрозы и устранить риски, возникающие в ближайшем будущем. В 2015 году в докладе не содержится информация относительно использования киберпространства для противозаконной радикальной активности и распространения насильственного экстремизма через социальные медиа. Специальный доклад на эти темы будет издан Европолом в 2016 г. в виде отдельного продукта.

КИБЕРАТАКИ И ВРЕДОНОСНЫЙ СОФТ

Вредоносные программы остаются наиболее распространенным и приносящим максимальный ущерб инструментом киберпреступности. Вокруг вредоносного софта сложилась целая экосистема, которая включает в себя изготовителей подобного софта, операторов рынка, рядовых киберпреступников и членов оргпреступных группировок и даже консультантов по вредоносному софту.

В настоящее время в законодательстве стран-членов ЕС выделяются три основных категории вредоносного софта: программы-вымогатели, средства удаленного доступа и программы-шпионы, извлекающие информацию из компьютеров и сетей и доставляющие их преступникам. Надо признать, что большинство вредоносных программ в настоящее время являются многофункциональными. В этой связи законодательство и подзаконные, а также ведомственные акты государств-членов ЕС надо привести в соответствии с техническими реалиями и определить, как вредоносный софт любой софт, который обеспечивает несанкционированное проникновение, нарушение или копирование любой информации, содержащейся в государственных, корпоративных и частных сетях и электронных устройствах.

Ключевая угроза – программы-вымогатели

Вымогательство остается главным видом киберпреступности в ЕС и соответственно главной угрозой. Почти в двух третях стран – членов ЕС именно на вымогательство с использованием вредоносных программ приходится основная доля преступлений в киберпространстве. В то же время, следует отметить, что столь высокая доля вымогательства в структуре киберпреступности в значительной мере связана с тем, что данный вид является так называемой низкоуровневой киберпреступностью, использующей наиболее простые программные средства. По своему характеру этот вид преступности тут же фиксируется жертвой и соответственно легко регистрируется. Поэтому, по мнению авторов доклада, вымогательство является не только наиболее массовым, но и наиболее легко фиксируемым видом преступности, маскирующим гораздо более масштабные виды преступления.

Основные программы для вымогательства

Криптолокер является наиболее широко используемой программой для вымогательства в странах-членах ЕС. Впервые он был зафиксирован в сентябре 2013 г. и с тех пор инфициро-

вал более четверти миллиона компьютеров в странах-членах ЕС. Наибольшее распространение данный вид вымогательства получил во Франции, Бельгии, Голландии, Сербии и Швеции. Любопытно, что в Норвегии не было зафиксировано вообще ни одного случая кибервымогательства.

Другим, гораздо более серьезным средством вымогательства стала программа CTB-LOCKER. Данная программа впервые была разработана на продажу в середине 2014 г. и с тех пор продается в сети Tor. После заражения компьютера, она предлагает своим жертвам выбор вариантов языка и после этого общается на родном языке жертвы. В отличие от Криптолокера, данная программа поразила в основном страны Восточной Европы, входящие в ЕС и Прибалтику.

Наряду с указанными программами в странах Восточной Европы, Беларуси, Украине и России процветают хакерские форумы и сайты в сети Top, на которых за различные цены – от 35 до 3000 евро – можно купить боты и многомодульные вредоносные программы, ориентированные не только на частных пользователей и корпорации, но и на проникновение через системы защиты финансовых учреждений. Оборот этого рынка измеряется десятками миллионов долларов.

Ключевая угроза – инструменты удаленного доступа (RATS)

RATS является законными инструментами, используемыми для доступа к системе третьей стороной, как правило, в рамках технической поддержки или по административным причинам. Во многих случаях RATS могут дать пользователю удаленный доступ и контроль над системой. В последние годы киберпреступники активно используют вредоносный софт для взлома и перехвата управления RATS. Особенное распространение эта практика получила в 2015 г. в связи с началом этапа массового перехода к интернету вещей. Если ранее RATS использовался в основном для кражи частной и корпоративной информации, то в настоящее время они все шире используются для доступа к удаленным микрофонам, веб-камерам и перенаправления видео и аудиопотока к преступникам. Одним из последствий этого процесса стало стремительное сращивание традиционных видов преступности с киберкриминалом. Киберкриминал все чаще берет по модели аутсорсинга функции слежения, наблюдения, разведки для таких традиционных преступлений, как кража, киднепинг и т. п.

Ключевая угроза – кража данных

Данные являются ключевым товаром в цифровом мире. Сегодня практически любой вид данных имеет большое значение. По имеющимся оценкам в 2015 г. до 70 % капитализации компаний в сфере интернетторговли, медиа и т. п. была связана с наличием у компании Больших Данных. В такой ситуации неудивительно, что большинство новых вредоносных программ разрабатываются с целью кражи данных. В отличие от Соединенных Штатов, где расположены крупнейшие базы и хабы данных, в Европе по-прежнему главной сферой кражи данных являются не интернет-компании, а финансовые учреждения. Соответственно наиболее востребованным преступным рынком товаром являются производимые на заказ банковские трояны – вредоносные программы, предназначенные для сбора данных и манипуляции транзакциями.

Особая угроза связана с тем, что в последнее время функции денежных хранилищ все больше переходят к гаджетам и смартфонам, а оборот все больше осуществляется в безналичной форме. Согласно имеющимся данным в странах-членах ЕС до 90 % смартфонов не имеют достаточного уровня защиты от хакеров. Поэтому все более популярным видом преступности становится изготовление и эксплуатация программ, проникающих в электронные кошельки и крадущих цифровой кэш. Наибольшие масштабы эти кражи приобрели в Великобритании,

Франции, странах Бенилюкс и Финляндии, а также Польше и Румынии. Наиболее низкий уровень наблюдается в Германии, Австрии, Швейцарии, где электронные платежи гораздо менее популярны.

Угроза – эксплойт

Эксплойты – это программы или скрипты, которые используют уязвимости в программах и приложениях для загрузки вредоносного софта на уязвимые машины. К числу наиболее популярных в 2015 г. эксплойтов следует отнести Dyre, Timba, Dridex, Carberg, Torpig, Chylock.

Наибольший ущерб в странах ЕС нанесли эксплойты Zeus и Spyeye. Эти две программы нанесли Европе ущерб в несколько десятков миллионов евро. реальный ущерб видимо гораздо больший. Обе программы разработаны российскими хакерами. Человека, который занимался продажей этих эксплойтов, прежде всего, Spyeye, удалось обнаружить в ходе Трансатлантической полицейской операции. В настоящее время русский хакер по фамилии Панин заключен в американскую федеральную тюрьму.

Угроза спама

В 2015 г. объем спама в Европейском киберпространстве существенно возрос. Спам является наиболее распространенным и дешевым способом распространения вредоносного программного обеспечения через электронную почту и ссылки в социальных сетях. Как правило, спам в Европе используется для установления удаленного, незаметного для пользователей, контроля над их компьютерами и гаджетами и создания обширных бот-сетей, используемых для киберпреступной деятельности. Основной объем спама в Европу поступает из России, Украины и Китая.

Все шире используются спамовые программы, как средства доставки других, еще более вредоносных специализированных программ. Подавляющая часть таких программ, как Zeus и других перечисленных выше попадает в сети через электронную почту.

В апреле 2015 г. ЕВРОПОЛ и J-CAT объединили свои усилия с европейским частным сектором и американскими коллегами из ФБР для борьбы с лавиной спамам из стран, не входящих в ЕС и НАФТА. В настоящее время правоохранители по обе стороны Атлантического океана согласованно действуют против российских, украинских и китайских хакеров и киберпреступников.

Угроза – мобильный вредоносный софт

Данные свидетельствуют, что объем и качество мобильных вредоносных программ растет быстрее, чем по софту в целом. При этом мобильные вирусы в настоящее время не включены ни в один из списков наиболее опасных угроз в странах-членах ЕС. Отсутствует также законодательство, которое регулирует борьбу с этим видом изготовления вредоносного софта.

Представляется, что это колоссальное упущение, поскольку именно смартфоны и гаджеты с каждым годом берут на себя все больший объем интернет-трафика.

В большинстве стран-членов ЕС считается, что вредоносные программы для мобильных устройств приносят меньший вред, недели их аналоги для полноценных компьютеров. Это является ярким примером, когда практика и законодательство серьезно отстают от реальностей информационных технологий. В большинстве отчетов относительно вредоносных программ по-прежнему первое место занимают вредоносные программы, связанные с подпиской жертв мошенничества на несуществующие мобильные услуги. В условиях все ширящегося

перехода финансовой сферы на использование гаджетов в качестве электронных кошельков и децентрализованных транзакций, киберпреступники используют недоработки правоохранителей из стран-членов ЕС для расширения масштабов деятельности. Пока ситуация не стала критической по единственной причине. В странах-членах ЕС, за исключением Великобритании, использование гаджетов как электронных кошельков и осуществления децентрализованных транзакций составляют соответственно 20 и 12 % от уровней США. Однако это отставание будет неминуемо наверстано в течение 2016–2017 гг. вследствие глобального характера мировой финансовой системы. Если правоохранительные органы стран-членов ЕС в ближайшие год-два не пересмотрят свое отношение к мобильному вредоносному софту, и не поставят борьбу с ним в центр своей деятельности, то Европа с ее высоким уровнем жизни и развитой финансовой инфраструктурой неминуемо станет основным местом приложения сил производителей и эксплуатантов мобильного вредоносного софта, ориентированного на преступления в финансовой сфере.

Будущие угрозы и развитие

Накопленный опыт правоохранительными органами стран ЕС и аналитика ЕВРОПОЛА свидетельствуют о происходящей смене ключевых угроз и рисков. Главные вредоносные угрозы, в том числе, поименованные выше, неуклонно сокращают масштабы своего применения. Частично это – итог деятельности правоохранительных органов. Однако главная причина в ином. Новое поколение вредоносных программ выходит на первый план. Также следует иметь в виду, что, если ранее вредоносный софт разрабатывали одиночки, либо небольшие команды в рамках инициативной хакерской деятельности, то в настоящее время можно говорить о сложившейся теневой IT индустрии, В этой индустрии действуют распределенные по всей планете команды. При этом, если раньше, как правило, одни и те же люди создавали программы и использовали их, то новой тенденцией становится появление многослойной структуры киберпреступности. Она включает в себя производителей софта для киберпреступников и хакеров, киберпреступные группировки, использующие этот софт, а также структуры, специализирующиеся на предоставлении киберкриминальной деятельности как услуги традиционным преступным группам.

Киберпреступность становится все более трансграничной. Для национальных правоохранительных органов и ЕВРОПОЛА в целом главная проблема уже сегодня и в ближайшей перспективе состоит в том, что, как правило, изготовители и в значительной мере эксплуатанты вредоносных программ территориально базируются за пределами Европы, а совершают свои преступления в юрисдикции стран ЕС. Ключевым вопросом в этой связи является отработка не декларативного, а процедурного и операционного международного сотрудничества по профилактике, обнаружению, доказыванию и пресечению киберпреступлений между странами-членами ЕС и странами, не входящими в ЕС, но обладающими развитым информационным потенциалом.

Лавинообразно нарастают уязвимости и эксплуатирующие их эксплойты нулевого дня. Происходит это по двум причинам. С одной стороны темпы увеличения производства программ, приложений и сервисов опережают темпы наращивания численности качественных работников информационной отрасли. Соответственно падает уровень программного кода. И даже в программах, выпускаемых крупными производителями, появляется все больше уязвимостей, которые немедленно используют хакеры. С другой стороны киберпреступность из одиночной и нерегулярной деятельности превратилась в огромную, многомиллиардную отрасль организованной преступности. Если в Европе правоохранителям удается препятствовать созданию хакерских школ, академий, курсов повышения квалификации, то за пределами Европы они создаются все больше и больше. В результате, если уровень профессионализма в

легальном секторе либо растет медленно, либо даже падает, то в киберпреступность приходит все большее число талантливых программистов и разработчиков.

Огромной угрозой для правоохранителей является хорошо финансируемое развитие стеганографии или шифрования. В условиях огромного спроса на шифрование личных и корпоративных данных эта отрасль информационных технологий не испытывает недостатка в финансировании, кадрах и внимании. Известно, что преступные синдикаты стараются переманить работников, занятых в военном, разведывательном и коммерческом секторах шифрования и стеганографии. Ни в одной из стран-членов ЕС нет порядка обязательного возобновления работникам, имевшим допуск к секретной и сверхсекретной информации о новых местах работы, как это принято, например, в разведке или в отрасли, связанной с атомными материалами. В итоге, предлагая более высокую оплату, преступным синдикатам удается переманивать кадры. Помимо доступа к уже имеющимся системам шифрования высококвалифицированные профессионалы создают для организованной киберпреступности собственные средства шифрования сетевого трафика, подчас превосходящего возможностью его расшифровки правоохранительными органами.

РЕКОМЕНДАЦИИ

В порядке повышения эффективности мультиюрисдикционных операций правоохранительными органами стран ЕС и ЕВРОПОЛА против киберпреступных групп и сообществ целесообразно сосредоточиться на следующих основных направлениях:

– отказаться от реактивного в пользу проактивного подхода, связанного с борьбой с киберпреступностью. Осуществить подготовку необходимых мер на национальном и общесоюзном уровне, изменения в законодательство, подзаконные акты, процедуры и программы, обеспечивающие проактивный подход. Сосредоточить внимание на разработке мощных систем постоянного мониторинга персон и сообществ с повышенным риском, как основы превентивного реагирования на угрозы.

– укреплять и развивать отношения с частным сектором и научными кругами в части повышения уровня интернет-безопасности и борьбы с киберпреступностью.

– всемерно развивать систему анализа вредоносного программного обеспечения (EMAS), созданного ЕВРОПОЛОМ.

Рекомендуется в рамках борьбы с киберпреступностью при всемерном развитии программно-аппаратных методов борьбы не забывать такие испытанные полицейские методы, как работа под прикрытием и агентурная работа. Наиболее впечатляющие успехи последних лет в борьбе с киберпреступностью были связаны не с программными средствами, а с успешными полицейскими операциями «на земле».

Целесообразно приступить к разработке технических, организационных, процедурных и программных требований к созданию единой в рамках ЕС базы данных по киберпреступности, включающей информацию по персоналиям, группам, преступным организациям, сведения о вредоносном софте, базы данных кейсов и т. п.

Активизировать работу правоохранительных органов стран-членов ЕС и ЕВРОПОЛА в части большей информационной осведомленности частного сектора и общества относительно масштабов и направлений киберпреступности. Обобщить и распространить передовой опыт создания ориентированных на школы, университеты и семьи курсов личной информационной гигиены и корпоративной информационной безопасности.

ИНТЕРНЕТ-СЕКСУАЛЬНАЯ ЭКСПЛУАТАЦИЯ ДЕТЕЙ (CSE)

CSE является постоянно развивающимся явлением, вовлекающим в свой оборот все новых граждан стран-членов ЕС. CSE является очень динамичным процессом, эксплуатирующим наиболее низменные человеческие страсти за счет наиболее развитых информационных технологий. Прорывы последних лет, связанные с дешевым широкополосным доступом к интернету повсеместно в странах ЕС, повышение качества и надежности передачи видеотрафика на дальние расстояния и наступление эры шифрования и анонимности стимулировании развитие CSE. В качестве основных направлений угрозы можно выделить преступную деятельность в пиринговых средах и darknet, прямую трансляцию сексуального насилия над детьми под заказ, сексуальное вымогательство, а также использование детей при оказании садомазохистских услуг и зрелищ. Приходится отметить стремительно растущий уровень компетентности правонарушителей с точки зрения использования самых современных средств шифрования и доставки контента. К сожалению приходится констатировать, что за последние годы, несмотря на то, что Европол обращал на эту проблему самое пристальное внимание, ситуация продолжает ухудшаться.

В значительной мере это связано с тем, что провайдеры услуг, связанных с CSE расположены за пределами Европы, в основном в Юго-Восточной Азии, Латинской Америке и некоторых странах Юга и Востока Европы. Соответственно Европол не имеет юрисдикции осуществлять преследование преступников в этих странах или даже блокировать соответствующие каналы.

Ключевая угроза – пиринговые сети

Пиринговые сети остаются основной средой для доступа к видео, содержащего сцены жестокого обращения с детьми, а также киберпространством распространения самими детьми и подростками нескромного контента. Пиринговые сети неизменно привлекательны для правонарушителей из-за простоты в использовании и надежности в анонимизации.

В условиях избыточного предложения облачных хранилищ киберпреступники получили эффективные средства хранения фото и видеоколлекций. Привычный способ борьбы с киберпреступниками в этой сфере путем их ареста и изъятия коллекций более не работает. Даже при задержании преступников коллекции, хранящиеся в зашифрованных облачных хранилищах, продолжают демонстрироваться теми, кто остался на свободе.

Необходимо подчеркнуть, что, по мнению научного сообщества, в ближайшем будущем пиринговые сети будут развиваться гораздо быстрее, чем интернет. При этом нет никаких оснований запрещать подобные сети. Соответственно правоохранительные органам с каждым годом придется работать во все более неблагоприятной среде, создающей дополнительные возможности для киберпреступников.

Ключевая угроза – Darknet

Наиболее благоприятной для преступников средой является darknet, в том числе сеть Tor. Ни одна другая среда, включая традиционные пиринговые сети, не предоставляет преступникам такого уровня анонимности, возможности транслировать потоковое видео и создавать торговые площадки.

Несмотря на публикации в американских научных журналах о возможности деанонимизации Tor, европейским экспертам и правоохранительным органам не известны случаи успеш-

ной программно-аппаратной деанонимизации. Наибольшие успехи в борьбе с педофилами в сети Tor в странах-членах ЕС достигнуты полицией Нидерландов, которая максимально использует старые проверенные методы работы под прикрытием и создание сети осведомителей.

Ключевая угроза – живые трансляции

В ближайшем будущем Европол ожидает взрывного роста услуг с предоставлением платного видеоконтента, связанного как с жестоким обращением с детьми и подростками, так и с трансляцией нескромных видео, осуществляемыми самими детьми и подростками.

Европол связывает это с тем, что в ближайшие два-три года интернет придет в наиболее бедные страны Азии, Африки и районы Латинской Америки. Чтобы заработать хоть какие-то деньги, любые натурные сцены будут организовывать не преступные синдикаты, а непосредственно дети и их родители в этих районах. Преступники будут заниматься только техническим обеспечением, продюсированием и коммерциализацией. Есть основания полагать, что Европа станет местом сбыта экзотических сексуальных видео, связанных с детьми. Параллельно с повсеместным распространением гаджетов, можно ожидать лавинообразного нарастания вымогательств подростков и родителей, связанных с недопущением в открытый доступ откровенных сцен, связанных с детьми и подростками.

Большой опасностью является низкая стоимость для потребителей контента с сексуальным насилием над детьми. Если еще два-три года назад данный вид контента был доступен только для лиц с высокими доходами, то сегодня он стал общедоступным. Помимо прочего, удешевление подобного видео приводит к тому, что полиции все труднее отслеживать оказание трансферты, связанные с данными услугами. Если относительно крупные суммы денег хорошо отслеживаются, то частые небольшие переводы не поддаются какому-либо контролю.

В последнее время полицейские силы ряда европейских стран выявили новый вид преступности, совмещающей онлайн и офлайн. В этом виде преступности трансляция потокового видео, связанного с сексуальным насилием над детьми является не только платным продуктом, но и одновременно приглашением посетить соответствующую страну и заняться тем же уже в реале. Полициям Нидерландов и Германии удалось раскрыть в 2015 г. группу, которая оказывала видео-туристические услуги для педофилов.

Основная угроза – онлайн привлечение и сексуальное домогательство

Как уже отмечалось, интернет-гиганты в коммерческих целях насаждают у детей, подростков и молодых людей привычку фиксировать каждый момент своей частной жизни в виде видео- и фотоконтента, выкладывая его на всеобщее обозрение. В результате, фото и видео, которые являются абсолютно приемлемыми для просмотра в кругу семьи или с доверенными партнерами, оказываются в открытой сети или хуже – в руках преступников, которые имеют мощный софт, позволяющий транслировать непосредственно с камер, фото и видео в специальные хранилища. В 2015 г. в Бельгии впервые были раскрыты две группы, которые установили контроль над видеокамерами в частных домах нескольких городов страны и использовали полученное видео для вымогательства и шантажа.

В Чехии удалось пресечь деятельность преступной группировки, которая в обмен на подарки и небольшие суммы денег просила детей в возрасте 10–13 лет делать определенные видео и фотографии и передавать им. В последующем материал был использован частично для трансляции на платных каналах, частично для шантажа.

В предельных случаях онлайн вымогательство может превратиться в сексуальное домогательство, где жертвы начинают совершать контролируемые поступки под угрозой распро-

странения непристойных материалов в сети. Такой образ действий отражает общую тенденцию, проявившуюся в последние годы в Европе, к все более экстремальным насильственным и унизительным для жертв видам преступлений.

Ключевая угроза – коммерческое распространение контента для педофилов

Существует необходимость более полного понимания тенденций в области монетизации и онлайн коммерческого распространения CSE. Поскольку спрос на такие услуги, хотя и создает рынок, измеряемый десятками миллионов долларов, в процентах к общей численности населения, к счастью предельно мал. Соответственно он специализирован не по страновому принципу, а по потребляемому контенту. Это привело к тому, что, хотя потребительский рынок расположен в самой Европе, организованные преступнее группировки, контролирующие рынок, базируются либо в странах, недавно вступивших в ЕС, либо за пределами Европейского Союза.

В условиях реализации концепции свободного интернета Европа страдает от того, что рекламные материалы по CSE размещаются в открытом интернете. Поскольку не существует признанного всеми странами перечня автоматически блокируемых интернет-ресурсов, преступники используют некоторые юрисдикции для того, чтобы размещать в открытом интернете фрагменты, привлекающие внимание, а также тексты с инструкциями, где можно найти соответствующий материал в пиринговых сетях или сети Tor. В этой связи было бы целесообразно начать проработку в рамках ООН обязывающего соглашения о безусловном запрете использования открытого интернета для определенных видов контента вне зависимости от юрисдикции его размещения.

Ключевая угроза – анонимные сети и трудность в определении правонарушителей

Как уже отмечалось, CSE преступники поставили себе на службу новейшие достижения информационных технологий и в настоящее время чувствуют себя комфортно и безопасно. По экспертным оценкам, в настоящее время полиции становится известно не более 10 % общего объема видеоконтента с CSE, причем наказывают примерно каждого пятого преступника, промышляющего этим видом киберпреступности.

За последние два-три года резко возрос технический уровень преступников. Использование сложнейших систем шифрования трафика, распределенных облачных файловых хранилищ, самоуничтожающихся серверов и компьютеров в настоящее время считается для преступников не исключением, а нормой. В Tor действует несколько онлайн-курсов по азбуке препятствования полицейским расследованиям.

Преступники используют распределенный хостинг. По данным на 2014 г. основным местом хостинга сайтов в открытом интернете, содержащих видео-, фото- или текстовой контент, как прямого, так и рекламного содержания, связанный с CSE, 37 % приходилось на США, 24 – на Россию, 16 – на Нидерланды и 11 – на Канаду.

Будущие угрозы и развитие

Исторически сложилось так, что CSE преступники идентифицировались полицией в ходе определения IP адресов. Однако с произошедшим в течение трех последних лет перетоком педофилов в пиринговые сети и darknet, подобный метод идентификации работает все хуже

и хуже. Кроме того известно, что в настоящее время преступники расходуют значительные ресурсы на создание глубоких анонимных сетей, затрудняющих установление связей между интернет-контентом и пользователем. В этих условиях представляется, что при всех упованиях на технические средства борьбы с CSE преступниками традиционные методы сохранят свое значение.

Ключевую роль, по крайней мере, в ближайшее время будет играть работа «на земле», осуществление операций под прикрытием, широкое использование возможностей деятельного раскаяния в борьбе с преступниками. Фактом является увеличение присутствия интернета в жизни детей и подростков. Согласно результатам недавнего исследования в Великобритании дети в возрасте от 5 до 12 лет тратят 14 часов в неделю на пребывание в интернете. Уже сегодня более 60 % детей в странах-членах ЕС в возрасте до 14 лет имеют мобильный телефоне с доступом в интернет. Еще в 2012 г. таковых было меньше 15 %. Можно смело предположить, что новые технологии, такие как гарнитуры виртуальной реальности, подстегнут CSE. Индустрия развлечения для взрослых является сегодня главным заказчиком для новых медиаформатов и новых технологий. Как показывают исследования, наибольшие деньги на рекламу и развитие новых визуальных технологий приходит именно их этой сферы, которая требует от разработчиков обеспечить все более высокую степень погружения и имитации реальности и интерактивности.

Рекомендации

Правоохранительные органы стран-членов ЕС должны постоянно оценивать уровень своей готовности в борьбе с CSE. Они должны взять на вооружение все доступные программно-аппаратные средства для превентивного пресечения трафика, связанного с CSE. Ключевым направлением борьбы с CSE является установление прямых и оперативных контактов правоохранителей стран-членов ЕС и Европола с компаниями в ЕС и за его пределами, предоставляющими услуги хостинга. Необходимо добиться положения, когда уже в досудебном порядке данные компании при предъявлении им доказательств о наличии на тех или иных ресурсах материалов, связанных с CSE, отключало бы их хостинг.

До сих пор остается неясной структура киберпреступности в сфере CSE. В этой связи на основе кооперации правоохранительных органов стран ЕС необходимо провести дополнительные специализированные исследования относительно геолокации, организационных форм преступных группировок CSE и их связи с традиционной организованной преступностью. Правоохранительные органы должны резко активизировать работу по прекращению деятельности групп в международных социальных сетях, прямо или косвенно способствующих потреблению контента CSE. В кратчайшие сроки законодательным органам стран-членов ЕС и законодательным органам ЕС необходимо разработать и принять поправки к национальным и общеевропейскому законодательству, позволяющие осуществлять тайную работу в киберпространстве и в реальной среде по ликвидации CSE.

Принимая во внимание все ширящийся трансграничный характер CSE, целесообразно выйти с инициативой создания постоянно действующей рабочей группы по CSE в составе представителей Европола, правоохранительных органов США, России, Китая, Индии и региональных структур Юго-восточной Азии. Такая структура может быть создана отдельно, либо как постоянно действующая группа в структуре Интерпола.

Учитывая, что с каждым годом киберпреступность, связанная с CSE все больше уходит в пиринговые сети и в сеть Tor и, принимая во внимание достаточно низкую эффективность работы правоохранительных органов стран-членов ЕС в этих сетях, целесообразно скоординировать усилия в этой области с другими странами. Необходимо обратиться с просьбой к ФБР – предоставить Европолу техническое и программное содействие по улучшению деано-

нимизации пользователей сети Tor, включая не только торговые площадки, но и потребителей незаконного контента.

ПЛАТЕЖНЫЕ МОШЕННИЧЕСТВА

В 2015 г. количество платежных карт, выпущенных в ЕС, составило более 1,1 млрд., что составляет примерно две платежных карты на душу населения. В 2015 г. через платежные карты было осуществлено транзакций на сумму 90 млрд. евро, при средней величине транзакции 57 евро.

В настоящее время на безналичные платежи в странах ЕС приходится уже почти две трети всего розничного товарооборота и оборота услуг. По оценкам специалистов к 2020 г. наличный оборот, если и сохранится, то не будет превышать 10 % от всего оборота. Стремительно растущая доля безналичных платежей породила гонку кибервооружений в сфере платежной преступности и контрмер со стороны банковско-финансового сектора и государств. Хотя в настоящее время отсутствуют достоверные данные о масштабах платежной преступности, согласно оценкам британских правоохранительных органов (наиболее продвинутых в этом направлении среди стран-членов ЕС), объем платежной преступности растет темпами порядка 20–25 % ежегодно.

В 2014 г. согласно отчету SEPA, общая стоимость мошеннических операций с использованием платежных карт превысила в ЕС 1,6 млрд. евро, что составляет рост порядка 10 % по сравнению с предыдущим годом. Как видим, данная цифра более чем в два раза ниже, чем британские показатели. Разница в значительной степени обусловлена различными методиками. Британский анализ использовал как прямые, так и косвенные данные, а также результаты отдельных обследований в банковской сфере. Что касается отчета SEPA, то он был составлен исключительно на основе данных государственной статистики и статистики правоохранительных органов.

В то же время в отчете SEPA указывается, что рост мошенничества, связанного с подделкой и кражей карт, составляет в настоящее время примерно 20 %. Согласно отчету SEPA, практически не растет объем мошенничества, связанного с поддельными транзакциями, а также мошенничеством с банкоматами. Вероятно, данные цифры не отражают реального положения дел.

Согласно данным ЕВРОПОЛА, банковские институты в редких случаях оповещают правоохранительные органы о внедрении в свои транзакционные сети и перенаправлении части платежей, либо о добавлении платежей к традиционной их сумме с последующим перенаправлением добавленных платежей на счета преступников. Такая позиция финансовых институтов связана с тем, что в постсноуденовский период они боятся, что правоохранительные органы поставят под контроль их транзакционные сети, в результате чего они могут столкнуться с большим количество исков со стороны частных и корпоративных клиентов.

Ключевая угроза – скимминг

В 2014 году только три государства-члена ЕС отметили увеличение числа преступлений, связанных с мошенничеством непосредственно с банкоматами.

Все три случая относятся к Восточноевропейским странам. В Западной Европе преступность, связанная с мошенничеством с банкоматами, резко снижается. Это связано с двумя обстоятельствами. С одной стороны, и это в текущем году было главным, практически все западноевропейские банки вложили очень крупные суммы денег в улучшение системы информационной защиты платежных сетей банк-банкомат. Уровень защиты оказался непреодолимым для одиночных, неорганизованных киберпреступников, которые в основном и промыш-

ляли мошенничеством с банкоматами. С другой стороны, в 2015 г. впервые в Европе появились бесконтактные платежные системы. Появление бесконтактных платежных систем резко ускорят в ближайшем будущем вытеснение наличных денег не только из государственного, но и частного оборота. В ближайшем будущем банкоматы в Западной Европе просто исчезнут.

Несмотря на неблагоприятные тенденции скиммеры продолжают совершенствовать свои инструменты и устройства, в основном в направлении миниатюризации. Можно также заметить тенденцию, что западноевропейские скиммеры начинают вахтовым методом или дистанционно действовать в Восточноевропейских странах-членах ЕС, Турции и Мексике.

В целом в ЕС в 2015 г. скиммерство снизилось на 26 %. При этом потери населения от скиммерства уменьшились лишь на 13 %. Это происходит главным образом из-за того, что обналичивание скомпрометированных карт происходит за пределами ЕС, в основном в Южной Америке и Юго-Восточной Азии, в первую очередь в Индонезии и на Филиппинах. Известно, что албаноязычные ОПГ, контролирующие скиммерство в ЕС, создали в Индонезии, Таиланде и Филиппинах постоянные базы, используемые для обналичивания скомпрометированных карт.

Ключевая угроза – вредоносный платежный софт

Следует выделить несколько основных направлений разработки и использования софта, связанного с карточным мошенничеством.

• Скиммингсофт – вредоносные программы, замаскированные под развлекательные. Торговые и иные приложения для смартфонов. Будучи внедренными в программную среду смартфона, они считывают карточные идентификаторы и позволяют удаленно пользоваться чужими банковскими и иными счетами.

• Джекпотинг представляет собой метод, который позволяет взять под контроль и использовать электронный кошелек, коими в настоящее время являются смартфоны и гаджеты. Если скиммингсофт позволяет удаленно компрометировать платежные средства, и прежде всего платежные карты, то джекпотинг означает фактически кражу электронного кошелька. При этом, обладатель электронного кошелька не понимает, что кошелек у него украли и продолжает им пользоваться. Как правило, при использовании джекпотинга преступники используют метод дополнительной транзакции, которая добавляется к любой реальной транзакции, осуществляемой владельцем кошелька. Обычно размеры такой транзакции не превышают одной десятой процента на каждую транзакцию.

• Блекбокс – принципиально новый вид преступлений. Своим появлением он обязан тому факту, что не менее 30 % продаваемых в ЕС гаджетов производится на тех же заводах, что и официальные продукты, но нелегально и продаются под произвольными брендами, по гораздо более низкой цене, чем оригиналы. В данных гаджетах устройство, позволяющее красть электронные кошельки, использовать платежные мошенничества и т. п. реализованы не на программном, а на аппаратном уровне. Соответственно, самый строгий софт-контроль, включая установку антивирусных программ, не показывает компрометацию гаджетов.

• Человек посередине – отмирающий, но еще существующий в Восточноевропейских странах вид мошенничества с платежными картами. В большинстве Восточноевропейских стран-членов ЕС при использовании платежных карт помимо владельца кары с ними соприкасается продавец в магазине, официант в ресторане и т. п., которые, используя технические устройства, компрометируют карты. В Западной Европе подобный тип преступности практически уже вымер.

• Ключевое мошенничество – торговые рынки скомпрометированных платежных карт. Поскольку в последние годы многие азиатские, африканские и латиноамериканские страны пытаются создать собственные замкнутые платежные системы, а также перенесли на свою тер-

риторию центры идентификации глобальных платежных систем, в 2015 г. бурно стали развиваться глобальные торговые площадки, в основном в darknet. Главным товаром на этих торговых площадках являются скомпрометированные платежные карты. Как правило, они приобретаются оптом покупателями из латиноамериканских, азиатских, африканских стран. Далее в этих странах они продают их индивидуальным покупателям. Существование рынков связано с тем, что, если в ЕС и странах Северной Америки четко и быстро работает информационная система отслеживания скомпрометированных карт, то в других районах мира она отсутствует, либо работает плохо. Поэтому скомпрометированную карту, которую невозможно использовать в Европе и Америке можно еще в течение недели, а то и месяца использовать в Азии, Африке и Латинской Америке.

Согласно данным операторов Visa и MasterCard, примерно 70 % ущерба, нанесенного владельцам карт в Европе связано с обналичиванием этих карт в других регионах мира. Пока отсутствует глобальная система отслеживания скомпрометированных карт в масштабах все планеты.

Ключевая угроза – транзакционное мошенничество

Наиболее быстрорастущим видом финансовой киберпреступности в ЕС является транзакционное мошенничество. Еще два-три года назад подобных преступлений не было. Появление и быстрый рост транзакционных мошенничеств связан с тремя группами факторов.

Первая группа факторов – это повсеместное распространение электронных кошельков, в качестве которых используются гаджеты. В 2015 г. в Европе появились и сразу приобрели популярность приложения к операционным системам android и iOS, позволяющие превращать смартфоны в мультикарточные электронные кошельки. При помощи гаджетов потребители теперь могут не только пользоваться кредитными картами сразу нескольких платежных систем, но и своим расчетным счетом в банке, а также различного рода скидочными картами. По состоянию на 2015 г. такие электронные кошельки были лишь у 6 % потребителей в странах Западной Европы. Однако, по мнению различных научных и бизнес-организаций, этот рынок является наиболее быстрорастущим финансовым рынком и к 2017 г. уже как минимум половина совершеннолетнего населения Западной Европы будет пользовать не привычными бумажниками, а мультикарточными электронными кошельками и гаджетами.

Вторая группа факторов сопряжена с эволюцией самих платежных систем. Если до 2013 г. монополию на рынке финансовых транзакций держали системы SWIFT, а также транзакционные системы крупнейших карточных операторов, то в 2014–2015 гг. картина начала стремительно меняться. Появляется все больше независимых платежных систем. Особо высокими темпами их количество растет в Европе. В немалой степени это связано с тем, что в Европе очень много лиц, занятых на промышленных предприятиях, в городском хозяйстве и т. п., не имеющих постоянного гражданства в странах-членах ЕС. Соответственно они отсылают огромные массивы денег, по оценкам – более 15 млрд. евро в год, своим семьям в основном в Африку и Азию. Все эти средства в основном приходятся на новые платежные системы, которые осуществляют переводы намного дешевле, чем классические операторы. Новые платежные системы, использующие как правило блокчейн, пока не имеют такой мощной защиты, как традиционные карточные операторы, и тем более система SWIFT.

Наконец, третья группа факторов связана с тем, что в настоящее время в странах-членах ЕС все публичные места оборудованы Wi-Fi. Данный тип сетей не имеет зашиты от хакеров. Поэтому при подключении смартфонов и гаджетов к Wi-Fi велика опасность проникновения вредоносного софта.

В итоге, хотя в настоящее время транзакционная преступность невелика по объему, она демонстрирует экспоненциальные темпы роста. Киберпреступники, как правило, не крадут

электронные кошельки и даже не компрометируют кредитные карты, а просто подключаются к электронным кошелькам и добавляют в каждую транзакцию микроплатеж. Анализ, проведенный исследовательскими центрами нескольких европейских университетов, показывает, что в данной области, требующей высочайшего уровня квалификации, действуют преимущественно киберпреступники из России и Великобритании.

Будущие угрозы и развитие

В западноевропейских странах-членах ЕС в последние годы быстро развивается 3D печать. Согласно данным Ассоциации 3D печати, Германия, Франция, Нидерланды и Великобритания входят в десятку стран, наиболее широко использующих 3D печать в индустрии и в быту. В 2015 г. в пяти странах ЕС были раскрыты группировки скиммеров, которые использовали 3D печать для фабрикации поддельных кредитных карт для стран, находящихся за пределами Европы. При этом в качестве матриц для 3D печати они использовали скомпрометированные в Соединенных Штатах и странах-членах ЕС карты. Все группировки, так или иначе, были связаны с Балканскими преступными сообществами, действующими в Европе и Южной Азии. Есть основания полагать, что данный высокотехнологичный вид преступности и далее будет активно развиваться.

Несомненно, наиболее быстрыми темпами будет расти преступность, связанная с гаджетами, как новым электронным кошельком и инструментом бесконтактных платежей. Если в 2011 г. по данным Visa Европа на бесконтактные транзакции приходилось 0,7 % от общего количества розничных транзакций, то в 2013 – 4 %, а в 2015 – 9 %. Это самый быстрорастущий финансовый мировой рынок. С учетом того, что в ЕС существует наиболее критическое отношение к наличным деньгам по сравнению с США, Россией, Китаем и другими регионами и странами, есть основания полагать, что в Европе электронные кошельки для бесконтактных платежей получат в ближайшей перспективе наибольшее развитие. При этом, как уже отмечалось выше, в Европе же имеет место наиболее полное покрытие Wi-Fi, а также разнообразие марок продаваемых гаджетов.

Вследствие комбинации данных факторов ЕВРОПОЛ ожидает в ближайшие годы экспоненциальный рост транзакционных платежных мошенничеств в Европе. При этом, поскольку это наиболее высокотехнологичный вид киберпреступности, требующий высочайшего уровня программистских и математических знаний, есть все основания полагать, что действовать на территории ЕС наряду с внутренними организованными преступными группировками будут хакерские команды из США, России, Индии. Это создаст дополнительные сложности для обнаружения, расследования и тем более предупреждения традиционных преступлений. Проблемы юрисдикции могут свести на нет не только усилия правоохранителей, но и эффективность тех или иных программно-аппаратных решений по борьбе с данным видом киберпреступности.

Рекомендации

Правоохранительные органы должны стремиться к активному развитию многосторонних инициатив, включая инициативы Европола по борьбе с мошенничеством. В рамках инициативы они должны не только укреплять кросс-государственные связи и обмен информацией, но и инициативно формулировать предложения по созданию в структуре Европола новых групп и команд по борьбе с наиболее опасными типами киберпреступности в платежной сфере. Государства-члены ЕС должны активнее контактировать с системой EMAS, своевременно направляя в нее новые образцы вредоносных программ и кода, используемых киберпреступниками. В целях снижения риска вредоносных атак на платежную систему правоохранительные органы должны содействовать выполнению на межнациональном и международном уровнях «Руко-

водящих указаний и рекомендаций Европола относительно кибератак на банкоматы, банки и платежные системы».

Правоохранительным органам различных стран необходимо повысить координацию в борьбе с торговыми площадками со скомпрометированными платежными картами и усилить свое сотрудничество под эгидой Европола и Интерпола с правоохранительными органами стран, где находятся основные покупатели скомпрометированных карт.

Необходимо создать постоянно действующую межведомственную и кросс-национальную рабочую группу Европола по борьбе с транзакционной киберпреступностью. Целесообразно пригласить к участию в этой группе представителей финансовых, деловых структур ЕС, а также представителей других стран и регионов с развитыми информационными технологиями.

Настоятельно необходимо реализовать в жизнь ранее принятые решения о создании в рамках ЕС специального защищенного канала для правоохранительных органов стран-членов ЕС, по которому они могли бы передавать всю необходимую информацию, касающуюся, в том числе, киберпреступности в финансовой сфере, и в первую очередь криминальных группировок, действующих в сфере транзакционной преступности и преступлений, связанных с платежными картами.

Необходимо также, как уже упоминалось в связи с CSE, установить рабочие взаимоотношения с хостерами во всех основных юрисдикциях, с тем, чтобы не допускать размещения в открытой сети интернет какой-либо информации, позволяющей продавать или распространять сведения о скомпрометированных картах. Применительно к транзакционной преступности и преступности с платежными картами, как никогда актуальными являются предложения активизировать контакты с ФБР относительно работы в сети Tor.

Правоохранительным органам стран-членов ЕС необходимо обратиться к исполнительным и законодательным органам своих стран, финансовым институтам с просьбой ассигновать необходимые ресурсы для разработки эффективного инструментария, позволяющего снизить ущерб от транзакционной преступности и преступности с электронными кошельками для бесконтактных платежей. Необходимо довести до сведения властей, что в условиях экспоненциального нарастания данного вида преступности у правоохранительных органов отсутствует программный инструмент, позволяющий активно противодействовать криминалу.

Необходимо сосредоточить усилия на унификации законодательства в различных странах-членах ЕС, а также упрощении юрисдикционных процедур в сфере карточного мошенничества, платежных систем и транзакционной преступности.

СОЦИАЛЬНЫЙ ИНЖИНИРИНГ

Независимо от того, сколько ресурсов компании и государственные органы и общественные организации, а также граждане тратят на информационную безопасность, они не могут полностью защитить свою информацию. Самым слабым звеном в информационной безопасности является человек. В одних случаях человеческий фактор сводит на нет огромные ассигнования и значительные усилия из-за ошибок, недостаточного уровня квалификации программистов, системных администраторов, специалистов по информационной безопасности. В других случаях, а таких большинство, инсайдер внутри компании целенаправленно и с выгодой для себя нарушает или даже разрушает транзакционную безопасность, осуществляет те или иные преступные действия. До публикации настоящего доклада, насколько известно, социальный инжиниринг, как важнейший элемент и направление киберпреступности не рассматривался правоохранительными органами какой-либо страны мира и какой-либо части света.

Под социальной инженерией понимается информационная атака, т. е. несанкционированное получение информации в корыстных целях. При этом получение информации осуществляется против воли и цели как лица, через которое получена информация, так и владель-

цев компании или ее руководителей. Следует отметить, что борьба с социальной инженерией в настоящее время практически невозможна в силу отсутствия в законодательстве всех стран-членов ЕС статей, квалифицирующих социальную инженерию, как уголовно или административно наказуемый вид деятельности.

Включением данного раздела в доклад, Европол стремится инициировать не только общественность, но и законодателей на рассмотрение этого вопроса с четким вычленением тех аспектов социальной инженерии, которые носят априори преступный характер и должны получить соответствующую законодательную оценку.

Необходимость этого связана с тем, что в настоящее время социальная инженерия превратилась в один из самых распространенных векторов атак на информацию, от которых сложнее всего защититься. К тому же тщательный анализ киберпреступности показывает, что практически по всем направлениям наиболее опасных и быстроразвивающихся видов киберкриминала имеет место сложное сочетание социальной инженерии с применением вредоносного софта.

Ключевая угроза – фишинг

Практически все государства-члены ЕС отмечают стабильную тенденцию к увеличению фишинга в их юрисдикциях. Главной мишенью фишинг-компаний в 2015 г. наряду с частными лицами были финансовые институты.

Следует констатировать, что ценой очень существенных затрат финансовым институтам удалось в 2015 г. заметно снизить ущерб от фишинг-атак. Результата удалось добиться за счет массового внедрения мощных систем, оснащенных элементами искусственного интеллекта, распознающими фишинговые письма и сообщения в общем объеме электронной документации.

В 2015 г. основной объем фишинг-атак приходится на англоязычные и франкоязычные страны и районы ЕС. При этом главным источником франкоязычных фишинг-атак является франкоговорящая Северная Африка, а англоязычных фишинг-атак Карибы. Качество и количество фишинга за последние несколько лет значительно увеличилось из-за больших успехов, достигнутых автоматическим переводом и прежде всего переводом Google.

В то время как компании вкладывают значительные средства в повышение информационно-коммуникационной безопасности, на первый план выступают прорехи «в человеческом брандмауэре». По мнению экспертов в Европе на гораздо более низком уровне, чем в США и России ведется подготовка кадров в области кибербезопасности и информационной гигиены в корпоративном секторе. Например, в Соединенных Штатах и в России никому в голову не придет открывать так называемые «нигерийские письма». Между тем, проведенные в Германии в 2014 г. исследования показали, что эти письма были открыты корпоративными пользователями в 23 % случаев, и в 11 % случаев привели к заражению корпоративных систем.

Для нецелевых атак основным способом распространения фишинговых писем является спам. К несомненным успехам международного сотрудничества следует отнести тот факт, что вот уже третий год уровень спама в странах-членах ЕС падает. Успешная борьба со спамом показывает, что в тех случаях, когда удается обеспечить международное сотрудничество и соединить подготовку кадров с применением эффективных программных средств, с киберпреступностью можно бороться успешно.

Основная угроза – мошенничество топ-менеджмента

Несколько стран-участниц ЕС, а также банковские ассоциации сообщили об увеличении в 2015 г. так называемой «беловоротничковой» киберпреступности. Это – различного рода

преступления топ-менеджмента, в основном в финансовой сфере, осуществляемые с использованием информационных технологий.

Еще более быстрыми темпами растет преступность, связанная с мошенническим присвоением прерогатив топ-менеджмента социальными хакерами. Один из наиболее широко используемых методов социального инжиниринга – это подключение к внутрикорпоративным телефонным линиям или информационным каналам с последующим сообщением персоналу якобы от имени генерального директора или его замов той или иной информации. Поскольку персонал привык доверять корпоративным информационным системам и телекоммуникациям, он принимает такие указания за чистую монету. Как правило, работникам поручается либо передать в адрес руководства ту или иную информацию или срочную справку, либо осуществить тот или иной платеж.

Если на начальном этапе хакеры пользовались в основном электронной почтой, то в 2015 г. гораздо большее распространение получили пранкерские технологии. При их применении группировка первоначально взламывает корпоративный канал оперативной телефонной связи или мессенджер, а затем, используя самые современные средства аудиомонтажа, отдает по закрытым каналам голосом начальника те или иные приказы, которые, как правило, исполняются незамедлительно.

В 2015 г. такого рода сложные операции, в которых были задействованы кибертехнологии, связанные с взломом телекоммуникаций, подключением к ним, дополнялись технологией модификации голоса, а также специфическими психологическими приемами, включающими подсознательные активаторы. Все это привело к тому, что нескольким финансовым институтам стран-членов ЕС был нанесен ущерб в 1,6 млрд. евро.

Будущие угрозы и развитие

Поскольку корпоративные взаимодействия все больше и больше уходят из реала в киберсреду, это открывает дополнительные возможности для социальной инженерии. Дополнительным фактором, усиливающим риски социально инженерии для корпоративных структур, становится ширящееся в Европе движение к удаленной работе, использованию аутсорсинга и распределенных безофисных систем. В странах-членах ЕС все больше компаний, в которых работники, включая не только функциональное руководство, но и линейный топ-менеджмент, крайне редко видят друг друга лично, и общаются в основном при помощи мобильных телефонов, мессенджеров и т. п.

В 2014–2015 гг. было широко распространено опасение, что прекращение поддержки все еще широко используемой операционной системы Microsoft XP приведет к новой волне мошенников – социальных инженеров, представляющихся службами поддержки Microsoft. Опасения оказались напрасными. Однако в прошлом году совершенно неожиданно для экспертов резко возросло количество мошенничеств с использование методов социальной инженерии, связанных с бухгалтерской деятельностью.

Принятие ЕС ряда новых стандартов бухгалтерского отчета потребовало для работников бухгалтерии бизнесов различных размеров внести некоторые изменения в свою работу и перенастроить свои программные средства. Поскольку в странах-членах ЕС нет общепринятых единых для всех стран систем бухгалтерского софта, то социальные инженеры, представляясь представителями той или иной фирмы-производителя подобного софта, договаривались о внесении необходимых изменений и коррекций в уже установленных на предприятиях бухгалтерских системах. В итоге, киберпреступникам удалось получить доступ к бухгалтерии тысяч предприятий.

Рекомендации

В ближайшее время законодательным органам стран-членов ЕС, а также комиссиям Европола целесообразно приступить к работе по созданию признаков преступного использования социального инжиниринга, провести кодификацию социального инжиниринга, сформировать формы отчетности и установить наказание за использование социального инжиниринга.

Общая позиция вероятно должна состоять в том, что все методы социального инжиниринга должны относиться к этически осуждаемым, а те из них, которые способны нанести материальный или моральный вред личности, группам или обществу, должны быть отнесены к преступной деятельности с соответствующим наказанием. Едва ли не крупнейшим упущением законодательства стран-членов ЕС и ЕС в целом является игнорирование социального инжиниринга, как быстроразвивающегося, крайне опасного, криминально ориентированного социального явления.

В настоящее время полностью отсутствует межгосударственный и межведомственный обмен информации о методах социального инжиниринга, персонах и группах, его использующих и интеграции киберпреступности и социального инжиниринга. Целесообразно рассмотреть вопрос о создании в структуре или под эгидой ЕВРОПОЛА постоянно пополняемой и находящейся в распоряжении правоохранительных органов стран-членов ЕС базы знаний по социальному инжинирингу, лаборатории анализа и верификации технологий и методов социального инжиниринга и базы данных по оргпреступным группировкам, использующим методы социального инжиниринга.

При проведении работы по сокращению масштабов использования социального инжиниринга в преступной деятельности, необходимо учитывать тот факт, что нигде в мире в настоящее время не существует законодательства, относящего социальный инжиниринг к криминальным видам деятельности. В этой связи надо быть готовым к ситуации, когда в Европе будут действовать социальные хакеры из других регионов мира, где социальный инжиниринг не наказуем. При этом свою работу они будут вести удаленно, находясь в пределах своих юрисдикций.

Все это требует уже сегодня начать консультации между представителями Европола и правоохранительными органами стран, не входящих в ЕС. Заслуживает внимания предложение – в самые ближайшие годы провести под эгидой Интерпола представительное международное совещание по использованию социального инжиниринга в связке с киберкриминалом в преступных целях.

Поскольку, несмотря на ускоренное развитие технологически продвинутых форм социального инжиниринга, социальные инженеры по-прежнему используют фишинг и спам, правоохранительным органам необходимо улучшить координацию с глобальными и национальными провайдерами веб-почты.

ПРЕСТУПНОСТЬ В СФЕРЕ ДАННЫХ

Наиболее быстро растущим видом киберпреступности являются кража, изменение или уничтожение данных. Если в 2013 г. от кражи данных пострадали 300 тыс. компаний и 40 млн. потребителей в Европе, то в 2015 г. – 700 тыс. компаний и 90 млн. потребителей. Не будет преувеличением назвать 2015 г. – годом больших краж Больших Данных. Данные являются цифровой нефтью информационной экономики. Поэтому данные представляют собой наиболее желанный трофей для киберпреступников.

В докладе IOCTA 2014 было подчеркнуто, что в ближайшей перспективе атаки на Большие Данные и их кража станут важнейшим направлением киберпреступности. Поэтому отсут-

ствие отчетности о данном виде преступности заметно искажает общую картину и не нацеливает правоохранительные органы на борьбу с кражей данных.

Нельзя не отметить, что в 2015 г. национальные правоохранительные органы ряда стран ЕС, в первую очередь, Германии, Великобритании, Бенилюкса и Франции ввели необходимую отчетность, а также создали Центры по борьбе с кражей данных, куда вместе с государственными правоохранительными структурами вошли частные электронные охранные компании и подразделения безопасности крупнейших корпораций.

Почти четыре пятых государств-членов ЕС сообщили, что в 2015 г. имел место значительный рост киберпреступлений, связанных с кражей и изменением данных. Более одной трети правоохранительных органов стран-членов ЕС отметили, что ими были обнаружены не только случаи кражи данных, но и находящиеся в пиринговых сетях и сети Tor торговые площадки, где главным товаром являются данные. По сведениям, предоставленным Европолом ФБР, покупателями украденных в странах-членах ЕС данных являются не только преступные группировки и разведки различных стран мира, но и известные корпорации.

По имеющимся данным, в среднем обнаруживается не более 20 % вторжений в корпоративные сети, приведших к утечке данных. При этом не более четверти из них идентифицируются и не более 10 % подобных случаев доводятся до суда.

Таким образом, в настоящее время за кражу данных попадают под суд лишь жалкие проценты от общего числа киберпреступников. С учетом, что цифровые данные – это золото сегодняшней экономики, нет сомнений, что данный вид преступности будет стремительно нарастать. Европейские правоохранительные органы и бизнес, как уже отмечалось, не только обладают менее развитыми инструментами борьбы с киберпреступниками, чем их американские и российские коллеги, но и не отдают себе отчет в опасности для бизнеса и общества этого вида преступности.

Данные крадутся не только для продажи, но и для шантажа. Так, в мае-июле 2015 г. киберпреступники взломали два крупнейших европейских сайта для взрослых, тех, кто ищет внебрачные связи. Преступникам удалось получить всю необходимую информацию о клиентах этих сайтов. В последующем они начали использовать ее для шантажа. О масштабах операции говорит тот факт, что один из сайтов имеет 3,5 млн. зарегистрированных клиентов по всему миру. Сколько из них живет в Европе неизвестно, но, думаем, что очень много. Однако известно, что благодаря краже данных с сайта AdultFrendFinder киберпреступники получили досье, в том числе на 1400 клиентов, которые были определены в качестве руководителей высшего звена компаний из списка Fortune 500.

Большинство нарушений целостности баз данных произошло в результате использования комбинированных методов кибератак и социального инжиниринга, в том числе и изнутри компании. 25 % нарушений были идентифицированы как мошенничества с использованием социального инжиниринга, 20 % – стали результатом инсайдерской деятельности, 15 % – явились следствием физической кражи или потерь данных, и 40 % стали результатом успешных кибератак.

DDOS-атаки

Примерно половина государств-членов ЕС считает DDOS-атаки значительной угрозой, особенно для малого бизнеса и частных граждан. Ежедневно на территории ЕС фиксируются сотни DDOS-атак. Многие из них генерируют трафик более 100 ГГб/сек. Три четверти DDOS-атак достигают своих целей. DDOS-атаки как правило имеют своей целью не борьбу с нежелательным контентом, а обычное вымогательство. В то же время следует отметить, что общее число DDOS-атак в странах ЕС снижается. Значительной степени это связан с тем, что европейским хостерам удалось резко повысить уровень информационной надежности своих ресур-

сов. В этих условиях преступное сообщество, предлагающее DDOS-атаку как услугу, повысили тарифы за осуществление атак. Если в 2013 г. они стоили от 1 до 5 биткойнов, то в 2015 г. – от 12 до 100 биткойнов, в зависимости от уровня защиты ресурса.

Главными сферами DDOS-атак в Европе являются развлекательная индустрия, сайты для взрослых и индустрия онлайн азартных игр. Такой выбор объектов атак связан с тем, что в силу характера деятельности ресурсы зачастую не сообщают об атаках правоохранительным органам, а предпочитают улаживать проблемы при помощи оплаты определенного выкупа.

Будущие угрозы и развитие

На практике, по крайней мере, в Европе, организации, подвергшиеся кибератакам с целью кражи данных, достаточно редко обращаются в правоохранительные органы. Данный факт объясняется твердой убежденностью европейского бизнеса, что правоохранительные органы не только не способны, но и не желают рассматривать сложные киберпреступления, связанные, в том числе, с кражей данных. У них, по мнению бизнеса, для этого нет необходимых кадров, программно-аппаратных средств и, наконец, такие преступления имеют низкий процент раскрываемости, а потому ухудшают полицейскую статистику.

Дополнительный фактор, объясняющий, почему потерпевшие от киберпреступников не обращаются в полицию, связан с репутационным ущербом. Финансовые учреждения, интернет-магазины, торговые сети, наиболее часто подвергающиеся кибератакам с целью кражи данных, не хотят выглядеть в глазах своих клиентов беспечными, не уделяющими должного внимания защите данных, организациями. Как показывают обследования, руководители бизнеса отмечают, что обращения в полицию в связи с кражей данных, как правило, по различным причинам получают огласку в СМИ. Соответственно о краже становится не только известно, но и общество ждет полицейского расследования и наказания виновных.

В ситуации, когда в лучшем случае раскрывается не более 10 % преступлений, связанных с кражей данных, скомпрометированными в глазах общественности оказываются и бизнес, и полиция. В результате, во многих, особенно в Западноевропейских странах-членах ЕС, на которые приходится львиная доля краж данных, сложилось своего рода негласное соглашение между бизнесом и правоохранительными органами. Одни стараются справиться с проблемой собственными силами, а другие – не настаивают на том, чтобы к ним обращались за помощью в раскрытии преступлений, связанных с кражами данных. В перспективе без разрешения этой ситуации масштабы кражи данных будут стремительно увеличиваться и поставят под угрозу бизнес-климат в странах-членах ЕС.

В то же время необходимо исходить из реального положения дел и понимать, что вряд ли только силами полиции удастся решить проблему кражи данных. Это настолько серьезная и быстро растущая проблема, что здесь нужны нетрадиционные решения, аккумулирующие потенциал и возможности всех сторон, заинтересованных в том, чтобы успешно противостоять преступникам.

Рекомендации

Главным условием и одновременно возможностью эффективной борьбы с кражей данных в странах-членах ЕС является формирование на национальном и общеевропейском уровне совместных структур и команд с участием правоохранительных органов, бизнеса, финансовых учреждений и научных центров. Эти команды должны осуществлять мониторинг, анализ, превентивное предупреждение, а в тех случаях, когда этого не удалось сделать – скорейшее обнаружение и задержание киберпреступников, крадущих данные. Такие команды, объединившие правовые возможности, опыт и авторитет правоохранительных органов, с новейшим

инструментарием научных центров и финансовыми и материальными ресурсами бизнеса, смогут успешно противостоять киберкриминалу. Поодиночке ни правоохранительные органы, ни бизнес, включая финансовые круги, не смогут не только подавить, но и уменьшить темпы наращивания преступности.

Наряду с созданием команд действия, необходимо усилить координацию национальных правоохранительных органов как на двух, так и на многосторонней основе. Также необходимо рассмотреть вопрос создания специальной лаборатории при Европоле по анализу приемов и методов кражи данных, имея в виду в первую очередь изучение сложных киберпреступлений, сочетающий использование вредоносного программного кода с методами социального инжиниринга.

Целесообразно национальным правоохранительным органам еще раз изучить системы отчетности, предусмотрев введение в них отдельной строкой киберпреступности, в том числе по отдельным направлениям. Такой подход, как представляется, оградит правоохранительные органы от критики общественности в связи с более низким, чем ранее, уровнем раскрываемости преступлений с одной стороны, и позволит получить более объективную картину тенденций в сфере киберпреступности на европейском континенте, с другой.

С учетом того, что объем затрат, необходимый для диагностики уязвимостей и определения трафика перенаправления украденных Больших Данных очень велик, следовало бы внимательно изучить вопрос создания мощного, оснащенного на самом высоком уровне общеевропейского центра по анализу и прогнозированию преступности в области кражи данных. Такой подход позволил бы при экономии средств каждой страной-членом ЕС изыскать необходимые массивные ресурсы для создания Центра, оснащенного лучшими программно-аппаратными средствами.

Атаки на критическую инфраструктуру

Европейская критическая инфраструктура по-прежнему находится в опасности. Ей все чаще бросаются вызовы со стороны киберпреступных групп, террористов, иных негосударственных субъектов и даже физических лиц. Наиболее уязвимы для атак Системы диспетчерского управления и сбора данных (SCADA), промышленные системы управления (ICS) и система автоматической идентификации (AIS).

В странах-членах ЕС по-прежнему находятся в эксплуатации системы, созданные в 90-е годы, не удовлетворяющие даже элементарным требованиям сетевой безопасности. Поскольку данные системы входят в сети, они ставят под угрозу общую сетевую промышленную и инфраструктурную безопасность ЕС.

Дополнительно в неудовлетворительное состояние с критической инфраструктурой свой вклад вносит осуществляемые без учета технологических последствий сделки по слияниям и поглощениям. Плохое управление, высокая текучесть кадров в отраслях критической инфраструктуры и их насыщенность не только на уровне рабочих, но и инженерного состава лицами, не имеющими постоянного европейского гражданства, резко повышает риски применения к системам принципов социального инджиниринга. В результате, уровень безопасности объектов и сетей критической инфраструктуры ЕС не может быть оценен не только как хороший, но и как удовлетворительный.

Главная проблема состоит в том, что объекты критической инфраструктуры становятся все более взаимосвязанными. В результате в рамках одной сети телекоммуникациями объединяются объекты различных программно-аппаратных поколений, обладающих качественно неодинаковым уровнем автоматизации и информационной защиты. При этом хорошо известно, что безопасность любой сети определяется уровнем информационной безопасности не самых защищенных объектов и даже не средним уровнем, а находится на уровне наиболее

незащищенного объекта или фрагмента. Иными словами, средства, израсходованные компаниями или государством с высочайшим уровнем автоматизации и информационной защиты, оказываются истраченными напрасно из-за того, что существуют незащищенные объекты и фрагменты сетей ЕС.

Известно, что уровень не только экономического, но и информационного развития стран-членов ЕС не одинаков. Если даже на уровне экономики и финансов различия в уровне зрелости создали определенные проблемы, то качественно различное состояние информационной безопасности узлов и сете в различных странах-членах ЕС является крупнейшей угрозой для экономики и функционирования социума в Европе.

Частично тема атак на критические инфраструктуры выходит за рамки данного доклада, поскольку наиболее вероятными субъектами таких атак являются террористические сети и иные негосударственные акторы. Однако в условиях набирающей мощь в Европе тенденции «киберпреступность, как услуга» есть все основания предположить, что технически отсталые и информационно малограмотные террористические сети, располагающие значительными финансовыми ресурсами, могут просто нанять киберпреступников в Европе для осуществления действий против критической инфраструктуры.

Европолу в 2015 г. стали известны данные, которые вызвали колоссальную тревогу и были немедленно доведены до всех правоохранительных органов стран-членов ЕС. Удалось выяснить, что средний срок между проникновением злоумышленников в объекты и сети критической инфраструктуры и обнаружением их составляет более полугода, а именно – около 200 дней. Фактически это означает, что в течение полугода киберпреступники, террористы и другие негосударственные акторы способны беспрепятственно разрушить основу европейской жизнедеятельности, взять ее под управление, в том числе с целью шантажа и вымогательства, или проникнуть через сети критической инфраструктуры в наиболее уязвимые и важные центры государственного управления и европейской безопасности.

Будущие угрозы и развитие

Зависимость европейской экономики и социума от информационно-коммуникационных технологий будет только расти. Одновременно будет нарастать интеграция в телекоммуникационных, энергетических и иных инфраструктурах стран-членов ЕС в единую европейскую инфраструктуру.

К счастью по не вполне ясным причинам, в Европе на сегодняшний день зафиксированы мало случаев кибердиверсий против критических инфраструктур. Однако Европол не видит ни одной причины, почему на данное счастливое стечение обстоятельств следует уповать и в будущем. В дальнейшем мы будем наблюдать увеличение числа кибернападений на брокеров данных и на критические инфраструктуры.

Более того, по мере того, как в странах-членах ЕС вслед за США стремительно начнет набирать силу интернет всего, неизбежно произойдет объединение инфраструктурных сетей с умными домами, кварталами и городами. Данное объединение создает риски не только осуществления крупномасштабных террористических актов, но и подвигнет преступников к переходу от шантажа и вымогательства отдельных семей или личностей к вымогательству муниципалитетов и региональных правительств.

Также неизбежно будет увеличиваться использование существующих уязвимостей нулевого дня, а также ошибок в программном коде, объем которых, согласно обследованиям, непрерывно увеличивается. Наконец, в условиях, когда европейская экономика уже длительное время существует в условиях кризиса спроса и крайне низких темпов, у все большего числа предприятий возникают сложности с проведением технического и программного обновления компьютерных средств. При отсутствии поддержки поставщика и продолжении использования

программно-аппаратных средств с истекшем сроком эксплуатации, еще более снизит и без того невысокий уровень информационной безопасности среднего бизнеса и различного рода инфраструктурных объектов, особенно на региональном и муниципальном уровне.

Укрепление кибербезопасности и борьба с киберпреступностью требует сочетания профилактики, обнаружения и преодоления последствий инцидентов. Наряду с этим правоохранительные органы должны обеспечить неотвратимость обнаружения и наказания виновников. Это ключевая проблема в сфере киберпреступности в Европе. Если в ближайшие годы не изменить ситуацию, когда лишь незначительная часть компьютерных преступлений раскрывается, а еще меньшая часть киберпреступников обнаруживается, и их дела доводятся до суда, то данную проблему решить не удастся. Специалисты в области высоких технологий, склонные к девиантному поведению в погоне за наживой будут с каждым годом все плотнее работать на европейском рынке.

Рекомендации

Для того чтобы правоохранительные органы могли эффективно расследовать данный тип криминала и опережающе реагировать на разрушительные атаки, необходимо в сотрудничестве с частным сектором и научными кругами повысить техническую оснащенность правоохранительных органов и насытить их специалистами в области инженерии данных.

Целесообразно наладить кооперацию правоохранительных органов стран-членов ЕС, предусмотрев закрепление за наиболее мощными в ресурсном и технологическом отношении странами функций координации и обучения правоохранителей других стран в части компетенций базовой страны. Необходимо совершенствовать системы национального законодательства и правоприменительных актов государств-членов ЕС с тем, чтобы обязать все организации, частных граждан, подвергающихся атакам, связанным с кражей данных, сообщать об этом правоохранительным органам.

Целесообразно изучить возможность создания общеевропейского Центра экспертизы и анализа данного вида преступности под эгидой Европола.

Обеспечить выполнение странами-членами ЕС Директивы ЕС об атаках на информационные системы, предусматривающие введение более жестких штрафов и уголовной ответственности за использование вредоносных программ, как способа совершения киберпреступлений. Во всех странах-членах ЕС уровень штрафов и наказаний должен быть не ниже, чем предусмотренные Директивой общеевропейские штрафы и наказания.

Странам-членам ЕС следует рассмотреть вопрос об обеспечении в своих странах расследования инцидентов атак на критические инфраструктуры в соответствии с принципами ENISA.

Странам-членам ЕС целесообразно в рамках Стратегии национальной безопасности создать единые межведомственные подразделения и команды для защиты ключевых национальных объектов критической инфраструктуры.

КРИМИНАЛЬНЫЕ ИНТЕРНЕТ-ФИНАНСЫ

Цифровое подполье зависит от потока денежных средств, разнообразия каналов их поступления и способов отмывки преступных доходов. Преступное цифровое подполье использует как традиционные банковские инструменты и транзакции, так и криптовалюты. Кроме того, цифровое подполье активно использует сложившиеся за пределами Европы нелегальные платежные системы, традиционно используемые террористами, преступниками и т. п.

Платежные механизмы, используемые злоумышленниками, подразделяются на следующие основные категории:

• Традиционные финансовые инструменты, включая банковские счета, платежные карты и т. п.;
• Сервисы денежных переводов, типа Western Union, MoneyGram и т. п.;
• Ваучерные, или чековые системы;
• Онлайн платежные сервисы, типа PayPal;
• Централизованные виртуальные валюты, типа WebMoney и PerfectMoney;
• Децентрализованные виртуальные валюты, типа биткойна;
• Другие предплатежные решения, типа предоплаченных дебетовых карт.

При рассмотрении вопроса, почему киберпреступность использует тот или иной тип платежей, необходимо исходить, прежде всего, из характера сделки. В этой связи могут быть выделены четыре основных сценария.

Межкриминальные платежи

В данную категорию попадают любые платежи, которые осуществляют преступники между собой. В последние годы этот тип платежей быстро растет в связи с тем, что все более широкое распространение получает бизнес-модель «криминал как услуга», Если еще несколько лет назад взаимозачет трофеев, полученных в результате преступных операций, проводился натуральным образом внутри оргпреступных группировок, то в последние годы картина поменялась. Сформировались преступные рынки, где одни преступники продают другим результаты своей деятельности, например, украденные данные, скомпрометированные кредитные карты, наркотики, живой товар и т. п.

Ранее незначительный денежный внутрипреступный оборот осуществлялся в основном либо через системы денежных переводов, типа Western Union, а также в рамках анонимных централизованных платежей, типа Web Money. В последние годы более четырех пятых внутрипреступного оборота ушло в сферу криптовалют. В то же время официальная статистика Европола говорит о несколько иных пропорциях. Согласно данным Европола, на биткойн приходится 40 % внутрипреступных платежей, 25 % – осуществляется через PayPal, оставшиеся 35% делятся примерно в равной пропорции между сервисами перевода наличных денег и теневыми системами типа Хавалы.

Легитимные преступные платежи

К данной категории относятся сценарии, когда злоумышленники осуществляют легальные платежи, используя законопослушные организации. Как правило, таким образом осуществляются платежи, связанные с различного рода бытовыми надобностями, а главное, с приобретением программно-аппаратных средств легального характера. Согласно данным Европола, более 60 % сделок такого рода используют традиционные безналичные виды оплаты, а 40 % приходится на наличную оплату.

Платежи, связанные с вымогательством

В силу резкого увеличения объема преступных услуг, связанных с производством контента, имеющего отношение к педофилии, жестокому отношению к детям, а также завладению различного рода персональными данными и нежелательным для жертв шантажа фото и видео контентом, у преступников появилась потребность в надежных финансовых проводках, опосредующих эту деятельность. Из правоохранительной практики известно, что до 70 % раскры-

тых преступлений, связанных с вымогательством, киднепингом и проч. раскрывалось в момент передачи наличных от жертвы шантажисту или отслеживание прохождения переводов.

Поэтому в настоящее время практически весь объем финансового оборота по этому направлению приходится либо на криптовалюты, либо на обычные банковские расчеты с использованием целой системы оффшорных компаний. В настоящее время на биткойн приходится одна треть платежей, две трети – на банковские трансферты. Однако еще два года назад на биткойн приходилось всего около 5 %.

Платежи, связанные с отмыванием денег

По данным Европола, каждый год примерно на 15–20 % возрастают приходящие в Европу потоки различного рода теневых денег. В большинстве случаев европейские банки являются лишь промежуточным звеном для перевода денег в лежащие за пределами Европы оффшорные юрисдикции, в основном связанные с Великобританией. Основную долю этих денег составляет незаконный вывоз капитала, связанный с преступностью, коррупцией и т. п. в новых индустриальных и развивающихся странах. Первое место в мире по нелегальному вывозу денег в Европу занимает Китай, второе – Россия, третье – Бразилия.

Наряду с незаконным выводом средств, постоянно растет оборот, связанный с обналичиванием скомпрометированных финансовых счетов и кредитных карт. Для отмывания средств в настоящее время наряду с оффшорной схемой широко используются транзакции, включающие в одну цепочку традиционные банковские переводы, переводы в централизованных виртуальных валютах и криптовалютах. Использование сложных схем с разными типами переводов и валют позволяет запутать правоохранительные органы, обрывая цепочки транзакций. В настоящее время более половины денег, связанных с незаконным выводом финансовых средств из страны, а также обналичиванием «грязных» доходов осуществляется с использование традиционных банковских переводов, а при относительно небольших размерах, при помощи бюро переводов наличных. Несмотря на шум в прессе, биткойн по-прежнему занимает лишь небольшую долю подобных сделок. В 2015 г. его доля была меньше, чем у WebMoney.

Будущие угрозы и развитие

Как это ни странно, основная часть использования биткойна в качестве платежного средства происходит при внутриевропейских платежах. Это показывает, что биткойн в настоящее время интересен подавляющей части киберпреступников не как средство платежа или хранения денег, а как средство разрыва цепочек. Его более широкое использование для внутриевропейских платежей объясняется тем, что невозможно отследить платеж в рамках единой европейской банковской системы.

Следует отметить, что криптовалюты постепенно получают признание на государственном уровне. Можно с уверенностью спрогнозировать, что в ближайшие годы не только большинство стран-членов ЕС, но и ЕС как институт признают криптовалюты как законное платежное средство, определив условия, форму и отчетность по их обороту. Это неизбежно, так же как неизбежен отказ от анонимности криптовалют. ЕВРОПОЛ поддерживает данный процесс, поскольку он позволит избежать отсутствия согласованности в подходе к криптовалютам у различных стран. Эти несогласованности используют кибермошенники и киберпреступники.

Европол настаивает, что при любом регулировании криптовалют должен быть использован принцип идентифицируемости пользователя. Отнесение криптовалют к преступным в корне неверно. Это свидетельствует о технической неграмотности. Вопрос состоит в ином. Необходимо обусловить возможность использования криптовалют обязательной идентификацией пользователей. Общим направлением развития европейской валютной системы должен

стать поступательный и постепенный переход к полностью электронному обороту различных, включая криптовалюты платежных средств с вытеснением нерегулируемых потоков наличностей и анонимных интернет-платежей.

Следует отметить, что на основе криптовалют формируется принципиально новая децентрализованная экономика. Она обещает снижение издержек и пользуется все возрастающей популярностью. Поэтому задача стоит не в запрете чего-либо, а в максимальном использовании заложенных на программном уровне возможностей для максимально полного учета любых платежных операций и недопущения незаконных операций.

Рекомендации

Расследователи и правоохранительные органы должны не избегать, а напротив максимально глубоко вникать в новые тенденции развития платежных средств, в первую очередь, криптовалют, блокчейна, как нового протокола, и новых форматов цифровых кошельков.

Правоохранительные органы должны сотрудничать и обмениваться знаниями с той частью криптосообщества, которая хочет вести дела в рамках закона и использовать на благо общества возникающие новые возможности.

Правоохранительные органы должны пристально следить за развитие альтернативных платежных средств и новых механизмов оплаты, анализировать их потенциал, определять возможности использования новых платежных средств киберпреступниками и инициативно выходить в законодательные органы для блокировки подобных возможностей.

Ключевое значение имеет сотрудничество правоохранительных органов с финансовым сектором, причем не только с банками, но и с компаниями платежных сервисов, операторами и разработчиками криптовалют, компаниями, занимающимися развитием электронных кошельков и т. п.

На основании анализа необходимо стремиться к внесению согласованных изменений в национальные законодательства с тем, чтобы в итоге обеспечить либо единые на уровне ЕС, либо единообразные с точки зрения правовых инструментов национальные законодательства по борьбе с отмыванием денег, включая преступное использование виртуальных валют.

КРИМИНАЛЬНЫЕ КОММУНИКАЦИИ

Интернет изменил форму и природу общения. Никогда в истории человечества не было таких возможностей для коммуникаций. В том числе для коммуникаций между преступником и жертвой, и преступником и преступником.

Способ коммуникации преступника и жертвы зависит от характера, масштаба и объема предполагаемого нападения. При массовых нецелевых атаках основным способом контакта с потенциальными жертвами остается электронная почта. Она является лучшим способом доставки спама. Кроме того, электронная почта используется при достаточно примитивных, а потому массовых случаях применения социального инжиниринга. При проведении сложных целенаправленных атак наряду с все той же почтой максимально широко применяются различного рода шифрованные мессенджеры и почтовые сообщения, либо сервисы быстро удаляемых сообщений. Замечено также, что в подавляющем большинстве случаев, связанном с педофилией и жестоким обращением с детьми широко используется Skype.

Коммуникации между преступниками

Наиболее широко для преступной коммуникации используются либо получившие широкое распространение в постсноуденовскую эпоху платные сервисы шифрованной почты через анонимные удаляемые ящики, либо шифрованные сервисы, типа мессенджеров. В последнее время все более широкое распространение получает общение на закрытых форумах darknet.

Более широкое использование шифрования

Более трех четвертей киберпреступлений в ЕС в 2015 г. было осуществлено с использованием на том или ином этапе преступной деятельности средств шифрования. Наиболее широко используются такие программы, как TrueCrupt и BitLocker. Среди высокоуровневой киберпреступности обязательным стандартом стало использование сложных, иногда специально созданных для собственных нужд систем шифрования. Они используются не только для переписки, но и для защиты всех видов преступных данных, начиная от членов банды и черной бухгалтерии, заканчивая хранилища скомпрометированных кредитных карт и т. п.

Анонимизация

Любые, даже низкоуровневые преступники, используют формы IP обезличивания. Наиболее активно применяются системы простых прокси-серверов и vpn. В 2015 г. в Европе имел место некоторый рост пользователей сети Tor, хотя темпы наращивания были в Европе ниже, чем на всех других континентах. Прекратилось развитие Европейской анонимной сети 12P. В значительной степени это связано с тем, что в докладе ЕВРОПОЛА за 2013 г. правоохранительным органам было рекомендовано ставить на мониторинг всех пользователей, действующих через клиент этой сети. Таким образом, наличие клиента данной пиринговой сети стало восприниматься правоохранительными органами, как возможности принадлежности пользователей к киберпреступникам. Соответственно это отпугнуло значительную часть пользователей от этой сети.

Будущие угрозы и развитие

Несомненно, действия Э. Сноудена способствовали активизации работы по развитию шифрования и анонимизации пользователей, а также тяге пользователей к использованию данных средств. Более того, некоторые крупные IT производители стали устанавливать по умолчанию в своих изделиях различные продукты шифрования. Все это создало значительные трудности для правоохранительных органов.

Необходимо восстановить баланс между интересами защиты частной жизни и данных и возможностью для правоохранительных органов получить доступ к сведениям, жизненно необходимым для расследования преступлений и пресечения террористической деятельности. Восстановление баланса не является легким делом, но надо стремиться к тому, чтобы выработать взаимоприемлемое компромиссное решение.

Рекомендации

Необходимо поставить вопрос о созидании общеевропейской базы vpn и прокси-серверов. В тех случаях, когда будет установлено, что преступники пользуются услугами того или

иного конкретного провайдера сервиса следует на законодательном уровне обязать его раскрывать соответствующую информацию.

Законодатели и политики вместе с промышленными и научными кругами и при самом широком привлечении общественности должны установить такой режим шифрования данных, который с одной стороны позволил бы пользователям защитить свою частную жизнь ми собственность, а правоохранительным органам эффективно заниматься конституционной деятельностью.

DARKNET

Использование анонимизации, прокси серверов и сети Top становится повседневным явлением в киберпреступности. Более половины стран-членов ЕС установили, что киберпреступники из этих стран занимаются противоправной деятельностью в сети dark net, связанной с реализацией незаконных фармпрепаратов и продажи скомпрометированных платежных карт. Более чем в трети стран установлено использование dark net в преступной деятельности, связанных с кражей интеллектуальной собственности, продажей незаконно полученной финансовой информацией и оборотом оружия. Почти треть правоохранительных органов ЕС перешла на режим целевого мониторинга сети Tor.

Распределение по доходам и эффективности преступников в dark net заметно отличается от традиционной преступности. Высокотехнологичная преступность намного порядков более монополизирована, чем традиционная. В 2015 г. установлено, что 1 % наиболее преуспевающих киберпреступников ответственен более чем за половину сделок, осуществляемых в сети Top.

В 2014 г. 21 страна приняла участие в совместной организации Onymous. В ходе операции удалось закрыть 619 доменов Tor, изъять большие объемы наличных денег, наркотиков, золота и серебра. Объемы изъятий составляет примерно треть общего нелегального рынка сети тор на 2014 г.

Несмотря на успешные операции, вместо закрытых торговых площадок появились новые, и менее чем за два месяца оборот сети был восстановлен.

В марте 2015 г. удалось закрыть торговую площадку Evolution. Однако полного успеха добиться не удалось, поскольку администраторы пропали вместе с 11 млн. евро, которые принадлежали поставщикам и потребителям нелегального товара.

Будущие угрозы и развитие

Налицо непрерывный рост как количества членов сети Tor, так и объемов нелегальных торговых площадок. Несмотря на прилагаемые правоохранительными органами различных стран усилия, торговые масштабы сети тор будут увеличиваться из года в год. Несомненно, преступники используют в своих целях растущую тягу бизнеса и общества к антимонопольным, децентрализованным торговым площадка типа OpenBazaar. Эта и подобные ей площадки функционируют на основе принципа равный с равным и прямого контакта между клиентами и производителями.

При этом, подобные торговые площадки берут значительно меньшую долю дохода за выполнение сервисных функций. Если при продаже через централизованные интернет-магазины торговцы удерживают от 10 до 30 % цены товары, то данные площадки – максимум 3–5%. Одновременно при децентрализованном виде торговли высокотехнологичным преступникам легче совершать противоправные действии, чем при централизованных программах, поскольку последние обладают мощными службами информационной безопасности, контроля и т. п.

Рекомендации

Правоохранительным органам необходимо осуществить глубокую разведку децентрализованных сетей, скоординировав свои усилия с научными кругами. Государства-члены ЕС должны обеспечить доступ специальным подразделениям Европола к национальным сетям с тем, чтобы Европол мог создать всеобъемлющую и единую базу данных скрытых сервисов и торговых площадок в Европе. Наряду с традиционной киберпреступностью создание такой базы крайне важно для противодействия таким масштабным видам преступности, как незаконный оборот лекарственных средств и огнестрельного оружия.

Наряду с сетью Tor необходимо не упускать из виду другие пиринговые сети, используемые, в том числе, для нелегальных онлайн торговых площадок. Правоохранительным органам в сотрудничестве с частным сектором и научными кругами необходимо разработать прогнозную модель децентрализованных рынков и других направлений использования блокчейн технологии, чтобы своевременно оценить риски и принять необходимые законодательстве. Организационные и технические меры для обеспечения развития децентрализованных рынков в законных рамках.

БОЛЬШИЕ ДАННЫЕ, ИНТЕРНЕТ ВЕЩЕЙ И ОБЛАКА

Как было впервые отмечено в IOCTA 2014, стремительное развитие интернета вещей бросает новые вызовы и предъявляет новые требования к правоохранительным органам. Спустя год можно констатировать, что большинство стран-членов ЕС вступило в принципиально новый этап развития информационно-телекоммуникационных технологий и киберсреды. Этот этап не так заметен, как появление интернета. Однако фактически он представляет собой переход от интернета к единой цифровой среде, когда стирается грань между реальностью и виртуальностью.

В ближайшие годы общественное развитие, а соответственно и динамика преступности, будут определяться переходом от интернета и интернета вещей к интернету всего, к Большим Данным и облачным технологиям. Вместе три этих направления технологического развития создадут принципиально новую среду обитания, а соответственно сферы развития преступности. Можно предположить, что с одной стороны появятся принципиально новые виды криминала, с другой – киберпреступность приобретет новые черты, а с третьей – информационные технологии станут неотъемлемым компонентом традиционной, в том числе уличной преступности.

Жизнь в цифровой среде предполагает, что правоохранительные органы в корне перестроят свою работу на основе сочетания новых технологий противодействия преступности, а также методов цифровых расследований, а с другой, переподготовки работников правоохранительных органов с тем, чтобы они могли использовать этот инструментарий.

Валютой сегодняшнего мира становятся данные. Поэтому информационно-коммуникационные технологии действуют таким образом, чтобы помимо решения основной задачи обязательно сохранять данные. За данными охотятся все, включая преступников. Однако для полиции задача состоит не только в том, чтобы предотвратить кражу данных, но и в том, чтобы научиться эффективно работать с Большими Данными.

Мало кто осознает, но огромные массивы данных создают для правоохранительных органов не меньшие, а возможно и большие сложности, чем недостаток данных. Согласно отчетам национальных органов полиции ряда стран-членов ЕС, в 2015 г. при расследовании достаточно большого числа преступлений использовались массивы, составлявшие несколько терабайтов данных. В одном случае для раскрытия преступлений пришлось изучить, проанализировать

и оценить 100 терабайтов данных. Фактически работу правоохранительных органов сегодня можно уподобить поиску иголки в стоге сена.

При всей сложности потенциальные выгоды от Больших данных для полиции гораздо большие, чем возникающие проблемы. Однако выгоды для полиции могут быть реализованы только в том случае, если на национальном и общесоюзном уровнях удастся создать мощные хранилища данных, оснащенные наиболее эффективными аналитическими и расследовательскими инструментами. При этом ключевое значение имеет тот факт, что недостаточно наличия баз данных с наиболее эффективной аналитикой, если ими будут пользоваться только чиновники правоохранительных органов, либо исследователи, работающие на полицию. Главное, чтобы система была доведена до рядового полицейского. Ряд стран ЕС поставили задачу в течение ближайших двух-трех лет оснастить низовых полицейских, работающих непосредственно «на земле» не только полной информационной поддержкой, но и возможностью использовать как услугу самую сложную аналитику и средства раскрытия, включая голосовые и видео опознавательные системы.

В то время как интернет вещей по-прежнему рассматривается в качестве новой сферы преступности, в 2015 г. реальностью стали преступления, связанные с использованием интеллектуальных медицинских устройств, вживленных в человека, а также различного рода устройств, непосредственно связанных с медицинскими, пенсионными и иными учреждениями.

Новым явлением стала тотальная оцифровка личной и социальной жизни, а также широчайшее распространение централизованных хранилищ цифровых идентичностей. Не будет преувеличением сказать, что Европа в 2015 г. вступила в эру интернета всего. Облачные вычисления – это распределенные масштабируемые ресурсы, необходимые для функционирования интернета всего и обработки Больших Данных. Чем дальше, тем большее развитие будут получать облачные вычисления. Уже сегодня распространение облачных вычислений создает принципиально новые технические и юридические проблемы для правоохранительных органов. Ранее, когда облачные вычисления были не столь развиты, бизнес защищал свои данные, в том числе, используя привычные средства физической защиты, размещая сервера в хорошо охраняемых помещениях. В настоящее время не только физические лица, но и малый и средний бизнес хранит свои данные, производит вычисления в облаках. Причем, как правило, в нескольких, к тому же относящихся к различным юрисдикциям.

Для правоохранительных органов главными проблемами в области интеллектуальных устройств, Больших Данных и облаков являются:

• Доступ к данным, в том числе надежная идентификация пользователей, имеющих законный доступ к тем или иным данным. Сюда же относится такая техническая проблема, как шифрование данных. Как правило, пользователи стремятся работать с хранилищами данных, имеющих высокий уровень шифрования. Соответственно в условиях распределенного хранения данных, когда шифруются файлы в различных юрисдикциях, правоохранителям бывает крайне сложно даже при установлении субъекта преступлений добиться от других государства, где расположены сервера хранения данных, предоставления доступа к шифрам. Распределенное хранение играет сегодня в большей мере в пользу преступников, а не правоохранительных органов.

• Цифровые расследования и экспертизы. Всеобщая оцифровка и информационно-коммуникационные технологии потенциально создают невиданные ранее возможности для превентивного мониторинга, профилактики преступлений и отслеживания намерений к совершению преступления. Однако проблема состоит в том, что программно-аппаратные возможности правоохранительные органы стран-членов ЕС не могут задействовать из-за законодательных ограничений. Не будет преувеличением сказать, что в ЕС сохраняется приоритет частной приватности над общественной безопасностью. В условиях стремительного наращивания разру-

шительного потенциала одиночек и малых групп преступников, сохранение такого приоритета в дальнейшем может поставить под угрозу общественный порядок и безопасность не в рамках районов и регионов, а стран и Союза в целом.

• Образование и повышение квалификации. Новые программно-аппаратные средства мониторинга, профилактики и расследования преступлений требуют не только прихода в правоохранительные органы новых сотрудников с университетским образованием, но и повышение компьютерной квалификации действующих работников.

• Вопросы приватности и защиты данных напрямую связаны с надежностью корпоративных систем информационной безопасности. В настоящее время в Европе уровень информационной безопасности существенно различается по странам-членам ЕС, а также в зависимости от отраслевой структуры и размеров бизнеса. Не достаточен уровень компьютерной грамотности населения, особенно в сфере информационной безопасности. Все это делает Европу притягательным местом действия для киберпреступных группировок из Северной Америки, России, Китая и Южной Азии.

• Проблемы киберпреступности в период формирования цифровой реальности невозможно решить без перехода на принципиально более высокий, чем в настоящее время, уровень трансграничной кооперации и международного сотрудничества правоохранительных органов.

В рамках подготовки к Докладу ЕВРОПОЛ разослал вопросник для правоохранительных органов стран-членов ЕС относительно мероприятий, которые они планируют по приведению в соответствие своей деятельности цифровой реальности.

Все страны сообщили, что разработали и начали осуществлять меры по совершенствованию национальных информационно-аналитических полицейских систем. За исключением двух стран, остальные начали переоснащение своих судебно-медицинских лабораторий, а также центров экспертизы новыми программно-аппаратными комплексами, связанными с цифровой преступностью, а также использованием информационно-коммуникационных технологий для раскрытия преступлений. Половина стран ЕС преступила к реализации программ обучения и повышения квалификации в сфере ИКТ. И лишь треть стран выделила в качестве приоритета резкое повышение уровня трансграничного сотрудничества и международной кооперации в борьбе с киберпреступностью.

Последнее обстоятельство не может не вызывать озабоченности, поскольку в условиях глобального цифрового мира самая качественная работа полиции на национальном уровне не сможет решить новых проблем.

Будущие угрозы и развитие

С каждым годом границы между реальной жизнью и киберпространством будут все более размытыми. Не будет преувеличением сказать, что уже сегодня наиболее активная часть общества, молодежь, на которую в том числе приходится и наибольшая доля преступности, живет в единой цифровой реальности. Представляется, что в самое ближайшее время придется сдать в архив разделение преступности на киберпреступность и традиционную. Все преступники будут использовать новые высокие технологии, и действовать в единой цифровой среде.

Широкое распространение Больших Данных, интернета всего и облачных технологий формирует принципиально такой новый вид преступности, как управление поведением жертв. С этим видом преступности полиция никогда не имела дела, для его определения нет правовой базы. В этой связи нет сомнения, что именно в эту серую зону устремятся преступники в самые ближайшие годы.

Можно предположить, что наиболее быстрорастущим видом высокотехнологичной киберпреступности будет кража больших массивов данных как ключевого товара цифрового мира. Есть основания полагать, что уже в настоящее время сложились интернациональные

оргпреступнные кибергруппировки, которые рассматривают Европу с ее более низким, чем в других местах уровнем информационной защиты, как главное поле своей активности по краже данных.

Все возрастающее количество данных будет делать все более востребованным программы аналитики и прогностики, в том числе использующие машинное обучение и искусственный интеллект. Есть основания полагать, что в самое ближайшее время развернется настоящая гонка вооружений между правоохранительными органами и транснациональными преступными группировками в области машинного обучения, нейронных сетей и искусственного интеллекта.

Все более широкое распространение интернета вещей и формирование интернета всего открывают невиданные возможности для киберпреступности. Учитывая все возрастающую зависимость, как отдельных людей, так и сообществ любого масштаба от программно-аппаратных средств, не сложно предположить, что эта зависимость будет эксплуатироваться преступниками по самым различным направлениям, начиная от шантажа, вплоть до убийств.

Уже в 2015 г. правоохранительными органами стран-членов ЕС зарегистрировано несколько сотен случаев взлома умных домов, использование как орудие убийств автомобилей, насыщенных интернет-компонентами, и даже взлом и захват управления над вооруженным ракетами военным дроном. Также в 2014–2015 гг. были зафиксированы взломы не только медицинских баз данных, но и систем жизнеобеспечения госпиталей и скорой помощи.

Несомненно, киберпреступники будут максимально использовать распределенные вычисления и облачные хранения данных, чтобы комбинируя различные методы оставаться необнаруженными правоохранительными службами.

Большие Данные и недостаточная во многих случаях их защита, несомненно, стимулирует преступников к разработке принципиально новых видов социальной инженерии, использующих глобальную осведомленность не только об отдельных людях, но и об их сообществах. Европол рассматривает социальную инженерию в сочетании с разработкой управляемых поведенческих моделей как ключевой вызов со стороны преступного сообщества.

Правоохранительным органам необходимо быть готовыми к различного рода веерным отказам и катастрофам, связанным с перенасыщенностью программно-аппаратными средствами. Как показывает опыт, в крупных городах в моменты стихийных бедствий или технических катастроф часто складывается атмосфера мародерства, массовые всплески насилия, краж и других преступлений. Многие европейские исследователи и специалисты в области рисков полагают, что с каждым годом возрастают опасности крупных технических катастроф в европейских мегаполисах, связанные с ошибками в программно-аппаратных средствах. Которые могут вызвать отключение критических инфраструктур и веерные сбои.

Рекомендации

Прежде всего, необходимо, чтобы работники правоохранительных органов осознали, что мы вступили в новую цифровую эпоху. Соответственно они должны быть готовы перейти с периодического на непрерывное обучение и повышение квалификации, чтобы быть способными отразить новые угрозы и воспользоваться новыми возможностями. Необходимо максимально активизировать совместные инициативы бизнеса и правоохранительных органов по оснащению их самой современной техникой и программными средствами, и осуществлению сквозного обучения работников правоохранительных органов.

Целесообразно на законодательном и организационном уровнях проработать концепцию сбора необходимых данных. Суть концепции состоит в том, чтобы запретить частному сектору собирать вообще любые данные как фоновый результат предоставления пользователям основной услуги. Целесообразно проработать вопрос о предоставлении возможности частному сек-

тору собирать и обрабатывать персональные данные лишь с согласия их владельцев. Во всех случаях необходимо обобщить мировой опыт сбора, хранения и обработки данных при их очистке от идентификаторов, указывающих на конкретных людей.

Необходимо максимально активизировать сотрудничество национальных правоохранительных органов как на двух- так и на многосторонней основе с возможным выделением страны-куратора по тому или иному направлению цифровой реальности. Правоохранительные органы страны-куратора вместе с Европолом должны аккумулировать и отрабатывать передовой опыт с целью последующей передачи всем правоохранительным органам стран-членов ЕС.

ГЛОБАЛЬНАЯ ПРЕСТУПНОСТЬ

Ниже приводится краткое изложение основных тенденций и киберкриминальных угроз по всему миру на основе данных правоохранительных органов за 2014–2015 гг.

Африка. Наметилась тенденция увеличения объемов киберпреступлений как внутри Африки, так и африканских киберпреступников в Европе. Наибольшее развитие киберпреступность получила в Северной Африке и на самом ее юге – в Южно-Африканской Республике. В отличие от общемировых тенденций, африканские киберпреступники более активно используют киберпространство для онлайн трансляций, рассчитанных на педофилию. Основные потребители находятся в Европе и Северной Америке. Другой отличительно чертой африканских киберпреступников является больший упор, чем где-либо на финансовую киберпреступность. Если в Европе и Северной Америке практически исчезла киберпреступность, связанная с взломом платежных автоматов, то в Африке это является основным видом киберпреступности. также Африка вместе с Южной Азией являются основными регионами продажи краденых кредитных карт и обналичивания незаконных электронных платежных средств. Последнее связано с нарушением шифрованных линий небанковских платежных систем. С учетом того, что постоянно увеличивается число граждан африканских стран, работающих в Европе, и их платежи домой составляют миллиарды евро в год, то африканские киберпреступники крадут до 5 % переводов по небанковским платежным системам ежегодно.

Лидером киберпреступности в Африке, превосходящим североафриканские страны и Южную Африку, является Нигерия. По данным правоохранительных органов ЕС она входит в число 10 топ-стран с точки зрения экспорта киберпреступности. Поскольку в самой Нигерии не слишком высок уровень интернетизации, то основным направлением киберпреступной деятельности для нигерийских преступников являются страны ЕС и другие европейские страны, не входящие в ЕС.

Америка. Северная Америка является не только неоспоримым лидером в области информационно-коммуникационных технологий, но и первенствует по масштабам и продвинутости киберпреступности. На Соединенные Штаты приходится не только наибольшая доля киберпреступников в мире, но и их жертв. Также США первенствуют в части размещения вредоносного контента в сети и киберпреступных программ.

На Соединенные Штаты приходится от 16 до 20 % всех вредоносных программ, произведенных в мире. В США совершается примерно 40 % киберпреступлений, связанных с финансами и платежными системами, а также кредитными картами.

20 государств-членов ЕС провели исследования, согласно которым выяснилось, что подавляющая часть сложных киберпреступлений, совершенных в Европе, были осуществлены либо подозреваемыми, расположенными в США, либо инфраструктурами, развернутыми в Америке.

Южная Америка. Южноамериканские киберпреступники проявляют незначительную активность в странах-членах ЕС. При этом Колумбия и Аргентина в 2015 г. входили в десятку наиболее спамящих стран. Такие страны, как Эквадор, Гватемала, Перу и Бразилия обладают

низким уровнем цифровой гигиены. Соответственно сайты и ресурсы, размещенные в этих странах, имеют более высокий, чем в среднем уровень содержания вредоносного кода. В 2015 г. Бразилия вошла в пятерку топ-стран по производству вредоносного софта. Наибольшие темпы роста в обеих частях Америки в 2015 г. продемонстрировала именно Бразилия. В самой Бразилии наиболее быстрыми темпами растет финансовая киберпреступность, связанная с взломом терминалов, кражей и обналичиванием кредитных карт, вредоносным вмешательством в платежные системы.

Азия. Также как и Соединенные Штаты, Китай вкладывает значительные средства в интернет-безопасность. Кроме того, особенности китайского управления интернетом поощряя шпионскую деятельность, пытаются препятствовать внутренней киберпреступности. При этом, почти половина государств-членов ЕС сообщила, что они зарегистрировали многочисленные киберпреступления, базирующиеся на использовании китайской программно-аппаратной инфраструктуры. По имеющимся оценкам с Китаем связано примерно 30 % глобальных сетевых атак и крупных киберпреступлений. В первую десятку стран по производству вредоносного софта входят такие страны, как Индия, Китай и Южная Корея. Согласно отчетности правоохранительных органов растет уровень киберпреступности в Японии, Тайване, Малайзии и Индонезии.

Отдельно надо отметить асимметрию киберпреступности в Японии. С одной стороны Япония занимает второе место по количеству случаев кибервымогательства. Также она занимает пятое место по уровню финансовых киберпреступлений. Однако такое положение связано не столько с высоким уровнем киберпреступности в Японии, сколько с тем, что согласно различным обследованиям, Япония является одной из трех лучших стран по уровню расследования и предупреждения киберпреступности.

Несколько азиатских стран специализируются на спаме, как виде киберпреступности. Несомненное первенство в этом плане держит Вьетнам, немного уступают ему Индия и Китай.

Филиппины, Индонезия, Таиланд, Вьетнам и Малайзия составляют крупнейший в мире регион по обналичиванию и использованию ворованных кредитных карт.

Европа. Из стран ЕС происходит 20 % мирового объема кибератак и киберпреступлений. Наибольшая доля киберпреступлений, осуществляемых в Европе, приходится из Нидерланды, Великобританию, Россию, Францию и Германию. Самый низкий уровень киберпреступности в мире имеют Дания, Швеция, Норвегия и Финляндия. Скандинавские страны имеют самый низкий уровень как преступлений внутри стран, так и преступлений из стран вовне.

С точки зрения правоохранительной деятельности ЕС, примерно половина государств-членов ЕС определили, что киберпреступники, осуществившие незаконные акты, действовали из юрисдикций Нидерландов, России, Великобритании и Германии. Кроме того, треть стран сообщила о преступниках, действующих из таких юрисдикций, как Австрия, Бельгия, Болгария, Чехия, Франция, Венгрия, Италия, Латвия, Польша, Румыния, Испания и Украина.

Океания. Австралия, несмотря на достигнутые успехи в борьбе с киберкриминалом, представлена по некоторым направлениям киберпреступности, как одна из десяти ведущих стран мира. В частности это относится к преступлениям с использование бот-сетей и в качестве источника массированных сетевых атак.

Любопытно, что остров Палау в Микронезии занимает второе место в мире по использованию доменов, имеющих юрисдикцию Палау для организации фишинг-атак. Практически в 100 % случае эти фишинг-атаки происходят из Китая.

Глобальные выводы и наблюдения

Киберпреступность становится все более агрессивной, изощренной и технически вооруженной. Эволюция киберпреступности происходит от одиночных, скрытых кибератак высококвалифицированных хакеров-одиночек к конфронтационным немаскируемым действиям киберкриминальных транснациональных группировок. В последние годы произошел переход от одиночного и стихийного киберкриминала к мощным многонациональным и трансконтинентальным сетям и организациям. Многие из них имеют хорошо законспирированное скрытое ядро, располагающееся за пределами ЕС, мощные сети в странах атак и наемных хакеров-одиночек и нестационарных групп, использованных для разовых операций. В настоящее время происходит переход от традиционных киберпреступлений, связанных с кражей кредитных карт, а также вымогательств, сопряженных с блокировкой компьютеров и т. п. к таким сложным видам киберкриминала, как атаки на ключевые финансовые институты, кражи данных, использование интернета всего для убийств и т. п. Отдельно надо сказать о развивающемся во всем мире использовании интернета как среды педофильских преступлений и демонстрации жестокого обращения с детьми.

Важнейшей чертой 2015 г. стало объединение использования вредоносного софта с изощренными видами социального инжиниринга.

Правоохранительные органы в 2015 г. в странах-членах ЕС добились заметных успехов в борьбе с киберпреступностью. Справедливо утверждать, что эти успехи были бы невозможны без теснейшего взаимодействия правоохранительных органов стран ЕС между собой на двухсторонней, многосторонней основе и с участием Европола. Общеевропейское сотрудничество в рамках ЕС является главным фактором, благодаря которому уровень киберпреступности в странах ЕС в среднем ниже, чем в регионах со сравнимым уровнем развития ИКТ.

Важнейшим фактором борьбы с киберпреступностью в ЕС является внедрение единых стандартов и принципов оперативной работы в рамках цикла EMPACT. Вновь созданная объединенная целевая группа действий против киберпреступников (J-CAT) приняла участие в ряде крупнейших национальных и межнациональных операциях по борьбе с киберпреступностью и внесла значительный вклад в их успешное осуществление.

J-CAT является постоянно действующей оперативной группой киберофицеров из нескольких государств-членов ЕС и государств-партнеров, не являющихся членами ЕС. Она расположена в штаб-квартире Европола и действует в контакте с его персоналом. Будучи оснащенной наиболее продвинутыми программно-аппаратными средствами, J-CAT участвует в расследовании наиболее важных и сложных киберпреступлений на национальном и наднациональном уровнях. Ее деятельность служит впечатляющим примером эффективного и действенного глобального сотрудничества по борьбе с киберпреступностью.

Эффект положительных результатов свидетельствует о том, что в Евросоюзе взят правильный курс на теснейшее взаимодействие правоохранительных органов, частного сектора, научных кругов и гражданского общества. В настоящем докладе упоминается, что благодаря этому сотрудничеству в рамках общеевропейского законодательства и национального законодательства удалось внести в 2015 г. целый ряд изменений, позволивших более эффективно бороться с киберпреступностью в финансовом секторе и в области электронной коммерции.

Для правоохранительных органов стран-членов ЕС очевидна необходимость и дальше крепить внутрисоюзное сотрудничество, одновременно улучшая взаимодействие с правоохранителями стран-партнеров, не входящих в ЕС.

Несмотря на впечатляющие достигнутые успехи, остались и некоторые трудности и недоработки, нуждающиеся в исправлении. К ним относятся:

• Необходимость исправления ситуации, сложившейся в настоящее время в сфере судебного сотрудничества со странами вне ЕС. Целесообразно наладить тесное сотрудничество по правоохранительной линии и линии правоприменения с Восточноевропейскими странами, включая Россию, и странами Юго-Восточной Азии;

• Коренное улучшение обмена информацией с частным сектором. Необходимо создание единых баз данных, которыми могли бы пользоваться правоохранители стран ЕС и представители компаний, эксплуатирующих объекты критической инфраструктуры, как в масштабах континента, так и отдельных стран;

• Совершенствование законодательства, как на уровне ЕС, так и отдельных стран в отношении наказания за различные методы применения с использованием ИКТ, шпионской деятельности в киберпространстве, кражи данных, использования устройств, приспособлений и т. п., соединенных с интернетом для криминальных целей, а также регулирование виртуальных валют.

В целях решительной борьбы с киберпреступностью необходимо не только совершенствование законодательства, но и активное использование правоохранительными органами систем превентивного мониторинга активности лиц, имеющих потенциально опасные квалификации. Известно, что среди молодежи стран ЕС нет недостатка в квалифицированных кодерах (программистах).

В этой связи победить преступность только методами наказаний не представляется возможным, особенно в ситуации, когда раскрывается не более 10 % от общего объема компьютерных преступлений. Если же лица, получающие образование в области высоких технологий, которое в Европе в значительной степени или полностью бесплатно, будут знать, что вместе с возможностью высокого заработка они приобретают дополнительную ответственность перед обществом, реализуемую через мониторинг их активности. Это позволит резко снизить приток в оргпреступные группировки талантливой молодежи.

Не будет преувеличением сказать, что сегодня сложилось противоречие между техническими и программными возможностями полиции и уровнем законодательства. Законодательство всегда в любой стране фиксирует обязательные для граждан нормы поведения и опирается не на будущее, а на прошлое. Пока динамика научно-технического прогресса была относительно медленной, с этой законодательной традицией можно было соглашаться.

Сегодня ситуация коренным образом изменилась. В подавляющем большинстве стран-членов ЕС нет специальных статей уголовного законодательства, нацеленных на кибер- и в целом высокотехнологичную преступность. Деятельность в этой сфере лежит в основном в серой зоне. С одной стороны она не признана законом. С другой – закон не преследует ее.

В настоящее время в странах ЕС отсутствует уголовное законодательство в отношении спама, использования dark net, как такового, вне закона находятся криптовалютные биржи, ничем и ничем не регулируются внебанковские платежные системы, особенно использующие биткойн. Бесспорно, не вся активность в серой зоне является преступной. Но наличие серых зон позволяет преступникам использовать отсутствие законодательства для преступлений. Наиболее ярким примером является отсутствие во всех странах ЕС регулирования одноранговых сетей, включая Tor. Невозможно запретить технологию, но можно и нужно прописать в общеевропейском и страновых законодательствах области и конкретные сферы, где та или иная технология не может быть использована ни в каком случае. Наказывать можно и нужно не за использование технологии, а за деятельность с определенной целью, которая противоречит интересам общества и потому является преступной.

Жесткое законодательное регулирование антиобщественного использования высоких технологий необходимо еще и потому расследование преступлений в сфере киберпреступности чрезвычайно дорогостоящи и сложны. Поэтому в сфере высоких технологий законодательство должно быть ориентировано на превентивную борьбу с высокотехнологичными преступ-

никами. Само по себе использование той или иной технологии вне общественно допустимых сфер должно стать достаточным основанием для привлечения гражданина к административной, а во многих случаях и уголовной ответственности.

Инвестиции в осуществление инициатив по профилактике имеют ключевое значение и смогут переломить ситуацию с распространением киберпреступности в странах-членах ЕС. Эти меры должны обязательно подкрепляться образовательно-информационной работой в семье и школе по повышению уровня информационной гигиены.

Чтобы выработать наилучшую тактику борьбы с киберпреступностью, необходимо внимательно проанализировать ее структуру. Объем киберпреступной деятельности прямо зависит от потенциальной прибыльности и обратно пропорционален объему раскрываемых преступлений.

Структура киберпреступности такова.

В ее основе – одиночные или малоорганизованные киберпреступники, использующие стандартные, зачастую дешевые или бесплатные программные средства.

В средней части находятся киберпреступники – выходцы «с улицы», которые проявили себя наиболее дерзкими, способными к быстрому обучению членами криминального сообщества. Как правило, именно их используют сначала на разовых операциях киберпреступные группировки. Такая сложная структура преступности позволяет ядрам киберпреступных группировок в большинстве случаев оказываться нераскрытыми. Поскольку попадаются даже при расследовании сложных киберпреступлений, представители среднего уровня, не знающие очно своих хозяев.

Вершина киберпреступности – это высококвалифицированные киберпреступники. Как правило, это небольшие группы, в которые входят с одной стороны представители традиционной преступности, выступающие как инвесторы, а также люди, предоставляющие услуги, связанные с адвокатурой, проникновением в государственные системы и т. п. Другую часть этой группы составляют, как правило, выпускники лучших университетов со всего мира, а также бывшие и действующие работники лучших компьютерных компаний. Верхушка киберпреступной структуры отлично ориентируется в инновациях и ставит их себе на службу. Более того, в последнее время у Европола появились доказательства, что киберпреступные группировки через специальные отмывочные фирмы регистрируют законные компании и венчурные фонды, инвестирующие в инновации. Не будет преувеличением сказать, что на вершине преступной пирамиды находятся люди, идущие в самом авангарде высоких технологий и использующие их против общества.

В структуре жертв киберпреступлений, как и в случае киберпреступности, большую часть – ее нижний уровень – составляют физические лица, малый и отчасти средний бизнес. В значительной степени они становятся жертвами киберпреступлений в силу крайне низкого уровня технической компетентности и осведомленности в области информационной безопасности. Несомненно, они располагают гораздо меньшими активами, чем жертвы более высокого уровня. Однако, количество в данном случае позволяет компенсировать незначительные масштабы активов у каждой отдельной жертвы.

Специфика киберпреступности состоит, в том числе, в том, что в отличие от традиционной преступности в цифровом пространстве зачастую легче ограбить 100 тыс. человек, чем совершить одно кибернападение на серьезную структуру. Именно легкость масштабирования киберпреступлений является едва ли не самой привлекательной чертой этого типа преступности для криминала.

Потенциальная прибыль при каждой атаке характеризуется тем, что существует прямая зависимость между уровнем квалификации и аппаратно-программного оснащения киберпреступников и прибылью от единичной атаки.

Можно выделить три категории киберпреступности и их жертв. Также как в реальном мире, в киберпространстве одиночные и малоорганизованные киберпреступники выбирают своими жертвами население и малый бизнес. Соответственно наиболее продвинутые и организованные злоумышленники стараются не размениваться по мелочам и не проводить массированных атак на рядовых пользователей, а действовать против организаций с наиболее ценными активами.

Впрочем можно предположить, что в ближайшем будущем ситуация может измениться. В том случае, если крупный бизнес и государственные структуры резко повысят уровень своей информационной безопасности, а организованные киберпреступники найдут способы одновременных атак, охватывающих не тысячи, а сотни тысяч и миллионы человек, то вполне может оказаться, что нынешняя структура изменится. Соответственно, наиболее технически и программно оснащенные группы будут атаковать наименее защищенные жертвы, и получать прибыль за счет эффекта масштаба, а не прибыли от отдельной сделки.

Структура наиболее эффективной стратегии правоохранительных органов такова. Для нижнего уровня наиболее эффективным является профилактическая работа и резкое повышение уровня осведомленности физических лиц и малого бизнеса в сфере киберпреступности. Возможно даже подумать, чтобы общество частично брало на себя затраты, связанные с информационной защитой. На среднем уровне правоохранительным органам не остается ничего иного, как действовать в традиционном ключе и ориентироваться, прежде всего, не на предотвращение, а на раскрытие преступлений.

Наконец, на высшем уровне с учетом чрезвычайной разрушительности кибератак и огромными масштабами ущерба целесообразно в пределах законодательных возможностей, делать акцент не на раскрытии преступления, а на их предупреждении. В этих целях необходимо использовать возможности, если для этого будут созданы законодательные предпосылки, превентивного мониторинга, активности лиц, обладающих высокорискованными квалификациями.

Кибербезопасность против киберпреступности. По данным Европола и национальных правоохранительных органов, едва ли не половина киберпреступлений не произошло, если бы граждане и организации ответственно относились к своей информационной безопасности. Значительная часть компьютерных преступлений совершается из-за того, что население европейских стран и бизнес безответственно относятся к вопросам цифровой гигиены и не принимают никаких мер к защите своих цифровых активов.

В итоге даже лица, обладающие только элементарными программными навыками, но склонные к девиантной деятельности успешно атакуют компьютеры и сети и извлекают из этих атак преступную выгоду. Одна полиция, сколько денег не расходуй, никогда не сможет справиться с киберпреступниками. если граждане и бизнес, вместо того, чтобы сотрудничать с полицией, своим бездействием фактически помогают преступникам.

В этой связи заслуживают внимания предложения о введении для европейских производителей, а также торговых организаций, реализующих продукцию, произведенную за пределами ЕС обязательных требований информационной безопасности продаваемых изделий. Практически немедленно такие законодательные минимальные требования должны быть введены в отношении бытовой техники, автомобилей и устройств для домов. Необходимо обязать бизнес оплачивать повышение уровня информационной безопасности. Иного способа в условиях экономии бюджета справиться с киберпреступностью не существует.

Об этом, например, свидетельствует опыт США. В этой стране был один из наиболее высоких уровней мошенничеств с платежными картами. При этом уже более двух лет существует специальная технология EMV, позволяющая резко повысить надежность платежных карт. Она не применялась, поскольку население, торговые организации и платежные компании не могли договориться, кто будет платить за внедрение технологии. Выход был найден

страховщиками. Страховые компании приняли решение устанавливать существенно различный тариф на страхование платежей в зависимости от уровня их защищенности процессинговыми компаниями, гражданами и торговыми организациями. В результате все три главных участника транзакции посчитали для себя более выгодным взять дополнительные расходы на себя, уменьшив страховые выплаты. Первый анализ данных показывает, что уровень киберпреступности, связанный с платежными картами немедленно снизился.

Данный пример показывает, что зачастую не надо заботу о тех или иных решениях перекладывать исключительно на государство. В подавляющем большинстве случаев вопросы информационной безопасности, а соответственно и сужения поля для киберпреступности, могут решаться не путем вертикальных связей между государствами, субъектами хозяйствования и населением, а исключительно по горизонтали.

Цифровой мир – это вообще мир распределенной обработки данных. Соответственно возникает вопрос о распределении ответственности. Например, кто несет ответственность за использование сети Tor наркобаронами, торговцами оружием, скриммерами и педофилами. Является ли ответственным ICANN? Организация утверждает, что не имеет к сети Tor никакого отношения. Может быть военно-морская разведка США, находившаяся у истоков проекта Tor? Нет, отвечают они. Проект был разработан исключительно в военных целях. Тогда, может быть, например, Шведский королевский благотворительный фонд, спонсирующий развитие сети Tor? Фонд отвечает, что глупо возлагать ответственность на производителя оружия за то, что этим оружием кого-либо убили.

В случае с Tor мы сталкиваемся с общей закономерностью, свойственной высоким технологиям. Практически любую высокую технологию можно использовать как во благо, так во зло. Сегодня притча во языцех – Tor. Статистика действительно свидетельствует, что доля преступных сайтов и ресурсов в этой сети намного выше, чем в интернете. Однако, с другой стороны, только Tor во многих странах гарантирует свободу слова и безопасное взаимодействие людей, борющихся против тоталитарных и авторитарных режимов.

Надо быть готовым к тому, что завтра то, что сегодня говорят про Tor, будут говорить про роботов и роботизированные автомобили. Видимо общество должно привыкнуть к мысли о том, что сама по себе технология не является ни благом, ни злом, а лишь инструментом, при помощи которого могут быть достигнуты разные цели. Однако, как мы полагаем, в перспективе Европейское сообщество должно задуматься о том, что производители, продавцы и возможно даже пользователи особо продвинутых технологий потенциально способных нанести обществу огромный вред, должны согласиться с большей прозрачностью для общества в лице правоохранительных органов, своей повседневной профессиональной жизни.

Это выводит нас на вопрос о праве на защиту частной жизни. Разоблачения последних лет, связанные с массовым электронным наблюдением, сместили баланс осведомленности и приватности в сторону максимальной защиты индивидуума от любой правительственной возможности не только вмешиваться, но и наблюдать за их личной приватной жизнью. Результатом этого вполне понятного и объективного процесса стала чрезвычайно опасная тенденция. В ситуации, когда киберпреступники и организованный криминал объединяют свои усилия не в национальном и даже не в континентальном масштабе, и все активнее пользуются продвинутыми технологиями, правоохранительные органы оказались спеленатыми по рукам и ногам многочисленными законодательными запретами. Цена появления антисноуденов, т. е. киберпреступников, которые нанесут ужасающий вред обществу, может оказаться слишком высокой для того, чтобы потом восстановить баланс.

Европолу кажется, что законодательные европейские органы чрезмерно пошли на поводу у манипулируемой общественности и ограничили возможности правоохранительных органов защищать общество и каждого отдельного гражданина. В этой своей чрезмерности они неправильно истолковали важнейший документ, а именно Декларацию ООН «О правах человека».

В ней записано: «Никто не должен подвергаться произвольному вмешательству в его личную жизнь, семью, дом. Каждый имеет право на тайну переписки, на защиту законом от такого рода посягательств».

Парадокс состоит в том, что без превентивного мониторинга это важнейшее право не может быть соблюдено. Каждый европеец при отсутствии возможности у правоохранительных органов осуществлять тщательный мониторинг, может стать жертвой хакеров, которые не просто ежедневно вторгаются в частную жизнь граждан, но и совершают разнообразные преступления. Ключевым в Декларации ООН является слово «произвольно». Законодатели должны четко определить условия, при которых правоохранительные органы могут быть явным образом уполномочены вторгаться в частную жизнь граждан.

Должен существовать независимый аудит, определяющий соответствие действия правоохранительных органов законом. Однако лишать правоохранительные органы права вести опережающий мониторинг невозможно.

Скорость, с которой общество и преступность технологизируются, в настоящее время превышает темпы адаптации полиции и других правоохранительных органов к цифровым переменам. Ситуация, при которой общество становится все более зависимым от информационно-коммуникационных технологий, имеет много последствий для полиции, как с точки зрения возможностей, так и проблем. С одной стороны видеофикация всего и вся, превращение данных в цифровую валюту мира, привычка фиксировать свое поведение, настроение в социальных сетях и т. п., переход от наличных денег к электронным создает гораздо более благоприятные возможности для опережающего мониторинга и сбора доказательств. С другой стороны, никогда раньше у преступников не было такой разнообразной гаммы орудий преступлений, и никогда раньше по некоторым видам преступность не была столь безнаказанной как сегодня. К сожалению, это две стороны одного и того же процесса.

Дополнительные сложности для правоохранительных органов создает то обстоятельство, что их организационная структура, прописанные процедуры, кадровый состав заточены на традиционные преступления. Не успела полиция адаптироваться к киберпреступлениям, как любые преступления стали осуществляться с использованием тех или иных высоких технологий.

Нельзя также не учитывать тот факт, что сама по себе логика развития информационных технологий носит распределенный характер. Это порождает тягу преступников к высоким технологиям и использования их даже для относительно простых преступлений. Если убийство происходит в результате использования огнестрельного оружия, то велика вероятность, что преступника заметят те или иные свидетели, или он попадет в поле зрения видеокамер и т. п. Если же убийство будет осуществлено путем перехвата управления автомобилем, путем задействования цепочки прокси-серверов, с компьютера, купленного исключительно для этого преступления через анонимную торговую площадку, то шансов раскрыть подобное преступление будет очень мало.

Сами по себе тенденции высокотехнологичной преступности заставляют задуматься о том, что правоохранительным органам, хотят они того или нет, или считает ли это полезным или нет общество, придется все больше переходить от расследования преступлений к выявлению преступного умысла и предупреждения преступления.

Такая жесткая постановка, возможно, вопрос завтрашнего дня. Сегодняшний важнейший приоритет для правоохранительных органов – это создание сплошной – от федеральных органов до местных правоохранительных структур – системы обучения высоким технологиям, как для проведения расследований и сбора доказательной базы, так и для мониторинга и профилактики.

Цена киберпреступности[21]

Киберпреступность в финансовом секторе.

Настоящий доклад не ставит своей целью изложение результатов детальных расчетов ущерба от финансовой киберпреступности Великобритании. В полном объеме эту задачу имеется в виду решить в ходе второго этапа исследований Detica и опубликовать в декабре 2015 г.

Учитывая остроту обсуждения проблемы киберпреступности в банковско-кредитной и финансово-инвестиционной сферах, авторы доклада сочли, тем не менее, возможным подробно описать свой подход к исследованиям финансовой киберпреступности и сделать первые прикидочные оценки.

Прежде всего, финансовый сектор Великобритании, в который входят не только банки и другие лицензированные кредитные организации, но и финансовые, инвестиционные и страховые компании, взаимные, индексные, хедж и пенсионные фонды, а также различного рода трасты и обслуживающая сектор инфраструктура, являются ключевым сектором британской экономики.

Согласно данным Банка Англии, в 2014 г. все виды банковских активов, а также активов других организаций финансового сектора, более чем в пять раз превышали ВВП Великобритании. Согласно прогнозу к 2020 г. превышение составит 6,5–7,5 раз.

По данным правительства, британский финансовый сектор вносит гораздо больший вклад в создание ВВП, чем соответствующие сектора в других странах ОЭСР. В Великобритании финансовый сектор создает в настоящее время 29 % ВВП против 19 % – промышленности. По прогнозам в 2020 г. на долю финансового сектора будет приходиться порядка 35 % ВВП, а промышленности – 23 %. Для сравнения, в Соединенных Штатах доля финансового сектора в ВВП составляет 11 %, в Германии – 9 %, а в Японии – 7 %. *(Справочно, в России приближается к 9 %).*

Британский финансовый сектор аккумулирует в себе последние достижения информационных, организационных и финансовых технологий, является движущей силой британской экономики. Данное положение сохранится на ближайшее десятилетие. Сектор будет вносить ключевой вклад в ВВП и экономический рост, обеспечивать занятость, социальную стабильность и политическую устойчивость страны. Именно от британского финансового сектора в решающей степени зависело, зависит и будет зависеть геополитическое положение Великобритании и конкурентоспособность британского бизнеса.

В этой связи нарастающая по экспоненте киберпреступность применительно к британскому финансовому сектору является первостепенной и жизненной угрозой не только экономике и уровню жизни британцев, но и национальной безопасности.

Киберпреступность в финансовом секторе понимается как противоправная деятельность против различного рода финансовых институтов и их клиентов, где главным орудием преступления выступают ИКТ. Кроме того, заслуживает также внимания включение в сферу финансовой киберпреступности всех видов преступности, связанных с противоправной деятельностью с целью извлечения выгоды путем незаконного присвоения цифровых (электронных) финансовых средств, других платежных инструментов и т. п.

[21] Доклад Центра Detica в партнерстве с офисом информационной безопасности британской полиции и при поддержке офиса кабинета министров Великобритании. 2015 г. (Извлечение)

Данная поправка важна в условиях неизбежной экспансии протоколов, типа блокчейн, предусматривающих новые типы финансовых операций, не носящих институционального характера, а осуществляемых в рамках принципа P2P или «равный к равному».

В начале 2015 г. исследовательская служба Конгресса США получила оценку глобальной киберпреступности в сфере финансов в расчете на 2014 г. в размере 600 млрд. долларов. Хотя детальный расчет по конкретным направлениям финансовой киберпреступности применительно к британскому рынку впереди, обобщение данных различных британских источников, а также мнений сотрудников ведущих финансовых учреждений, специальных служб и т. п. позволяют сделать вывод, что оценка американских коллег, вероятно, реалистична. Если ошибка имеется, то, скорее всего, носит характер процентов, а не порядков.

Предварительные данные по Великобритании свидетельствуют, что ежегодный ущерб от киберпреступности в финансовом секторе за вычетом кражи интеллектуальной собственности и использования инсайдерской информации, составляет порядка 70–80 млрд. фунтов стерлингов. С учетом мощности британского финансового сектора и его места в мировой финансовой системе, две изложенных экспертных оценки в целом соответствуют друг другу и, несомненно, могут являться отправной точкой для проведения детальных расчетов по конкретным направлениям финансовой киберпреступности.

Необходимо специально отметить, что обе полученных оценки сделаны на основе так называемой двухфакторной методологии. Напомним, что двухфакторная оценка ущерба от киберпреступности включает в себя:

Во-первых, оценку прямого ущерба бизнеса, а также правительства и граждан от операций киберпреступников по хищению интеллектуальной собственности, других видов цифровых активов, коммерческой тайны, онлайн мошенничества и т. п.

Во-вторых, включает в себя затраты, которые вынужден нести бизнес, а также правительство и отдельные граждане для предотвращения криминальных кибератак, повышения безопасности всех видов цифровых активов, и соответственно снижению риска оказаться жертвой киберпреступников.

В исследовании ущерба от киберпреступности в финансовой сфере, которое будет опубликовано в декабре 2015 г., будет впервые в мире использована более обоснованная и мобилизующая на практические действия трехфакторная система оценки цены финансовой киберпреступности. Подробно о ней говорилось ранее. В данном контексте отметим лишь, что наряду с упомянутыми выше двумя факторами, в оценку будет включен и третий фактор: прямая и где возможно обоснованно рассчитать – косвенная прибыль, а точнее доход киберпреступности от криминальной деятельности против финансовых институтов всех видов, и их клиентов.

Применительно к финансовой киберпреступности будут изучаться два типа акторов, а именно – бизнес и граждане. Защита бизнеса и граждан от киберпреступников является, прежде всего, долгом полиции. Что касается государства, то финансовая преступность в этой сфере, как показывают данные исторического анализа, в подавляющем большинстве случаев связана с актами финансово-экономической агрессии со стороны других государств, а в будущем, возможно, террористических сетей и групп. В этой связи борьба с нарушением целостности британской финансовой системы и отражении киберугроз государственным финансам и Банку Англии является заботой не полиции, а вооруженных сил страны и разведывательных служб. Оценки в этой области, применительно к финансовой сфере, могут быть сделаны только на основе закрытых и секретных материалов.

В этой связи они не являются предметом изучения Detica, как независимого исследовательского центра.

В рамках данного материала основное внимание сосредоточено на вычленении основных видов финансовой киберпреступности и определении принципиальных подходов к оценке ущерба, базирующихся на доступных исследователям и общественности данных.

В обобщающем докладе «Цена финансовой киберпреступности 2015 г.» будут осуществлены расчеты по следующим основным видам финансовой киберпреступности:

– **Кардерство**. Исторически хищение кредитных карт, а также нарушение электронных коммуникаций и средств защиты, позволяющие злоумышленникам использовать чужие кредитные и дебетовые карты, является одним из старейших видов финансовой киберпреступности. В строгом смысле слова, прямое хищение кредитных карт не относится к киберпреступности, поскольку кредитная карта может быть похищена вместе с кошельком, сумкой и т. п. в рамках традиционной уличной преступности. Соответственно в прошлом было крайне сложно разделить в кардерстве две составляющих – собственно киберпреступность и традиционную уличную преступность, включая грабежи, щипачество и т. п.

С прогрессом ИКТ ситуация стремительно меняется. Еще в 2013 г. из 84 % британцев, пользующихся кредитными картами, лишь 6 % использовали в качестве кредитных карт мобильные приложения к гаджетам. В 2015 г. по оценкам Союза платежных систем Великобритании, таковых уже почти 20 %, причем среди молодежи – более 50. По оценкам подавляющего большинства британских и американских специалистов в области платежных систем, банковского дела и процессинга, в 2020 г. не менее чем у двух третей населения Великобритании кредитные карты заменит гаджет. В этой связи можно с уверенностью сделать вывод о том, что весь кардинг в ближайшие годы перейдет в киберпространство.

Даже украденный телефон без соответствующей блокировки программных решений безопасности, а также сложных программ, позволяющих преодолеть не одноуровневую, а многоуровневую систему идентификации пользователя, будет бесполезен для преступника. Поэтому есть все основания полагать, что в эту сферу придут высокотехнологичные преступные группировки. Они вытеснят или подчинят себе одиночек и неорганизованные группы, которые действуют на этом рынке сегодня.

Экспертная, а не расчетная, оценка электронного кардерства, как вида финансовой киберпреступности, для Великобритании составляют в настоящее время порядка 1–2 млрд. фунтов стерлингов в год.

– **Пеймент-криминал**. Быстро развивающимся направлением киберпреступности является использование криминалом процессинговых и иных платежных систем. Этот вид криминала относится к числу наименее рискованных. За всю историю правоохранительных органов различных государств было зафиксировано всего четыре случая выявления с последующим наказанием преступников. При том, что всего в этих государствах было обнаружено более 50 подобных случаев.

В отличие кардерства, пеймент-преступники не осуществляют прямой кражи средств с кредитного либо дебетового счета юридических и физических лиц. Данный вид преступности базируется на хакинге и высоком уровне программирования. Преступники вскрывают коды коммуникаций процессинговых центров и платежных систем и добавляют каждому выбранному или полученному на основе генератора случайных чисел платежу некоторую, обычно незначительную дополнительную сумму. Согласно исследованиям британских и американских специалистов в области финансовой кибербезопасности, в Соединенных Штатах не более 5, а в Британии – не более 7 % клиентов обратили внимание на добавленную сумму, когда она составляла от общей суммы платежа не более 1 %. Клиенты, как правило, воспринимали данную сумму, как некий дополнительный тариф процессинговой или платежной компании, взимаемый на том или ином основании. Казалось бы, преступники имеют мизерную выгоду при необходимости первоначальных внушительных затрат, связанных с аппаратным оснащением и наймом высококвалифицированных программистов и хакеров. Однако, потенциальная выгода может быть огромной. Например, в Великобритании ежедневно с использованием систем электронных платежей и независимых платежных систем переводятся средства в размере нескольких десятков миллиардов фунтов стерлингов только населением, а также малым и небольшим

бизнесом. Понятно, что даже 1 % скажем от 10 млрд. фунтов стерлингов в день составляет немного ни мало, как 100 млн. фунтов стерлингов или от 3 до 4 млрд. в год.

Первые случаи пеймент-преступности были зарегистрированы еще в нулевые годы в Южной Азии. Там широкое распространение получили независимые платежные системы, не связанные с глобальными карточными компаниями. Первые зафиксированные случаи выявили тесную связь киберфинансовых преступников с исламским террористическим подпольем в Индонезии и Малайзии.

До недавнего времени в Британии случаи пеймент-криминала имели разовый, несистемный характер и осуществлялись одиночками, либо маргинальными хакерами. Причиной такого положения являлось то, что до самого последнего времени более 90 % электронных платежей в Великобритании приходилось на крупнейшие банки Сити и глобальные карточные компании типа «Виза», «МастерКарт», «Диннер Клаб» и т. п. Банки и глобальные компании имеют мощные, хорошо защищенные, выделенные телекоммуникации, стойкую криптографическую защиту сигналов, отлаженную систему внутренней безопасности. Работать в таких условиях преступники не любят. Оборотной стороной такого положения являются достаточно высокие издержки, связанные с внутренними и особенно трансграничными электронными переводами, которые в отдельных случаях достигают до 7 % от пересылаемой суммы.

В этих условиях в финансовом секторе с каждым годом все более широкое распространение получает метод обратного заимствования. Впервые этот метод был разработан в 2013 г. профессором Р. Раджишваном из Бомбейского университета. Суть метода в том что, если раньше относительно отсталые страны заимствовали решения у технологических лидеров, то теперь все чаще наиболее развитые страны берут на вооружения решения. первоначально разработанные для бедных, не всегда технологически развитых стран. Эти решения, как правило, просты, относительно надежны и очень дешевы.

Соответственно на Западе вообще, и в Великобритании в частности, все более популярными становятся независимые платежные системы, завязанные на вездесущие гаджеты и одноранговые сети. Они обеспечивают бесплатный внутристрановой и крайне дешевый международный перевод средств. По прогнозу британского правительства уже в 2016 г. более двух третей британцев и 85 % британских граждан в первом поколении и трудовых мигрантов для перевода денег будут использовать не банки и традиционные банковские компании, а независимые платежные системы. Дешевизна этих систем в немалой степени объясняется тем, что для передачи они используют не специально выделенные линии, а интернет или различного рода одноранговые сети, а также не имеют специальных внутренних служб безопасности.

Не говоря уже о том, что согласно оценкам правоохранителей, немалая часть подобных платежных систем может быть куплена и даже создана высокотехнологичными преступными группировками, финансовым киберпреступникам легко будет заниматься пеймент-криминалом в таких мало защищенных, не имеющих институциональной безопасности и завязанных на насквозь инфицированные гаджеты, сетях.

– Криминальное программирование. В настоящее время цифровые активы британских банков и иных финансовых институтов, включающие стоимость аппаратной части, корпоративно-информационные системы, базы данных, торговые, клиентские, учетные и иные программы, по своей стоимости составляют более 70 % неденежных активов финансового сектора (за исключением недвижимости Сити).

Сохранность и целостность цифровых активов британских банков является залогом их эффективной работы и конкурентоспособности. По мере экспансии ИКТ в банковский сектор и особенно непосредственно в подготовку и совершение сделок на всех типах финансовых рынков, от качества, конфиденциальности и защищенности программного обеспечения зависит не только благосостояние финансовых институтов, но и их конкурентоспособность. Все большее число сложных программных комплексов, используемых банками, стоит более мил-

лиона фунтов стерлингов каждая. Затраты на некоторые из них превышают десятки миллионов. В 2014 г. «Барклайс Бэнк» приобрел аналитико-прогнозно-торговую платформу ценой в 176 млн. фунтов стерлингов.

В условиях, когда программные продукты становятся основным производственным фактором, у сектора мультипликативно возрастают возможные размеры ущерба, который могут нанести разработчики, программисты, системные администраторы, занимающиеся созданием, совершенствованием и обслуживанием сложных программных финансовых комплексов.

Британские банки и иные финансовые институты предпочитают по согласованию с полицией, в ряде случаев – спецслужбами, а также Банком Англии не предавать широкой огласке инциденты, связанные с криминальным программированием внутри банков. Этим банки Сити отличаются от своих американских коллег.

В 2012–2014 гг. на Уолл-Стрит прошло серия арестов программистов, которые либо похищали разработанные ими для банка программы, имея в виду их использовать в собственных целях или передать конкурентам, либо вносили в программный код специальные фрагменты (бэкдоры), делающие программы уязвимыми для хакеров и внешних манипуляторов. Наиболее известным стал случай с российским программистом С. Алейниковым. Его банк-работодатель «Голдман Сакс» сообщил ФБР о нанесенном программистом потенциальном ущербе, измеряемом полутора миллиардами долларов. В ходе состоявшегося судебного процесса программист получил тюремный срок заключения, но при этом, размеры нанесенного ущерба подтверждены не были.

В ходе исследования при беседах с руководством Банка Англии, руководителями соответствующих подразделений полиции и специальных служб, удалось выяснить, что подобные американским случаи происходили и в Великобритании. Более того, в ходе интервью было высказано мнение, что не столько их количество, сколько масштабы нанесенного финансовым учреждениям ущерба от криминального программирования банковских и иных платформ, постоянно и экспоненциально увеличиваются. При этом интервьюируемые отказались сообщить конкретные цифры и наименования учреждений, где случились подобные инциденты.

Как бы там ни было, есть, по крайней мере, два фактора, которые будут способствовать взрывному росту издержек финансовых институтов, а соответственно доходов преступного мира от деятельности криминальных финансовых программистов.

Во-первых, будет продолжаться экспансия ИКТ технологий в финансовый сектор. Есть все основания полагать, что уже на горизонте 2020 г. этот сектор превратится в один из наиболее роботизированных секторов британской экономики.

Во-вторых, это будет происходить в ситуации, когда выпускники британских университетов неохотно идут в традиционное программирование, связывая свою карьеру с такими перспективными направлениями, как биоинформатика, синтетическая биология, глубокое машинное обучение, искусственный интеллект и т. п. В этих условиях компании, специализирующиеся на финансовом софте, а также банки и иные подобные институты, оказываются перед необходимостью во все возрастающих масштабах нанимать программистов и разработчиков из третьих стран, прежде всего, Украины, России, Польши, Южной Европы и, конечно же, Индии.

Надо отметить, что в подавляющем большинстве указанных стран, в силу ряда исторических причин ослаблена деловая этика и не сформировалось уважение к закону с малых лет. Кроме того, многие программисты из стран постсоветского пространства, Восточной Европы и Индии имеют за плечами большой хакерский опыт, а соответственно прямо или косвенно связаны или как минимум имеют знакомства с представителями организованных преступных группировок.

Комбинация отмеченных выше двух обстоятельств заставляет пессимистически смотреть на возможности финансового сектора в ближайшем будущем минимизировать потери и

убытки от криминального программирования. Имеются все предпосылки к тому, что эта цена будет только возрастать. Причем весьма быстрыми темпами.

Невозможно бороться с явлением или процессом, если он не диагностирован и не оценен. Без количественной оценки размеров ущерба от преступности невозможно эффективно бороться с ней. В этой связи Правительство Великобритании совместно с Банком Англии целесообразно внимательно изучить опыт Федеральной Резервной Системы, федеральных органов власти США по созданию обязательной государственной системы отчетности о киберинцидентах в корпоративных информационных системах, и шире – программно-аппаратных комплексах банков и иных финансовых институтов, подпадающих под лицензирование. Только имея статистику, которая будет доступна не только государственным чиновникам, но и исследователям, можно надеяться на минимизацию нарастания размеров ущерба от криминального программирования для финансового сектора.

– Хайп-преступность[22]. Железный закон инвестиций предполагает, что за исключением специальных ситуаций, процент прибыли на инвестиции прямо пропорционален уровню риска. Чем выше риск, а соответственно возможность потерять деньги, тем большую прибыль можно получить на вложенные ресурсы. Однако также известно, что финансовый рынок, как и любые другие рынки, является неравновесным, несимметричным и непрозрачным. Соответственно крупные или особо продвинутые инвесторы пользуются данными свойствами рынка, и извлекают доходы из так называемых «специальных» ситуаций, связанных с несбалансированностью, непрозрачностью и т. п., получая максимум доходов при минимуме риска.

О данной, неотъемлемой особенности финансовых рынков широко пишут не только специализированные источники, но и общедоступные электронные ресурсы. Им посвящены сюжеты на телевидении и иных средствах, рассчитанных на самые широкие слои. Трудно осуждать мелких инвесторов за то, что они хотят не терять деньги на финансовых рынках, а преумножать их подобно финансовой элите и технологически продвинутым инвесторам.

Начиная с конца прошлого века в США, Великобритании и Европе все большее развитие и масштабы получают такие методы коллективного инвестирования, как взаимные, индексные, хеджевые фонды. При этом наиболее высокодоходные, использующие специальные ситуации, хеджевые фонды закрыты для мелких инвесторов, поскольку по законодательству США и Великобритании требуют значительных одноразовых вложений средств от отдельного вкладчика, в разы превышающего среднюю заработную плату в этих странах.

Данными обстоятельствами и настроениями воспользовались криминальные финансисты, создавшие так называемые хедж-фонды для бедных или хайпы. В своем подавляющем большинстве подобного рода структуры являются обычными пирамидами, где доходы старым вкладчикам выплачиваются из средств, вкладываемых в программу новыми ее участниками. В некоторых случаях принципы пирамиды добавляются инвестициями в высоко рискованные активы.

Чтобы привлечь максимальное число участников организаторы хайп-программ определенный период времени – как правило, от трех месяцев до полутора лет – выплачивают средства. Средний срок действия хайпов, в которые вовлечены граждане Великобритании, составил в 2014 г. пять с небольшим месяцев.

Несмотря на очевидно преступный по британскому законодательству характер подавляющего большинства хайпов, случаев преследования британской полицией или службами Министерства финансов организаторов хайпов в ходе исследований выявлено не было. Не преследовались даже британские граждане – организаторы хайпов. Причин две. Как правило, британцы

---

[22] *High-yield investment program (HYIP) – дословный перевод: высокодоходные инвестиционные программы. По сути, являются современным высокотехнологичным названием хорошо известных схем Понци и незабвенного Мавроди. – Прим. переводчика.*

организуют не чисто пирамидальные хайпы, а хайпы, вкладывающие средства в высокорискованные активы и проводящие выплаты дополнительных доходов ранним участникам за счет средств поздних участников не по статье «прибыль», а по иным, зачастую экзотическим статьям. В данной ситуации хайпы становится сложно отличить от стартапов, и соответственно даже в случае обнаружения хайпа и установления его организаторов, судебные перспективы оказываются сомнительными.

Другая, и главная причина, состоит в том, что существует множество стран, где хайпы не запрещены. Соответственно, в условиях свободной циркуляции информации, капиталов в глобальном интернете, организаторы хайпов размещают их, включая и хостинг соответствующего сайта, в странах с благоприятной юридической и налоговой системами, а клиентов мобилизует в Великобритании и других развитых странах.

На дополнительные размышления наводят также результаты исследования, проведенного совместно Лондонской школой экономики и Тринити-колледжем. В ходе исследования, посвященного хайпам, было проанализировано участие в подобных мошеннических программах граждан Великобритании с различным уровнем дохода, а также статусом резидента. Часть данных подтвердили предварительно сформулированную гипотезу. Основную часть участников хайпов составили представители наиболее, если можно так выразиться, состоятельных слоев бедных и малообеспеченных граждан, а также самые низы среднего класса. Однако открытием для исследователей стал тот факт, что более 15 % участников хайпов принадлежат если не к элите, то к самому верхнему уровню среднего класса, а также британским богатым.

Второй вывод исследования показал, что жители Британии в третьем и более поколениях практически не участвуют в хайп-программах. Это удел британцев во втором (17 %), а также в первом поколении (83 %). Иными словами, в хайпы оказываются вовлечены люди, не имеющие семейного опыта британской деловой и финансовой культуры, навыков взаимодействия с финансовыми институтами, а также формирования в британской образовательной системе рационального мышления.

В данном исследовании была сделана оценка, что ежегодно британцы в хайп-программах теряют более 2 млрд. фунтов стерлингов. В ходе исследования мы предполагаем привлечь максимально возможные объективные данные, чтобы подтвердить либо опровергнуть оценку сделанного на основании экспертных суждений и огромного числа интервью с жертвами хакеров.

Исходя из трансграничного оперирования хайп-структур и национального характера ущерба от хайп-программ, в качестве предварительной рекомендации авторы настоящего исследования предлагают Правительству задуматься о возможности принудительной блокировки на уровне интернет-провайдеров доступа к расположенным на зарубежных хостах сайтов хайп-компаний. Безусловно, подобный запрет легко обходится не только искушенными хакерами, но и простыми пользователями. Однако, ориентируясь на конкретный состав хайп-пользователей, можно высказать гипотезу, что большинство из них не подозревает о наличии простых инструментов обхода запретов на посещение тех или иных сайтов, заблокированных провайдерами.

– **финансовый просоциоинжениринг.** Пресса сообщила, что в 2014 г. британские юридические лица не досчитались почти полутора млрд. фунтов стерлингов, которые хранились на счетах британских банков и финансовых институтов. Эти потери в подавляющей части связаны с просоциоинжинирингом. Программный инжиниринг представляет собой сочетание хакерства со злонамеренным внесением в программный код покупных или собственных программ, ответственных за хранение, учет, обработку данных и принятие на их основе финансовых и инвестиционных решений. Социальный инжиниринг традиционно связывается с использованием особенностей человеческой психологии для получения, а точнее выведывания информации, либо манипулирования поведением конкретных людей.

Начиная с нулевых годов, международная банковская система все более быстрыми темпами переходит не только на электронное хранение данных и электронные деньги, но и на электронный документооборот. Электронный документооборот становится общеделовым стандартом, свойственным для финансовых институтов из всех технологически развитых стран.

С переводом отчетности, бухгалтерских, юридических и платежных документов, преступная деятельность, как ни странно, не затрудняется, а облегчается. В традиционных финансах и экономике с бумажным документооборотом и персональным общением всех участников финансовых и бизнес процессов, представлялось трудноисполнимым без сознательного содействия участников подменить платежные документы, данные бухгалтерской отчетности, задним числом внести изменения в подписанные договора и т. п. С переходом всей деловой, юридической, бухгалтерской, финансовой и иной документации и ее оборота в электронную форму, а также с заменой живого общения использованием мессенджеров, коммуникаторов, электронной почты и т. п., возможности киберпреступников кратно возрастают.

Располагая доступом внутрь компании или банка, за счет использования методов социальной инженерии, киберпреступные группировки получают возможность не разрушать, а подменять и изменять различного рода данные. При этом в подавляющем большинстве случаев замена данных оказывается неотслеживаемой и обнаруживается лишь после осуществления тех или иных крупных мошеннических платежей.

Как свидетельствуют сотрудники правоохранительных органов, использование методов социального инжиниринга позволяет вовлечь в криминал сотрудников банков и других финансовых учреждений таким образом, что они даже не подозревают о своей преступной деятельности, искренне полагая, что выполняют те или иные указания собственников или вышестоящих уровней управления.

Криминальный финансовый просоциоинжиниринг является весьма ресурсоемкой, сложноорганизованной и высокотехнологичной сферой. Как правило, преступные операции такого типа достаточно долго планируются и включают в себя самые различные фазы, начиная от стадии проникновения, заканчивая фактическим осуществлением одной крупной, либо постоянных небольших транзакций со счетов юридических лиц. Зачастую между стадией проникновения и временем транзакции проходят даже не недели, а месяцы.

Какая-либо отчетность, а также обязанность финансовых институтов различных типов сообщать о выявленных инцидентах, связанных с данным типом киберфинансовой преступности, в Великобритании отсутствует. Это не позволяет сделать, по крайней мере, сегодня каких-либо обоснованных и документированных количественных оценок. В то же время из частных бесед с работниками Банка Англии и ведущими британскими банкирами и топ-менеджерами крупных хедж-фондов, финансовых компаний и т. д. удалось установить, что данный тип преступности активно развивается и более того, наносит с каждым годом все больший ущерб британской финансовой системе. В ходе встреч большинство представителей финансового мира признались, что они скорее недооценивают, чем переоценивают эту угрозу и весьма вероятно не имеют информации о многих уже произошедших и происходящих на регулярной основе подобных случаев не только в целом в банковской системе, но и конкретно в их собственных банковских учреждениях.

Казалось бы, данной информацией должны обладать аудиторские фирмы. Однако многочисленные факты, касающиеся дела Энрона, аудита разорившихся банков в США и Великобритании и т. п., заставляют подозревать многие, даже ведущие аудиторские компании, как минимум в снижении уровня компетентностей и в неспособности своевременно выявлять преступления и мошенничества.

– FTS-преступность[23]. Самый крупный рынок мира – это рынок Форекс. Ежедневный оборот мирового рынка Форекс составляет более 1 трлн. долларов. Подавляющую часть этого оборота делают средние, мелкие и частные инвесторы. В настоящее время более чем у 12 млн. британцев открыты легальные форекс-счета. Количество нелегальных форекс-счетов по некоторым оценкам примерно равно числу легальных. К нелегальным форекс-счетам относятся форекс-счета в мошеннических компаниях, не имеющих соответствующих лицензий от регулирующих органов.

Потребительский рынок Форекс, а также других инвестиционных инструментов, предназначенных для мелких и мельчайших инвесторов, имитирует и копирует финансовые рынки, где действуют институциональные и частные инвесторы. С одной стороны это выражается во все большем увлечении финансового рынка для граждан различного рода производными финансовыми инструментами. Для подавляющего большинства мелких частных инвесторов полноценные фьючерсы, опционы, а тем более производные деривативы высших порядков являются слишком сложным инструментарием. Поэтому на рынке, рассчитанном на граждан, появляются свои финансовые инструменты, балансирующие на грани с мошенничеством.

Наиболее популярным из них является бинарные опционы. По сути, это инвестиционно-образное наименование лотереи. Инвестор в бинарных опционах должен угадать, будет ли расти тот или иной инструмент, например, валюта, цена на нефть и т. п. через 5, 10, 15 мин. или час. Математики посчитали, что при прочих равных условиях потерять любую сумму на бинарных опционах в 16 раз вероятнее, чем на сверхвысокорискованном рынке Форекс. На рынке Форекс свои первоначальные вложения теряет в Великобритании чуть менее 90 % инвесторов. Несложно посчитать, что на рынке бинарных опционов, в конечном счете, теряют практически все и всё.

В условиях высокой рискованности рынка Форекс, а также других финансовых рынков, рассчитанных на мелких и мельчайших индивидуальных инвесторов, им активно продаются различного рода FTS.

Когда деловые электронные ресурсы, специализированные телевизионные программы и индустрия финансового онлайн-обучения не устает повторять о пришествии эры торговых роботов в крупнейших международных и британских финансовых институтах, создается максимально благоприятная почва для продажи гражданам FTS, которые являются своего рода микроторговыми роботами. Некоторые из подобных программ ведут торговлю в полностью автоматическом режиме, другие выполняют роль советников для пользователей.

Цена на FTS колеблется от нескольких десятков фунтов до 3–5 тыс. фунтов стерлингов с дополнительной платой за абонементное обслуживание в части консультаций, обновления версий и т. п. Масштабы рынка FTS для мелких и сверхмелких инвесторов составляет по различным оценкам от 300 до 700 млн. фунтов стерлингов. При этом практически все эксперты сходятся на том, что темпы роста этого рынка составляют до 100 % в год.

Такой умопомрачительный рост связан с тем, что полностью автоматизированные, не требующие участия человека FTS, покупают наиболее малообразованные и далекие от финансового рынка пользователи, как правило только что приехавшие в Великобританию, или получившие гражданство в течение своей жизни. Поскольку беженцев и новых британцев становится все больше и больше, есть основания полагать, что данный рынок будет и далее расти взрывными темпами.

Было бы преувеличением относить всех разработчиков и программистов, занятых в FTS, к числу преступников. Также было бы несправедливо утверждать, что FTS вообще не способны показывать устойчивых прибыльных результатов. Анализ финансовой и математико-статисти-

[23] *Finance trade system – автоматические финансово-торговые системы. Используются частными и мелкими корпоративными инвесторами для торговли на рынках Форекс (Forex), фондовом рынке и т. п. – Прим. переводчика.*

ческой периодики, докладов различных финансовых институтов показывают, что существует определенное число FTS, дающих высокую, а иногда очень высокую прибыль в течение длительного периода времени. Однако реальность такова, что практически все подобные FTS имеют совершенно иную цену, чем FTS, предлагаемые на рынке для граждан, и используются финансовыми институтами различного масштаба и институциональными инвесторами как внутренние, скрываемые и особо охраняемые финансовые инструменты. Любая эффективная FTS сама по себе является важнейшим цифровым активом, ни в коем случае не предназначенным для широкого использования.

В этой связи FTS для населения изготавливают либо программисты и разработчики, а также различного рода стартапы, стремящиеся через эксперименты с чужими деньгами разработать действительно эффективные торговые системы для собственного использования, либо те, кто заранее понимает, что их инструменты принесут покупателям только убытки.

Подавляющую часть подобного рода продукции создают преступники-программисты-одиночки, либо программистские преступные группы. Как правило, они стараются не формализовать свои организационные структуры, что повышает их неуловимость и безопасность. В то же время, по оценкам офицеров британской полиции, в последние два года наблюдается процесс синдикации этого рынка, когда крупные киберпреступные группировки, в основном выходцы с постсоветского пространства, берут под контроль одиночек и небольшие группы и облагают их своего рода налогом за право работать на британском рынке FTS.

Несмотря на относительно небольшие размеры прямого ущерба граждан от покупки FTS, в значительной мере, созданных преступниками, реальные потери граждан, а соответственно доходы киберпреступности, на порядки выше. Как показывают частные и журналистские расследования, проведенные за два последних года в немалом числе случаев производители частных FTS аффилированы с преступными, мошенническими форекс-порталами. В этих случаях владельцы подобных форекс-порталов, для того, чтобы создать рекламу соответствующим FTS, а также привлечь больше денег пользователей на портал, преднастраивают торговых роботов таким образом, чтобы они первоначально обеспечили все возрастающие размеры выигрыша, и лишь затем, когда инвесторы войдут во вкус, практически гарантированно вели подавляющую их часть к проигрышу. В этом нет ничего нового. Именно таким образом устроены подпольные казино и карточные клубы. Теперь это действует в киберпространстве.

– **Киберпреступность, связанная с высокочастотным трейдингом**. Если FTS – это автоматический трейдинг для бедных, то высокочастотный трейдинг – это прерогатива крупнейших финансовых институтов и инвесторов. Стоимость высокочастотных трейдинговых платформ и систем коммуникации тщательно скрывается финансовыми институтами, но в ряде случаев составляет десятки, а возможно и сотни миллионов фунтов стерлингов.

В настоящее время высокочастотный трейдинг, а также использование автоматизированных торговых платформ берет на себя более 70 % всего мирового оборота глобальных финансовых рынков. Британские банки и иные финансовые институты – не исключение. Они, также как и учреждения Уолл-стрит, находятся среди лидеров. По некоторым оценкам в крупнейших банках мира, включая основные британские, более 90 % сделок в настоящее время подготавливаются и осуществляются торговыми робото-техническими платформами. Данные показатели относятся к срочным финансовым рынкам, где сделки осуществляются в режиме онлайн и не включают в себя рынки IPO, M&A и т. п.

Киберпреступность, связанная с высокочастотным трейдингом и сложными автоматизированными торговыми платформами, это прерогатива крупных высокотехнологичных криминальных кибергруппировок, располагающих значительными ресурсами, возможностями и кадрами. Имеются три основных направления деятельности криминала в этой сфере.

Первое связано с основой высокочастотного трейдинга – системами информационных коммуникаций. При этом виде трейдинга счет идет не на секунды, а на миллисекунды, поэтому

преступники занимаются перехватом сигналов, либо их задержкой. Это позволяет клиентам преступных группировок, к которым зачастую относятся легальные финансовые структуры, получать долесекундные преимущества в знании о новой рыночной информации, либо создавать препятствия для конкурентов.

Вторым известным направлением является сознательное злонамеренное проникновение в программные комплексы торговых платформ с целью вывода их из строя в строго определенных ситуациях. Такого рода операции киберпреступники опять же производят на заказ. Они позволяют за счет отказа одного или нескольких крупных участников рынка прогнозируемым образом уменьшить общие объемы торгов и соответственно спрогнозировать движение цены на тот или иной актив.

Наконец третий вид киберпреступности, связанный с роботизированной торговлей потенциально носит наиболее опасный характер. До настоящего времени достоверно не было установлено ни одного случая подобной киберпреступности, в отличие от описанных выше двух направлений. Но по твердому убеждению математиков, IT специалистов и финансистов, с которыми проводились консультации, данный вид финансовой преступности неизбежно появится в ближайшее в прямом смысле слова время.

Высокочастотный трейдинг и сложные алгоритмические торговые платформы являются программно-аппаратными комплексами. Как любая программа, они выполняют те или иные действия строго по записанным в программе правилам. Любая программа представляет, в конечном счете, набор алгоритмов, использующих какие-либо математические модели, в которых устанавливается зависимость между переменными с целью максимизации результатов.

По мнению специалистов, имея как минимум двухлетнюю историю работы любого программного комплекса, можно с высокой степенью вероятности, определить, какие алгоритмы и математические модели лежат в основе программы по действиям этого комплекса на рынке. Далее можно понять, на какие конкретно новости, события и факты и каким образом, а точнее, по каким правилам реагируют торговые роботы при принятии решений о купле, продаже или отсутствии реакции на рынке. Зная набор событий, фактов и новостей, можно предугадать действия торговых роботов самого сложного вида. Далее, принимая во внимание, что сигналы о событиях торговые роботы получают по телекоммуникационным каналам и соответственно сигналом для операции является не само по себе событие, а его отражение в информационных агентствах, системах деловой информации, типа «Блумберг» или «Рейтерс», на телевидении и т. п., несложно сделать заключительный шаг. Он состоит в манипуляции новостными или событийными потоками или конкретными фактами, т. е. сообщение, а не событие становится сигналом для операции торгового робота.

Принимая во внимание, что преступное сообщество не только широко представлено в средствах массовой информации, но и проникло в организации-поставщики баз данных, а также деловых событий, нетрудно понять, что киберпреступники заранее могут предсказать действия совокупности торговых платформ, как отклик на то или иное событие. Если событие не подтвердится, то рынок будет скорректирован. Этот механизм открывает широкий простор для финансовой киберпреступности. Именно здесь коренится возможность получения ей не миллионных, а миллиардных прибылей.

В заключение хотелось бы отметить следующий ключевой факт. **Финансовая киберпреступность является наиболее прибыльным, а потому опасным видом киберпреступности вообще.** В случае экономической киберпреступности, которой посвящена основная часть доклада с детальными расчетами, киберпреступникам необходимо не только криминальным путем овладеть тем или иным активом, но и реализовать его. Любая реализация актива, добытого преступным путем, чревата следами, дополнительными затратами и риском.

Преступников, в конечном счете, интересует ни интеллектуальная собственность, ни коммерческая тайна, ни различного вида цифровые активы и даже ни краденные из интер-

нет-магазина товары, а деньги. В случае финансовой киберпреступности добычей криминала становятся именно деньги, либо абсолютно конвертируемые активы в виде различных инструментов финансового рынка. В данном случае отпадают дополнительные затраты, время и риски, связанные с окэшиванием активов. Может возникнуть вопрос: ведь в случае финансовой преступности остается необходимость отмывки денег. Однако, как свидетельствует история преступности и опыт борьбы с ней в глобальном масштабе никогда никому и нигде не удалось поставить действенный заслон этому процессу. Криминальные деньги являются кровью глобальной экономики. Без нее современная финансовая система существовать не может.

Кто они – компьютерные преступники?

На самом высоком уровне, используя наиболее сложные инструменты и методы, киберпреступностью занимаются **иностранные спецслужбы**. Используя киберкриминал, иные государства могут оказывать существенное влияние на экономику Великобритании путем кражи интеллектуальной собственности, промышленного шпионажа и расстройства целостности финансовой британской системы. Киберпреступные группы, за которыми стоят иностранные разведки, как правило, высоко организованы, используют самый современный высокотехнологичный инструментарий и располагают обширными ресурсами. Безусловным лидером в государственной киберпреступности против Великобритании является Китай. Особое внимание государственная киберпреступность уделяет краже интеллектуальной собственности. Это позволяет не только решить вопросы государственной безопасности для этих стран, но и повысить конкурентоспособность их экономики за счет прямой кражи технологий, разработок, программ. Кроме того, такие кражи позволяет минимизировать государственные расходы на НИОКР и тем самым преодолеть технологическое отставание.

Другим приоритетом для государственных киберпреступников является промышленный шпионаж, включая кражу коммерческой информации у британских и базирующихся на Британии трансграничных корпораций, которые широко вовлечены в международные контракты, тендеры, конкуренцию за рынки сбыта. Имеющиеся данные показывают, что, как правило, такого рода кибершпионажем и киберпреступностью занимаются не сами по себе азиатские хозяйственные субъекты, а стоящие за ними, а в Китае – над ними, правительства.

Следующий уровень – это **большие организованные преступные сети.** Они с каждым годом все больше переориентируются на киберпреступность, которая привлекает их максимальной выгодой при относительно невысоких инвестициях и минимальном риске. Есть основания полагать, что банды из менее технологически развитых государств сосредоточены, прежде всего, на крупных онлайн мошенничествах и онлайн кражах данных и ресурсов у бизнеса. Здесь безусловными лидерами являются преступные группировки, базирующиеся на Центральной и Восточной Европе и Юго-Восточной Азии.

Криминальные сети и группировки из стран с развитыми IT технологиями сосредотачиваются на финансовой киберпреступности и коммерческом шпионаже. Последний включает в себя не только традиционный промышленный шпионаж, связанный с технологиями, документацией и т. п., но и добычей инсайдерской информации, необходимой для конструирования сложных сделок и игры на финансовом, особенно фондовом рынках. Здесь лидерами являются российские кибергруппировки, которые приобрели транснациональный характер и имеют филиалы в Великобритании, странах ЕС, Соединенных Штатах. В последние годы конкуренцию русским начинают составлять мексиканские преступные группировки, использующие в основном американских программистов и хакеров, и бразильские сети.

В условиях нарастания глобальной конкуренции и долгосрочного углубляющегося кризиса мировой экономики, вероятно, следует ожидать, что **законные организации** – легальные корпорации, компании, финансовые институты, университеты и т. п. – будут все активнее

вовлекаться в киберпреступность, прежде всего, по таким направлениям, как кража интеллектуальной собственности, промышленный или научно-технологический шпионаж и добыча закрытой коммерческой информации преступными методами. При этом маловероятно, что подавляющая часть легальных организаций будет создавать внутри организации специализированные группы и подразделения, занимающиеся киберпреступлениями. У крупных и известных организаций слишком велики риски репутационных потерь, а соответственно и колоссального снижения капитализации, если произойдет утечка информации о подобного рода деятельности.

В этой связи следует ожидать активизации процессов, которые идут последние 10 лет. Они связаны с формированием рынка вольных преступных команд и преступников-одиночек, которые через специальную сеть посредников нанимаются на выполнение тех или иных конкретных заданий. Думается, что все большее число талантливых программистов, разработчиков, «белых» хакеров будет вовлекаться в преступную деятельность через хорошо отлаженную и законспирированную сеть посредников, ядро которых составляют бывшие сотрудники спецслужб и правоохранительных органов.

В условиях, когда конкуренция возрастает, а финансово-экономические условия ухудшаются, для всё большего числа юридических лиц становится важной не столько максимизация прибыли, сколько обеспечение выживаемости, вряд ли следует ожидать сохранения сложившейся западной и особенно британской деловой этики. Есть основания полагать, что перед угрозой проигрыша в конкурентной борьбе, банкротства, дефолта и т. п., все большее число компаний будет искать посредников, которые позволят им достигать целей любыми, в том числе преступными средствами.

На низшем уровне – **небольшие группы и отдельные киберпреступники** будут продолжать осуществлять, расширять и совершенствовать свою киберкриминальную деятельность против малого бизнеса, стартапов и отдельных граждан Великобритании. Именно эти сектора бизнеса и общества наиболее уязвимы перед высокотехнологичными преступниками. Есть основания полагать, что на этом уровне в число основных направлений киберпреступности будут входить кибермошенничества, кража личных данных, мошенническая онлайн торговля, фискальные мошенничества и вымогательства и скрейвейрпреступность.

При том, что в среднем уровень сложности методов и программных инструментов, использованных киберпреступниками – одиночками, либо небольшими группами будет заметно уступать аналогичным показателям для более высоких преступных уровней, следует ожидать и многочисленных исключений. Вероятно, что особенно в ближайшие годы, на начальной стадии формирования пирамиды киберпреступности, отдельные криминальные индивидуумы и группы, работающие по найму на более высоких уровнях, будут склонны к получению дополнительного заработка на самом нижнем уровне в качестве «вольных стрелков», работающих на себя.

Часть II
О формировании мафиозно-террористических государств

Связи между терроризмом и транснациональной организованной преступностью[24]

А. Характер связей

Теоретически, цели террористов и транснациональных организованных преступных групп различны. Террористические группы преднамеренно подрывают государственную власть и пытаются добиться политических изменений с помощью насильственных мер по многим причинам, в том числе идеологического характера. Демонстративные нападения и целенаправленное насилие, в том числе сексуальное насилие и насилие в отношении меньшинств, осуществляются для привлечения внимания международных средств массовой информации, которые, в свою очередь, вносят свой вклад в осуществляемые этими группами усилия по вербовке сторонников. Террористы исходят из того, что чем шире распространяются их взгляды, в том числе средствами массовой информации, тем большее число сторонников, общественных деятелей и активистов они сумеют привлечь на свою сторону. Деньги рассматриваются не как цель, а как инструмент, дающий им возможность продолжать борьбу с государственной властью.

Группы, вовлеченные в транснациональную организованную преступную деятельность, занимаются, как правило, подпольной деятельностью, стараясь не привлекать к себе внимания со стороны государственных органов и средств массовой информации. Преступные организации используют существующее положение дел в целях обогащения и не пытаются добиться политических перемен. Цель осуществляемого ими подрыва государственной власти состоит в том, чтобы создавать, расширять и сохранять условия, благоприятствующие их деятельности.

На практике же вышеприведенное теоретическое различие не всегда очевидно. Некоторые террористические группы связаны с транснациональной организованной преступностью и принимают активное участие в ее деятельности. Оба типа таких групп играют определенную роль в сохранении нестабильности, которая в свою очередь служит благодатной почвой для деятельности этих групп. Транснациональные организованные преступные группы могут предоставлять финансы, оружие и другие средства, необходимые террористическим группам для поддержания их деятельности.

О наличии связей между террористическими и транснациональными организованными преступными группами не раз говорилось в последние годы, при этом существуют разные мнения о характере, масштабах и глубине таких связей. Поскольку терроризм и транснациональная преступность непрерывно эволюционируют, без конкретных примеров, свидетельствующих о том, что эта проблема представляет собой растущую угрозу для международного мира и безопасности, сложно вынести какие-либо общие суждения о том, каким образом происходит их взаимное усиление.

---

[24] Доклад Генерального секретаря ООН об угрозе, связанной с извлечением террористами выгоды из транснациональной организованной преступной деятельности. Совет Безопасности ООН, 21 мая 2015 г., S/2015/366. (Извлечение)

С концептуальной точки зрения взаимодействие между террористическими и транснациональными организованными преступными группами не является прямолинейным. Террористические группы извлекают выгоду из деятельности транснациональной организованной преступной деятельности с помощью таких методов, как: принуждение или обложение налогами, сотрудничество и непосредственное взаимодействие.

Во-первых, некоторые террористические группы осуществляют сбор платы за «безопасный» провоз контрабанды. Поступают сообщения о том, что действующие в Сахеле преступные группы платят организации «Аль-Каида» в странах исламского Магриба за беспрепятственный провоз товаров из Западной Африки на побережье Средиземного моря.

Во-вторых, некоторые террористические группы, судя по всему, сотрудничают с транснациональными организованными преступными группами с целью получения специальных сведений, например, о методах отмывания денег, и оперативной поддержки, в частности для получения доступа к контрабандистским маршрутам или для изготовления поддельных документов для въезда иностранных боевиков-террористов. В Ираке и Сирийской Арабской Республике так называемое «Исламское государство Ирака и Леванта» (ИГИЛ) использует давно существующие контрабандистские сети для экспорта добытой незаконным путем сырой нефти с использованием автоцистерн, эксплуатируемых, как правило, частными посредниками.

В-третьих, некоторые террористические группы напрямую участвуют в преступной деятельности. Имеются сообщения о том, что Исламское движение Узбекистана для финансирования своих террористических операций принимает непосредственное участие в незаконном обороте наркотиков. Аналогичным образом, группировка «Абу-Сайяф», как утверждается, раскололась на ячейки, большинство из которых, судя по всему, руководствуются скорее погоней за деньгами, нежели идеологией.

B. Основные направления

1. *Незаконный оборот оружия*

Одной из причин, создающих угрозу для безопасности, является незаконная торговля стрелковым оружием, легкими вооружениями и боеприпасами. Такое оружие, дешевое, легкое, простое в обращении, которое нетрудно перевозить и прятать, чаще всего применяется террористами и организованными преступными группами для совершения нападений. Бесконтрольное стрелковое оружие неизменно является источником проблем на всех континентах. Накопление стрелкового оружия само по себе не может стать причиной конфликтов, в которых оно используется, однако его чрезмерная концентрация и широкая доступность являются одними из ключевых факторов, способствующих возникновению конфликтов. Насилие носит все более смертоносный и продолжительный характер, усиливается чувство незащищенности, что, в свою очередь, ведет к повышению спроса на оружие.

Для обеспечения своего оперативного потенциала террористические группы используют оружие, поставляемое региональными преступными сообществами контрабандным путем. После падения правительства Ливии в 2011 году принадлежащие государству запасы оружия были разграблены и незаконно переправлены в соседние и более отдаленные страны, где они попали в руки террористов и организованных преступных групп, которые в настоящее время используют их для дальнейшего распространения нестабильности в регионе и за его пределами.

2. *Торговля людьми и незаконный ввоз мигрантов*

Значительные доходы от торговли людьми получает, например, ИГИЛ. Организация Объединенных Наций располагает документально подтвержденной информацией о том, что ИГИЛ, в особенности с июня 2014 года, занимается торговлей женщинами и детьми между

Ираком и Сирийской Арабской Республикой, объектом которой являются езидские и туркменские девочки, которых ИГИЛ захватил в Ираке и переправил в Сирию, чтобы продать их в качестве сексуальных рабынь. Несовершеннолетних мальчиков, захваченных ИГИЛ или зачисленных на службу в качестве «добровольцев», также насильно перевозят через границу для прохождения военной подготовки и проведения идеологической обработки.

Террористические группы могут быть причастны к незаконному ввозу боевиков в зоны конфликтов, который осуществляется через широкую сеть вербовщиков, изготовителей поддельных документов и лиц, осуществляющих доставку людей в зоны конфликтов. Террористические группы могут также эксплуатировать потоки беженцев и мигрантов, которые собирают значительные суммы для оплаты безопасного проезда.

По мнению Исполнительного директората Контртеррористического комитета, террористические организации и организованные преступные группы в Юго-Восточной Европе извлекают выгоду из незаконного ввоза людей путем сбора «налогов», осуществляемого во время пересечения границы или после незаконного обустройства мигрантов. Эксплуатация незаконных мигрантов и жертв торговли людьми дает террористическим организациям возможность проводить вербовку в Юго-Восточной Европе и Центральной Азии.

3. *Незаконный оборот наркотиков*

Согласно оценкам, данным в рамках Программы УНП ООН по борьбе с торговлей опиатами в Афганистане, в 2009 году доходы афганского движения «Талибан» от *торговли опиатами* составили около 155 млн. долл. США; эта сумма была получена за предоставление организованным преступным группам наркоторговцев «защиты» и беспрепятственного транзита на территориях, где они имеют значительное присутствие. В то же время афганские наркобароны используют доходы от незаконной торговли наркотиками в Афганистане для финансирования «Талибана». Движение «Талибан», помимо сотрудничества с наркоторговцами, подключается к каждому звену производственно-сбытовой цепочки, задействованной в процессе торговли наркотиками (выращивание, производство и незаконный оборот, в частности путем обложения фермеров налогами, например, взимая 10-процентный «ушр» («земельный налог») с дохода фермеров, выращивающих опийный мак, в провинции Гильменд. Влияние движения «Талибан» на производственно-сбытовую цепочку ощущается также в связи с расположением лабораторий по производству наркотиков в непосредственной близости от учебных лагерей «Талибана».

Согласно оценкам УНП ООН, приведенным в докладе “Transnational Organized Crime in West Africa: A Threat Assessment” («Транснациональная организованная преступность в Западной Африке: оценка угрозы») (февраль 2013 года), в 2010 году в Европу из Западной Африки было незаконным образом доставлено 18 тонн *кокаина* на сумму примерно 1,25 млрд. долл. США по оптовым ценам; это означает, что в указанном году приблизительно 10 процентов находящегося в Европе кокаина (внутреннее потребление плюс конфискованные партии) поступило из Западной Африки. Постоянно поступают сообщения о том, что контрабанда кокаина осуществляется по суше через пустыню Сахара на средиземноморское побережье. Помимо того, что эта территория труднопроходима, а протяженность дорог невелика, за данный регион ведут борьбу вооруженные группы. Часто утверждается, что эти группы получают средства благодаря участию в незаконном обороте наркотиков, но при этом убедительных доказательств, подтверждающих это утверждение, пока недостаточно. В переправке наркотиков через Западную Африку предположительно участвует организация «Аль-Каида» в странах исламского Магриба (АКИМ). Торговцы, регулярно использующие дороги в Сахеле, сообщают о том, что к неофициальному обложению налогами всех контрабандных товаров причастна некая группа, связанная с действующей в этом регионе организацией «Аль-Каиды» в Исламском Магрибе.

Согласно сообщениям, к осуществлению незаконного оборота наркотиков или к получению от него выгоды причастен ряд других групп, в том числе, помимо прочего, ИГИЛ, Фронт «Ан-Нусра» и Исламское движение Узбекистана.

4. *Незаконный оборот культурных ценностей* Еще одна тенденция, вызывающая все большую озабоченность, особенно в Ираке и Сирийской Арабской Республике, связана с разграблением культурных ценностей и их незаконным оборотом, осуществляемым террористическими группами. ИГИЛ, Фронт «Ан-Нусра» и другие лица и организации, связанные с «Аль-Каидой», получают доход, участвуя в разграблении предметов культурного наследия в Ираке и Сирийской Арабской Республике и в их незаконном вывозе. Доход, полученный в результате этой деятельности, используется для поддержки их усилий по вербовке и для укрепления их оперативных возможностей. По данным Организации Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО), незаконные раскопки археологических объектов в Сирийской Арабской Республике являются одним из основных источников незаконного оборота культурных ценностей и наносят этим объектам серьезный и необратимый ущерб, как и поставка похищенных при разграблении предметов для продажи на региональных и международных черных рынках. Как было отмечено Группой по аналитической поддержке и наблюдению за санкциями, ИГИЛ получает доходы за счет обложения грабителей налогами. Грабежи становятся более систематическими и организованными. Например, сообщалось о том, что ИГИЛ стало принимать более широкое участие в раскопках в исторических местах и использует для этого подрядчиков с бульдозерами. Выкопанные предметы затем продаются местным перекупщикам. Доходы, полученные в результате незаконного оборота культурных ценностей, используются для финансирования и поддержки террористической деятельности.

5. *Незаконная эксплуатация природных ресурсов и торговля ими*

Имеются многочисленные примеры эксплуатации террористическими группами, прямо или косвенно, природных ресурсов на территориях, находящихся под их контролем. К числу таких природных богатств относятся минеральные ресурсы, в частности золото, древесный уголь и нефть. Так, согласно данным Группы контроля Организации Объединенных Наций по Сомали и Эритрее, общий объем экспорта древесного угля из Сомали в 2013 и 2014 годах превысил 250 млн. долл. США. Примерно третья его часть, по оценкам, пришлась на организацию «Аш-Шабааб».

Согласно информации Группы по аналитической поддержке и наблюдению за санкциями, наиболее важным источником постоянных доходов ИГИЛ является незаконная продажа нефти и его способность задействовать давно существующие сети контрабанды сырьевых товаров, для чего используются баржи, большое количество бочек и трубы малого диаметра, обычно применяемые при орошении. Однако преобладающим методом контрабанды сырой нефти, как представляется, является использование автоцистерн, во многих случаях эксплуатируемых частными посредниками. Сообщается, что посредники находят покупателей как в этом регионе, так и на международном рынке. ИГИЛ захватило несколько действующих месторождений, на которых добываются тысячи баррелей в день; поступления от этой добычи могут составлять до 2 млн. долл. США в день.

В Афганистане движение «Талибан» глубоко проникло в сектор природных ресурсов и довольно широко обложило этот сектор поборами: «Талибан» непосредственно участвует в добыче природных ресурсов. Движение также вымогает или пытается вымогать деньги у имеющих правительственную лицензию или нелицензированных горнорудных предприятий; и выступает в роли «поставщика услуг» для этих горнорудных предприятий.

6. *Похищение людей с целью получения выкупа*

Террористические группы все активнее вовлекаются в похищение людей с целью выкупа или в похищение людей с целью получения политических уступок, особенно на Ближнем Востоке, в Северной Африке, в Сахеле и в Средиземноморском регионе, часто при поддержке со стороны транснациональных преступных сетей. Полученные от выкупа средства позволяют террористическим и преступным группам расти, вербовать сторонников или закупать оружие, что сказывается на безопасности.

В тех случаях, когда террористы прибегают к похищению людей с целью выкупа в качестве одного из источников финансовых средств, они часто не принимают прямого участия в самом похищении, а действуют с помощью бандформирований, которые похищают жертв и передают их в руки террористов.

Для ИГИЛ получение выкупа по-прежнему является важным источником финансирования, что перекликается с основанной на похищении людей тактикой «Аль-Каиды» в Ираке. Жертвами в основном являются местные жители, а также небольшая группа работников международных гуманитарных организаций и журналистов.

В Афганистане число граждан страны и иностранцев, похищенных движением «Талибан» с 2003 года по 2014 год, постоянно увеличивалось. Общая сумма выкупа, уплаченная за освобождение иностранцев, составляет, по оценкам, не менее 16 млн. долл. США. Движение «Талибан» – или преступные группы, действующие от его имени, – все в большей степени используют похищения людей не в качестве средства запугивания и устрашения, а как механизм, мишенью которого являются ценные в финансовом отношении иностранцы или местные граждане.

Основными источниками дохода организации «Аль-Каида» в странах исламского Магриба является торговля людьми и похищение людей с целью получения выкупа. Согласно оценкам, доходы этой группы за период с 2008 года составляют приблизительно 91,5 млн. долл. США. В Нигерии и Камеруне «Боко харам» также выбирает в качестве жертв высокопоставленных должностных лиц этих стран.

7. *Отмывание денег и финансирование терроризма*

Доходы транснациональной организованной преступности могут использоваться для оказания содействия террористическим организациям и финансирования террористических актов с помощью разных способов, к числу которых относятся злоупотребление статусом некоммерческих и благотворительных организаций как в целях сбора средств на террористическую деятельность, так и в целях перевода денежных средств; использование новых способов оплаты, в том числе современных телекоммуникационных технологий и новых финансовых продуктов, таких как электронные валюты; и физическая трансграничная перевозка валюты и оборотных документов на предъявителя. По оценкам Исполнительного директората Контртеррористического комитета, эта практика особенно широко распространена в некоторых регионах; в Восточной и Западной Африке организованные преступные группировки, активно использующие наличные денежные средства, зачастую связаны с терроризмом.

В Пакистане организация «Лашкар-и-Тайба» использует подставные благотворительные организации для прикрытия своей деятельности, в том числе занималась сбором средств, принимает меры в обход санкций, а также предоставляет социальные услуги (строит школы и больницы в общинах), одновременно вербуя в свои ряды новых членов.

По сведениям Группы по аналитической поддержке и наблюдению за санкциями, «Аль-Каида» и ее филиалы продолжают использовать в своих целях формальные и неформальные финансовые системы, чтобы с их помощью перемещать средства через границы и финансировать свою деятельность.

С. основные политические и стратегические последствия

Извлечение террористическими группами выгоды из организованной преступной деятельности представляет все большую угрозу международному миру и безопасности. Их деятельность хорошо финансируется, с ней труднее бороться, и она обладает большими оперативными возможностями. Это, в свою очередь, ведет к усилению прямой угрозы с их стороны, суверенитету государств, в том числе за счет проведения военных кампаний и установления контроля над территорией и населением, не ограничиваясь пределами одного государства.

Такие группы, как ИГИЛ, коренным образом изменили характер глобальных угроз, исходящих от террористических организаций. Взаимодействуя с транснациональными организованными преступными группами, а также самостоятельно совершая преступления, ИГИЛ продолжает аккумулировать ресурсы, необходимые для установления и удержания контроля над территорией и населением.

Как показывает ситуация с «Боко харам», нестабильность в плане безопасности в одной из частей страны может быстро распространиться на соседние страны и поставить под угрозу безопасность целого региона. Согласно Управлению Организации Объединенных Наций по координации гуманитарных вопросов, с момента объявления чрезвычайного положения в Нигерии в мае 2013 года, почти 1,9 миллиона человек в регионе были вынуждены покинуть свои дома, в том числе 1,5 миллиона человек в Нигерии, 96 000 человек в Камеруне, 50 000 человек в Нигере и 15 000 человек в Чаде. Кроме того, значительное число нигерийцев ищут убежища в соседних странах.

Кроме того, террористы, извлекающие выгоду из транснациональной организованной преступности, могут подорвать легитимность государства и более медленными темпами, что может в итоге отразиться на международном мире и безопасности. Доходы, полученные преступным путем, часто используются для дачи взяток должностным лицам правительства. Коррупция подрывает принцип верховенства закона и является благодатной почвой для дальнейшей преступной деятельности, создавая порочный круг безнаказанности. Это, в свою очередь, ведет к ослаблению государственных институтов, подрывает устойчивое экономическое развитие, а также лишает легитимности государство.

Слабость государственной власти побуждает террористов и преступников к тому, чтобы стремиться получить контроль над ключевыми районами, в частности маршрутами торговли людьми и контрабанды, а также секторами экономики для ведения своей противозаконной деятельности. В некоторых случаях незаконные субъекты предоставляют защиту и даже социально-экономические блага населению, проживающему на контролируемой ими территории, что еще больше ослабляет и подрывает легитимность государства, а также возможности в плане обеспечения надлежащего управления.

В развивающихся странах ограничены возможности для законной трудовой деятельности, что может быть одним из многих факторов, в силу которых отдельные лица вступают в преступные или террористические группы и которые могут способствовать сохранению проблемы отсутствия безопасности. Кроме того, миллионы людей могут зависеть от незаконной экономической деятельности для удовлетворения своих базовых потребностей и могут выступать против инициатив по борьбе с преступностью или негласно препятствовать их осуществлению.

Серьезность угрозы, исходящей от ИГИЛ и связанных с ним групп и организаций[25]

Угроза

Становлению ИГИЛ способствовали затяжные конфликты в Ираке и Сирийской Арабской Республике и обусловленная ими политическая нестабильность и отсутствие безопасности, а также ослабление государственных институтов и неспособность государства осуществлять действенный контроль над собственной территорией и границами. Меньше чем за два года ИГИЛ удалось захватить обширные территории в Ираке и Сирийской Арабской Республике, управление которыми осуществляется с помощью сложной, квазибюрократической структуры получение доходов, которая является достаточно гибкой и диверсифицированной и позволяет компенсировать сокращение поступлений из отдельных источников. ИГИЛ также извлекает выгоду из его связей с лицами и группами, замешанными *в транснациональной организованной преступности*. Оно использует имеющиеся в его распоряжении финансовые средства для финансирования текущих военных кампаний, управления находящимися под его контролем территориями, а также распространения конфликта за пределы Ирака и Сирийской Арабской Республики. Оно разработало чрезвычайно эффективную и сложную стратегию коммуникации, благодаря которой насаждаемое им искаженное представление о мире находит отклик у небольшого, но постоянно растущего числа недовольных граждан, которые отказались от принятых в их странах основных ценностей или перестали чувствовать сопричастность этим ценностям.

Наблюдаемое в последнее время распространение сферы влияния ИГИЛ на страны Западной и Северной Африки, Ближнего Востока и Южной и Юго-Восточной Азии наглядно свидетельствует о росте темпов и масштабов обострения угрозы всего за 18 месяцев. Сложный характер совершенных в последнее время нападений и объем связанного с ними планирования, координации и технического оснащения вызывают обеспокоенность в отношении хода развития событий в будущем. Кроме того, его базовая идеология является достаточно привлекательной для других террористических групп, в результате чего некоторые из них, в том числе Совет исламской молодежной шуры и «Исламское государство Ирака и Леванта в провинции Ливия (Дерна)» в Ливии, организация «Моджахеды Кайруана» и «Джунд аль-Хилафа» в Тунисе, «Исламское движение Узбекистана», «Тегрик-э-Хилафат» в Пакистане и «Ансар аль-Хилафа» на Филиппинах, принесли клятву верности так называемому халифату и самопровозглашенному халифу. ИГИЛ также извлекает выгоду из постоянного притока иностранных боевиков-террористов, которые продолжают сниматься с насиженных мест для пополнения его рядов. Еще одной серьезной проблемой является возвращение иностранных боевиков – террористов с полей сражений в Ираке и Сирийской Арабской Республике и в других зонах конфликта, поскольку благодаря им у ИГИЛ появляется возможность обеспечить свое присутствие в государствах их происхождения и использовать их навыки и боевой опыт для привлечения новых сторонников, создания террористических сетей и совершения террористических актов.

ИГИЛ за пределами Ирака и Сирийской Арабской Республики

[25] Доклад Генерального секретаря ООН об угрозе для международного мира и безопасности, которую создает ИГИЛ (ДАИШ), и о масштабах усилий Организации Объединенных Наций по оказанию поддержки государствам-членам в борьбе с этой угрозой. Совет Безопасности ООН, 29 января 2016 г., S/2016/92. (Извлечение)

О растущей угрозе для международного мира и безопасности, которая исходит от ИГИЛ, свидетельствует его стратегия распространения влияния на весь мир, разработка которой, возможно, представляет собой ответную реакцию на утрату территорий в Ираке и Сирийской Арабской Республике, которая в последнее время была вызвана международными усилиями в военной области. На 15 декабря 2015 года клятву верности ИГИЛ, по сообщениям, принесли группы из разных стран мира. Кроме того, в связи с объявлениями ИГИЛ о создании новых «провинций», в 2016 году ожидается рост числа и численности связанных с ИГИЛ групп. Это вызывает серьезную озабоченность, поскольку такие группы, как представляется, копируют тактику ИГИЛ и осуществляют террористические акты от его имени.

В 2016 году и последующий период государствам – членам следует готовиться к дальнейшему увеличению числа иностранных боевиков – террористов, которые по поручению ИГИЛ будут направляться в другие государства. С 2014 года клятву верности Абу Бакру аль-Багдади и провозглашенному «халифату» принесли многочисленные группы и лица, однако только в Ливии и Афганистане связанные с ним группы в настоящее время контролируют сколь-либо значимые территории. Действующая в Ливии связанная с ИГИЛ группа пользуется наибольшим вниманием и получает наибольший объем помощи и рекомендаций со стороны ядра ИГИЛ. В Афганистане и Пакистане ИГИЛ продолжает формировать сеть контактных лиц и сторонников, которые осуществляют нападения от его имени. 13 января 2016 года связанная с ИГИЛ группа «Провинция Хорасан», которая действует в Пакистане и Афганистане, выступила с заявлением, в котором взяла на себя ответственность за нападение на консульство Пакистана в Джелалабаде, Афганистан.

Серьезные нарушения прав человека

ИГИЛ продолжает совершать ужасающие нарушения прав человека в отношении лиц, находящихся под его контролем. Такие меры воздействия на «неверных», как казни, пытки, отсечение конечностей, истязания, гонения на этнической и религиозной почве и публичная порка, с отрезвляющей ясностью показывают, насколько варварские методы оно готово использовать для достижения своих целей. ИГИЛ систематически преследует население и членов общин, которые отказываются подчиниться его экстремистской идеологии, в том числе христиан, езидов, шиитов и суннитов. За время, прошедшее с момента появления ИГИЛ, сексуальное рабство в отношении женщин и девочек используется в качестве средства устрашения для унижения и подчинения жителей целых населенных пунктов. Сексуальное насилие, когда оно используется или поощряется как метод или тактика ведения войны или как часть широкомасштабных или систематических нападений на гражданское население, может приводить к значительному усугублению и затягиванию вооруженного конфликта и мешать восстановлению международного мира и безопасности. С учетом этого использование ИГИЛ сексуального и гендерного насилия в качестве тактики терроризма стало неотъемлемой частью его стратегии установления контроля над территорией, унижения человеческого достоинства жертв и вербовки новых сторонников.

Кроме того, тысячи детей становятся жертвами, исполнителями и свидетелями кровавых преступлений ИГИЛ. Эта группа систематически ведет идеологическую обработку детей начиная с 5-летнего возраста, воспитывая из них будущих боевиков. Миссия Организации Объединенных Наций по оказанию содействия Ираку (МООНСИ) и Управление Верховного комиссара Организации Объединенных Наций по правам человека (УВКПЧ) постоянно получают сообщения о том, что ИГИЛ осуществляет насильную вербовку детей и использует их в ходе военных операций. Ряд размещенных в социальных сетях видеоматериалов предположительно посвящены вербовке и обучению детей в лагерях ИГИЛ в Ираке и Сирийской Арабской Республике. Систематические действия ИГИЛ по вербовке детей и жестокому обращению с

детьми и сообщения об организации в ряде регионов молодежных учебных лагерей не могут не вызывать серьезную озабоченность.

Гуманитарный кризис

Международное сообщество сталкивается с гуманитарным кризисом беспрецедентных масштабов. Конфликт в Сирийской Арабской Республике является крупнейшей и наиболее сложной чрезвычайной ситуацией гуманитарного характера последнего времени, переросшей в поистине международный кризис. Только в Сирийской Арабской Республике родные места было вынуждено покинуть порядка 12 миллионов человек (включая более четырех миллиона человек, которые обратились с просьбой о предоставлении убежища в соседних государствах), а свыше 13,5 миллиона человек нуждаются в гуманитарной помощи. Появление ИГИЛ в Ираке и Сирийской Арабской Республике привело лишь к обострению гуманитарного кризиса. В отсутствие политического урегулирования в обозримом будущем и в условиях продолжающейся военной конфронтации вполне вероятно, что в 2016 году число людей, затронутых внутренним конфликтом в этих двух странах, будет расти. Присутствие значительного числа перемещенных лиц также ложится значительным бременем на ресурсы государств, соседствующих с зонами конфликта.

Уничтожение и разграбление культурных объектов и памятников материальной культуры

Частью стратегии ИГИЛ является также практика широкомасштабного и систематического уничтожения и разграбления культурных объектов, которая указывает на наличие тесной связи между такими аспектами конфликтов и терроризма, которые затрагивают культурные и гуманитарные вопросы и вопросы безопасности.

Источники финансирования ИГИЛ

Способность ИГИЛ быстро и эффективно мобилизовать огромные финансовые ресурсы для целей вербовки и территориальной экспансии наглядно показывает серьезный характер угрозы, создаваемой для международного мира и безопасности террористическими организациями, которые используют приемы, аналогичные тем, которыми пользуются транснациональные организованные преступные группировки, постоянно подстраивая свои стратегии финансирования к меняющейся обстановке.

ИГИЛ является богатейшей террористической организацией в мире. Источники ее финансирования были подробно описаны в ряде докладов, в том числе в докладах Исполнительного директората Контртеррористического комитета, Группы по аналитической поддержке и наблюдению за санкциями и Группы разработки финансовых мер борьбы с отмыванием денег. Источником средств является главным образом эксплуатация природных и экономических ресурсов оккупированных территорий (включая нефтяные месторождения и нефтеперерабатывающие предприятия и сельскохозяйственные угодья), а также ограбление банков, вымогательство, конфискация имущества, пожертвования иностранных боевиков-террористов и разграбление древностей.

По оценкам многих докладов, включая доклады МООНСИ, в 2015 году объем поступлений, полученных ИГИЛ от продажи нефти и нефтепродуктов, составил от 400 до 500 млн. долл. США. Поступления от продажи нефти ИГИЛ использует для приобретения оружия, военного снаряжения и боеприпасов. Ожидается, что благодаря воздушным ударам международной коалиции по нефтеперерабатывающим предприятиям и нефтехранилищам, перекрытию путей незаконного вывоза и продажи и приобретения нефти в 2016 году произойдет постепенное сокращение нефтяных поступлений ИГИЛ как в абсолютном выражении, так и в виде

доли в общих поступлениях. Воздушные удары наносятся и по местам добычи других ресурсов, в том числе газа и фосфатов. Кроме того, для дальнейшей разработки существующих ресурсов требуются специалисты и значительные капиталовложения, доступ к которым может быть ограничен. Вместе с тем диверсификация источников финансирования позволяет ИГИЛ быстро заменять оскудевшие источники поступлений другими.

ИГИЛ разработало сложную систему конфискации имущества и активов, в том числе в банках (по данным МООНСИ, из отделений, расположенных в находящихся под контролем ИГИЛ провинциях Ирака была изъята наличность на общую сумму в 1 млрд. долл. США, только в Мосуле было изъято банковской наличности на сумму в 675 млн. долл. США). ИГИЛ также производит конфискацию домов государственных чиновников и других лиц, которые уезжают из контролируемых им районов, и продает их на местном рынке, предоставляя скидки своим членам. Кроме того, путем поборов ИГИЛ облагает налогом хозяйственную деятельность порядка 8 миллионов человек, проживающих на подконтрольных ему территориях. Оно пытается узаконить такую систему «налогообложения», называя поборы «религиозным налогом», или «закятом». «Налог» взимается по ставке в размере не менее 2,5 процента с выручки от хозяйственной деятельности, со стоимости промышленных товаров и сельскохозяйственной продукции, включая пшеницу, ячмень, хлопок и скот; со стоимости услуг подрядчиков и торговых предприятий в западных и северных провинциях Ирака; с грузовых автотранспортных средств, въезжающих на подконтрольные ИГИЛ территории. По данным МООНСИ, поступления от сборов с грузовых автотранспортных средств составляют порядка 900 млн. долл. США в год. В некоторых случаях величина поборов достигает 10 процентов на том основании, что «страна воюет».

Чтобы ограничить возможности ИГИЛ в плане взимания подобных поборов, правительство Ирака недавно приняло решение прекратить выплату заработной платы работникам, находящимся на подконтрольной ИГИЛ территории. Вместе с тем, как представляется, для перевода денег от живущих за границей родственников используются местные услуги по типу «хавалы», которые поддаются регулированию с очень большим трудом. В то же время в более долгосрочной перспективе использовать такую систему «налогообложения» станет труднее. По информации Продовольственной и сельскохозяйственной организации Объединенных Наций (ФАО), сказанное касается в первую очередь сектора сельского хозяйства, поскольку на подконтрольных ИГИЛ территориях из-за низкого качества семян снижается урожайность таких сельскохозяйственных культур, как пшеница и ячмень.

Подобно транснациональным организованным преступным группам для обхода международного эмбарго ИГИЛ использует практику отмывания денег и контрабанды, прибегая к услугам контрабандистских сетей. ИГИЛ продает нефть и сельскохозяйственную продукцию по сниженным ценам, используя сложившиеся маршруты для их контрабандного ввоза в Ирак и Сирийскую Арабскую Республику и вывоза из этих стран. По прибытию в страны назначения определить страну происхождения товаров, особенно нефтепродуктов, весьма непросто. Основные продукты питания и сырье для населения доставляются грузовиками в составе автоколонн, а контрабандные товары прячутся в грузовиках и вывозятся с подконтрольных ИГИЛ территорий. Со всех, кто находится на подконтрольных ему территориях, ИГИЛ взимает «налоги» и сборы.

Под неусыпным контролем ИГИЛ находятся многочисленные археологические памятники в Ираке и Сирийской Арабской Республике, причем ИГИЛ взимает с расхитителей плату, размер которой устанавливается после предварительной оценки стоимости изымаемых предметов, и выдает лицензии на произведение раскопок. Как сообщает Организация Объединенных Наций по вопросам образования, науки и культуры (ЮНЕСКО), по оценкам Американской школы восточных исследований, разграблению подверглось около 25 процентов мест археологических раскопок в Сирийской Арабской Республике (включая свыше 21 процента

на подконтрольных ИГИЛ территориях). За последние четыре года Сирийская Арабская Республика изъяла или добилась возвращения свыше 6000 памятников материальной культуры (в том числе 1000 из Ливана). ЮНЕСКО отмечает, что, учитывая масштабы мародерства и значительную экономическую ценность изъятых предметов, вполне вероятно, что многие такие предметы в настоящее время хранится членами преступных сетей. Следует ожидать, что как только обстановка станет более спокойной, преступные сети начнут выбрасывать на рынок дополнительные предметы, которые до этого находились на хранении. По предварительной информации, полученной ЮНЕСКО от государств-членов, объектом контрабанды становятся, как правило, многочисленные мелкие предметы, например монеты и статуэтки, последующая реализация которых осуществляется с помощью интернет-платформ.

В дополнение к упомянутым выше источникам поступлений ИГИЛ продолжает получать выгоду от внешних пожертвований и выкупа, выплачиваемого семьями заложников, прежде всего езидами. По оценкам МООНСИ, в 2014 году объем таких выплат составил от 35 до 45 млн. долл. США. Предполагается, что для освобождения 200 иракских езидов в январе 2015 года была выплачена сумма в размере 850 000 долл. США. ИГИЛ использует сексуальное насилие для мобилизации ресурсов и финансирования своей деятельности, включая получение выкупа и продажу женщин и девочек через сети торговли людьми и на рынках рабов. Оно также получает добровольные платежи от желающих забрать иностранных боевиков-террористов из зон конфликтов. По данным Исполнительного директората Контртеррористического комитета и Группы по аналитической поддержке и наблюдению за санкциями, поступления от иностранных боевиков-террористов представляют собой значительный источник финансирования. Телеграфные переводы, изъятие денег со счетов кредитных карточек известных иностранных боевиков-террористов и денежные переводы указывают на то, что между подконтрольными ИГИЛ территориями и другими странами происходит постоянное движение финансовых средств. Для более глубокого понимания того, как устроены финансовые сети, действующие в приграничных городах, включая роль посредников, требуются дополнительные исследования.

Для мобилизации средств ИГИЛ и связанные с ним группы по-прежнему широко пользуются Интернетом и социальными сетями. Согласованное злоупотребление этими технологиями позволяет генерировать поступление значительных средств, причем обнаружить такие злоупотребления без поддержки со стороны поставщиков Интернет-услуг непросто. Это направление вызывает особую обеспокоенность в связи с потенциальной возможностью его использования иностранными боевиками-террористами, возвращающимися из Ирака или Сирийской Арабской Республики, а также местными сочувствующими для мобилизации достаточного объема финансовых средств на цели вербовки и для планирования террористических нападений в разных частях мира.

Приток иностранных боевиков-террористов в ряды ИГИЛ и связанных с ним групп и организаций

Вербовка

По данным Группы по аналитической поддержке и наблюдению за санкциями и других источников, привлекательность ИГИЛ для потенциальных новобранцев достигла беспрецедентного уровня. Так, по оценкам, в деятельности организации «Аль-Каида» и ИГИЛ и связанных с ними групп принимают активное участие около 30 000 иностранных боевиков-террористов из более чем 100 государств-членов.

Для привлечения под свои знамена новых членов ИГИЛ делает упор на социально – экономические трудности и чувства отчуждения, маргинализации, дискриминации и преследования, которые усугубляются, в частности, видимым или реальным отсутствием благого управ-

ления, неравенством, несправедливостью и отсутствием возможностей. Оно пытается создать у потенциальных новобранцев представление о том, что они смогут повысить свое социальное положение, ощутить чувство родства, самобытности и нужности, исполнить религиозный долг и собственное предназначение.

Предварительные исследования свидетельствуют о том, что в основе мотивации иностранных боевиков-террористов лежит целый ряд социально-экономических и геополитических условий в сочетании с индивидуальными обстоятельствами, которые проявляются в определенный момент времени и обусловливают уязвимость конкретного человека для вербовки или участия в совершении актов воинствующего экстремизма и терроризма.

По данным Специального представителя по вопросу о сексуальном насилии в условиях конфликта, вербуя молодых, одиноких и экономически обездоленных мужчин, стремящихся получить статус, власть и сексуальные утехи, не доступные в странах с консервативным социальным укладом, ИГИЛ также обещает им женщин. Кроме того, ИГИЛ располагает многочисленной командой специальных сетевых посредников, задача которых состоит в выявлении лиц, проявляющих интерес к этой группе на сетевых форумах. Склонение потенциальных сторонников к террористической деятельности на местном уровне или к поездке на подконтрольную ИГИЛ территорию основывается на информации о конкретных социальных и индивидуальных обстоятельствах человека.

Использование Интернета и социальных сетей в качестве средства пропаганды и вербовки

Угроза, создаваемая ИГИЛ, усугубляется в силу все возрастающей технологической вооруженности группировки. Для пропаганды своих идей среди тех, кто потенциально может вступить в его ряды, ИГИЛ все чаще использует Интернет и социальные сети. Как представляется, ИГИЛ удалось с помощью информационно-коммуникационных технологий (ИКТ), и в первую очередь через социальные сети, наладить низкозатратную и мощную систему, позволяющую вести пропагандистское вещание, выявлять потенциальных кандидатов для вербовки и специально выделять людей, которые убеждали бы их вступать в ее ряды. По этой причине резко возросло число иностранных боевиков – террористов, направляющихся в Ирак и Сирийскую Арабскую Республику. Работники органов прокуратуры и правоохранительных органов многих из затронутых действиями ИГИЛ государств все чаще сообщают о том, что иностранные боевики-террористы, потенциальные боевики и террористы, действующие в одиночку или небольшими группами, но официально не связанные с ИГИЛ, изучают пропагандистские материалы группировки в Интернете и общаются в Интернете с ее членами и сторонниками[26]. После того как сетью “Twitter” были закрыты тысячи счетов таких пользователей, ИГИЛ стал использовать другие социально-медийные сети, например, систему мгновенного обмена сообщениями “Telegram”[27]. Когда “Telegram” начнет закрывать каналы, так или иначе связанные с ИГИЛ, ИГИЛ и все, кто ее поддерживают, по всей вероятности, перейдут на пользование новыми платформами.

ИГИЛ также продемонстрировал способность адаптировать рассылаемые им интернет-сообщения с учетом аудитории. Тематику видеоматериалов, размещенных ИГИЛ онлайн за последние два года, составляли: военные действия (30 процентов); беседы с моджахедами

[26] В Соединенных Штатах Америки почти 80 процентов желающих влиться в ряды иностранных боевиков-террористов, загружали из сети материалы экстремистской пропаганды, распространяли их в Интернете либо общались в сети с другими экстремистами.

[27] Осенью 2015 года в числе рабочих каналов “Telegram” действовали каналы на английском, арабском, боснийском, индонезийском, немецком, турецком и французском языках, у каждого из которых было до 10000 пользователей.

(25 процентов); сюжеты, в которых ИГИЛ изображается как функционирующее и утопическое «государство» (18 процентов); а также казни (15 процентов). Чисто религиозная тематика реже фигурирует среди этих сюжетов. Видеоматериалы, как правило, качественно отредактированы и подготовлены на основе фильмов-боевиков и видеоигр. Такой подход применяется с целью привлечь не только молодых людей, жаждущих действовать, но и специалистов, в том числе врачей, инженеров, специалистов по информационно-коммуникационным технологиям, а также женщин и девочек. Кампании ИГИЛ по разработке собственной фирменной символики и маркетингу сопровождаются кампаниями по радикализации и вербовке отдельных граждан, и эти кампании проводят хорошо подготовленные специальные инструкторы, которые используют приложения, позволяющие беседовать в чатах в режиме онлайн, системы видеоконференционной связи и другие средства информационно-коммуникационных технологий.

Доказано, что информационно-коммуникационные технологии играют исключительно важную роль в подготовке поездок иностранных боевиков-террористов, вливающихся в силы ИГИЛ и связанных с ним группировок, в обучении «эффективным практическим методам «борьбы и распространении информации о них, а также при планирования терактов. На интернет-форумах ИГИЛ обсуждается, как наилучшим образом избежать обнаружения при пересечении границ, передвигаясь по маршрутам, которые не вызовут подозрения, а также через государства, которые имеют репутацию не обеспечивающих надлежащего контроля на своей границе. Хорошо документированы также случаи использования ИКТ для создания самодельных взрывных устройств. На интернет-форумах, где обсуждаются вопросы, касающиеся ИГИЛ, и которые проводятся на уровне «темной паутины», их участников регулярно информируют о наиболее эффективных средствах шифрования и рекомендуют использовать новые продукты в тех случаях, когда надежность применяемых ИКТ-технологий ставится под сомнение.

Еще одну проблему представляет собой сложность глобальной системы ИКТ, в связи с чем возникает ряд трудных юрисдикционных вопросов, касающихся применимости внутренних законов и полномочий государств в отношении обеспечения их соблюдения. Частным корпорациям при осуществлении своих международных операций необходимо находить способы улаживать проблемы, обусловленные коллидирующими нормами внутригосударственного законодательства. Например, компания “Facebook” разработала руководящие принципы сотрудничества с правоохранительными органами любой страны мира, в частности в том, что касается сохранения данных и реагирования на экстренные запросы. Многие частные корпорации уже применяют собственные правила пользования их услугами и могут либо удалять информацию, имеющую отношение к ИГИЛ, либо аннулировать счета пользователей, нарушающих эти правила. Подобные меры применяются корпорациями в связи с такими видами террористической деятельности, как вербовка террористов и подстрекательство к совершению террористических актов. Большинство крупных корпораций на инициативной и добровольной основе просматривают загружаемую их пользователями информацию и удаляют ту, которая не отвечает установленным ими правилам и условиям[28].

Продажа через Интернет иракских и сирийских памятников древности продолжается, несмотря на то, что торговля ими запрещена во всем мире, как предусмотрено Советом Безопасности в его резолюции 2199 (2015). Незаконные торговцы такими памятниками старины, возможно, прямо или косвенно связанные с ИГИЛ, используют платформы социальных сетей для поиска потенциальных покупателей незаконно приобретенных и вывезенных артефактов.

[28] В 2014–2015 гг. компания YouTube удалила 14 миллионов видеозаписей; Компания Facebook еженедельно получает от своих пользователей и анализирует 1 миллион уведомлений о нарушении правил пользования ее услугами (не только в связи с размещаемой террористической информацией), а компания Twitter закрыла за последние месяцы около 2000 счетов, связанных с ИГИЛ.

Передвижение иностранных боевиков-террористов

Иностранные боевики-террористы продолжают прибывать в Ирак и в Сирийскую Арабскую Республику через соседние страны. В некоторых случаях этому способствуют сходство языков и отсутствие визовых требований. ИГИЛ на деле доказал, что может эффективно устанавливать, какие меры противодействия в отношении него принимают государства-члены, и действовать в обход их. Он также доказал свою способность мастерски оповещать потенциальных иностранных боевиков-террористов с помощью Интернета и социальных сетей о любых возможных проблемах и опасностях. Даже в тех случаях, когда то или иное государство выявляет слабые места, облегчающие трансграничное перемещение иностранных боевиков-террористов, ИГИЛ может легко воспользоваться аналогичными слабыми местами, которые имеются у соседних государств.

ИГИЛ разместил в Интернете инструкции с целью облегчить передвижение иностранных боевиков-террористов в Ирак и Сирийскую Арабскую Республику. В этих инструкциях четко просматривается, что ИГИЛ хорошо осведомлен о том, какие методы применяются государствами-членами для выявления иностранных боевиков-террористов, а также о системных недостатках в контексте осуществления мер, принимаемых для отслеживания маршрутов их передвижения. Очевидно также, что ИГИЛ прекрасно информирован о трудностях в плане выявления иностранных боевиков-террористов до тех пор, пока они не отправляются непосредственно в распоряжение ИГИЛ. Многие из потенциальных боевиков не представляют интереса для правоохранительных органов в государствах их происхождения или проживания, и, следовательно, контроль за ними не осуществляется. В инструкциях ИГИЛ, кроме того, изложена подробная информация о наиболее легко проходимых маршрутах передвижения, о маршрутах, которых лучше избегать ввиду усиленных мер контроля на них, а также о том, как оптимально добраться до территорий, находящихся под ее контролем.

Наряду с этим ИГИЛ демонстрирует все больший интерес к совершению террористических актов за пределами подконтрольной ему территории и способность их осуществлять. Такие нападения совершают не только «местные» террористы, но и лица, прошедшие подготовку за рубежом, в том числе на территориях, удерживаемых ИГИЛ.

Планирование терактов ИГИЛ и содействие их осуществлению

Распространение пропагандистских материалов с помощью средств ИКТ является частью военной стратегии ИГИЛ, которое ставит своей целью дестабилизировать государства за пределами Ирака и Сирийской Арабской Республики, провоцируя конфронтацию между «верующими» и «вероотступниками». После того как под контролем ИГИЛ в 2014 году оказалась большая территория, организация изменила свою тактику, особенно во второй половине 2015 года, когда география совершаемых группировкой терактов стала расширяться. Результатом стала целая серия терактов, совершенных сторонниками ИГИЛ, которые действовали в одиночку или небольшими группами (речь идет, в частности, о нападениях на: музей в Брюсселе; кафе в Сиднее, Австралия; музей и курорт в Тунисе; поезд, следовавший в Париж; а также о теракте в Управлении здравоохранения графства Сан-Бернардино). Главной особенностью этих терактов было то, что их организация не отличалась сколь-либо существенной сложностью.

Теракты в Париже и Джакарте являются свидетельством существенного сдвига в направлении проведения крупномасштабных операций за пределами государств Ближнего Востока. Весьма вероятно, что террористы, действующие в одиночку, также будут продолжать совершать нападения. В терактах, совершенных в Париже в ноябре 2015 года, прослеживаются все

элементы классической схемы терактов «Аль-Каиды»: длительная подготовка, выбранные для нападения многочисленные объекты, запланированная серия нападений, следующих одно за другим, и участие структуры, состоящей из целого ряда скоординированно действующих подразделений, работу которой на месте направляет руководитель операции, а возглавляют лица, планирующие ее деятельность и находящиеся в Сирийской Арабской Республике, а также их пособники за пределами Франции. Новая сложная задача обусловлена присутствием небольших локальных группировок и одновременно наличием террористов, перемещающихся между Ираком и Сирийской Арабской Республикой. Данные, собранные за период с января 2015 года, свидетельствует о наличии эффективной оперативной связи между ИГИЛ и его боевиками за рубежом. Такие нападения указывают также на безусловное наличие у группировки потенциала, необходимого для того чтобы: выбирать в качестве целей крупные объекты (включая рестораны, стадионы, туристические объекты и концертные залы); выносить рекомендации относительно применения при совершении поездок тактики запутывания следов; обеспечивать оказание материально-технической поддержки; обучать навыкам обращения со средствами коммуникации, оружием и взрывчатыми веществами; удаленно вести реестр потенциальных террористов; и обращаться к сторонникам во всем мире с призывами содействовать проведению таких операций.

Те возможности, которыми ИГИЛ и связанные с ним группировки, а также его самопровозглашенные члены и сторонники располагают в плане поддержания связи из любой страны мира с помощью современных высокотехнологичных средств связи, включая мобильные телефоны и средства шифрования, для перевода финансовых средств, оказания материально-технической поддержки (например, посредством предоставления в аренду квартир и транспортных средств, приобретения оружия и изготовления начиненных взрывчаткой жилетов) и в целях запутывания следов в ходе поездок при подготовке террористических актов, являются свидетельством того, что они способны развертывать операции за пределами подконтрольной им территории.

Поскольку ИГИЛ стал использовать террористов-смертников для совершения терактов за пределами непосредственно подконтрольных ему районов, серьезность угрозы, которую он представляет для международного мира и безопасности, значительно возрастает. Даже несмотря на то, что при совершении терактов современные виды вооружений не применяются (а используются главным образом автоматическое оружие и начиненные взрывчаткой жилеты), об их эффективности реально свидетельствует как число жертв таких терактов, так и ощущение отсутствия стабильности и безопасности, которое испытывает гражданское население. Есть основания полагать, что ИГИЛ, возможно, рассчитывает в долгосрочной перспективе обеспечить себе возможности для того, чтобы при совершении терактов использовать более современные виды оружия, в том числе химическое и биологическое.

Серьезную обеспокоенность вызывают также все более широкие возможности террористических групп в плане вербовки боевиков из реестра иностранных боевиков-террористов, прошедших специальный отбор и подготовку для проведения таких террористических актов. Эти лица могут быть знакомы друг с другом на протяжении целого ряда лет, могли содержаться в одной и той же тюрьме, могли вместе побывать в Сирийской Арабской Республике, возможно, говорят на одном и том же языке и/или являются выходцами из одной и той же страны или общины. Это позволяет обеспечить согласованность их действий и повышает их шансы на успех.

Изощренный характер многих терактов, совершенных в последнее время, позволяет предположить, что боевики ИГИЛ адаптируются к принимаемым по отношению к ним правоохранительным мерам и мерам безопасности. В этих условиях судебные, правоохранительные органы и службы безопасности часто оказываются в невыгодном положении в тех случаях, когда речь идет о террористах, которые действуют в одиночку или которых сложнее распознать

как террористов. Это в первую очередь касается правоохранительных органов и разведывательных служб, работающих на основе агентурного сбора информации. Опыт показывает, что даже если в период, предшествующий большинству терактов, совершаемых террористами-одиночками, есть люди, которые знают о том, что человек, который впоследствии и окажется преступником, испытывает недовольство, исповедует экстремистскую идеологию, взгляды и готов участвовать в насилии, они, как правило, не информируют об этом соответствующие органы. Это ограничивает возможности выявить потенциального преступника или заблаговременно получить информацию о возможном теракте.

Возвращенцы

Угроза, создаваемая иностранными боевиками-террористами, возвращающимися после боевых действий в Ираке, Сирийской Арабской Республике и других зонах конфликта, в которых они участвовали на стороне ИГИЛ, является еще одной серьезной проблемой для многих стран их происхождения. В целом, функции возвращенцев состоят в том, чтобы расширить присутствие ИГИЛ, охватив новые государства, и создавать сети в целях совершения в будущем террористических актов, осуществления планирования и мер по оказанию содействия. В настоящее время не ясно, сколько иностранных боевиков-террористов из рядов ИГИЛ скорее вернутся на родину, чем останутся в зонах конфликта или направятся в третьи страны, и какова вероятность того, что по возвращении они будут участвовать в террористической деятельности. При этом велика вероятность того, что по мере утраты своих иллюзий многие из них вернутся на родину. Однако, как показывает опыт, даже несмотря на то, что лишь очень немногие иностранные боевики-террористы, воевавшие в рядах ИГИЛ, после возвращения домой занимаются террористической деятельностью, вероятность успешной организации специально подготовленными иностранными боевиками-террористами терактов с большим числом жертв более высока. Следует также отметить, что возвращенцы могут оказаться ценным источником информации и могут убеждать других не заниматься террористической деятельностью, ссылаясь в этом отношении на собственный опыт и организуя в этих целях активные кампании по контрпропаганде.

Часть III
Мафия и миграционный кризис

Миграционные потоки в ЕС[29]

Последние годы в Европе наблюдается беспрецедентный рост числа нелегальных мигрантов. С 2013 по 2015 г. миграционные потоки растут по экспоненте, и нет оснований полагать, что объемы и темпы нелегального антропотока (потока людей) в ЕС уменьшатся в 2016 и последующих годах. В 2015 г. более одного миллиона нелегальных мигрантов смогло проникнуть на территорию ЕС. Подобное развитие событий оказало глубокое влияние на криминальный ландшафт Европы, наложило дополнительное бремя на бюджеты стран-членов ЕС, создало политическую напряженность и вызвало целый ряд других неблагоприятных последствий.

Европейские криминальные сети стремительно адаптировались к нелегальным антропотокам и сделали их заметным источником увеличения своих доходов и фактором усиления воздействия на политику, бизнес и общество. Есть основания полагать, что криминальные сети, действуя через свои ближневосточные филиалы и партнеров, частично спровоцировали рост миграции благодаря целенаправленной работе информаторов и агитаторов в лагерях беженцев.

Более 90 % мигрантов, стремящихся в страны ЕС, в той или иной степени пользуются услугами криминальных сетей. Эти услуги, в первую очередь, нелегальным упрощением процедур и незаконным получением прав на проживание в странах ЕС. Значительное число криминальных сетей и групп, получают значительные и все возрастающие объемы прибыли, связанные с антропотоком. Сложилась целая индустрия обслуживания нелегального антропотока, а также использования мигрантов как мулов для перевозки наркотиков, оружия и т. п.

Криминальные сети эксплуатируют отчаяние и уязвимость мигрантов. Они предлагают широкий спектр услуг по упрощению процедур, включая оказание транспортных услуг, предоставление пунктов и лагерей размещения на маршруте от места высадки в Европе до страны назначения, изготовление поддельных документов, предоставление через коррумпированных чиновников в странах размещения документов, проживание и даже гражданство.

Во многих случаях нелегальные мигранты, не имеющие достаточных денежных средств, вынуждены платить за эти услуги предоставлением себя в качестве нелегальной рабочей силы, согласием на участие в преступных группах, контролируемых криминальными сетями, передачу детей в сексуальную индустрию, контролируемую преступностью, а также для съемок видеопродукции педофильского характера и содержащих кадры жестокого обращения с детьми.

Денежные и обменные доходы европейского криминала от нелегального антропотока имеют тенденцию к стабильному увеличению. Только в 2015 г. преступные сети, участвующие в незаконном ввозе мигрантов, и обслуживании антропотоков, имели оборот от 3 до 6 млрд. Евро. По оценкам Европола, уже в 2016 г. эти цифры удвоятся или утроятся за счет налаживания кооперации различных преступных сетей, их функциональной специализации, а также завершения формирования рынков, связанных с монетизацией, работорговлей, проституцией, продажей видеоконтента педофильского и иного криминального характера и других видов натуральной оплаты мигрантами за оказываемые им нелегальные услуги.

Не будет преувеличением сказать, что незаконный ввоз мигрантов в страны-члены ЕС, а также преступные услуги и промыслы, связанные с использованием антропотоков в крими-

[29] Доклад Европола. 22 февраля 2016 г. (Извлечение). Migrant Smuggling in The EV. Europol report, 22 February 2016.

нальных целях, являются наиболее быстрорастущим сегментом организованной преступности в Европе. Дополнительные сложности порождает наметившееся в 2015 г. сращивание криминального обслуживания антропотоков с традиционными контрабандными сетями, генерирующими огромные прибыли за счет наркотрафика, нелегальной торговли оружием, сигаретами, алкоголем и т. п.

В криминальных услугах незаконным мигрантам задействованы транснациональные криминальные сети, руководство и основную часть которых составляют лица различных **исламских конфессий**. Значительную роль в обслуживании антропотока играет **албаноязычная организованная преступность**, наиболее влиятельная в балканском регионе, а также широко представленная в центрально-европейских странах, прежде всего Австрии, Германии, а также в Скандинавских странах.

Также замечено активное участие трансевропейских преступных группировок с большим представительством выходцев их криминальных сетей Италии, имеющих длительную историю. Наращивают свое представительство в этом сегменте преступности криминальные группировки, имеющие корни в Румынии и других странах Восточной Европы. В подавляющем большинстве – это не новые преступные группировки, а криминальные сети, начавшие действовать в восточноевропейских странах еще в 90-е годы, до их вступления в ЕС.

По итогам 2015 г. и первых недель 2016 г. основная масса нелегальных мигрантов в Европе приходится на жителей Сирии, Пакистана, Афганистана и Ирака. Они составляют основную часть нелегальных мигрантов. Однако сводить проблему исключительно к ближне- и средневосточному кризису было бы неверным. С 2012 г. стабильно увеличивается численность нелегальных мигрантов из Сенегала, Сомали, Нигера, Марокко, Ливии и других африканских стран.

По оценкам специалистов, вероятное в ближайшие годы циклическое сокращение количества осадков и вызванные этим температурные рекорды, сопровождающиеся засухами, исчерпанием водных ресурсов оазисов и т. п., могут активизировать незаконную миграцию из Африки примерно в таких же масштабах как с Ближнего и Среднего Востока.

Не следует забывать о продолжающейся миграции из таких стран как Индия, Бангладеш, Китай и Вьетнам. В своей подавляющей части мигранты из этих стран имеют первичное разрешение на въезд в страны-члены ЕС, и становятся нелегальными мигрантами после завершения срока действия соответствующих документов, связанных, как правило, с посещением родственников и т. п.

Наиболее предпочтительными для мигрантов странами, на которые в настоящее время выпадает максимальная нагрузка нелегального антропотока, являются Германия, Швеция и Великобритания. Такие страны, как Австрия, Венгрия и т. п. являются в основном транзитными пунктами на пути к трем указанным странам. Следует иметь также в виду, что реальные масштабы нелегальной миграции в Великобританию и Францию на порядки выше официальных цифр. Это связано с тем, что в соответствии с законодательством Великобритании и Франции, в этих странах могут проживать и работать граждане стран, ранее входивших в их колониальные империи. В Африке действует огромный рынок производства поддельных документов, которыми оснащаются не только жители африканских, но и ближневосточных стран, стремящиеся попасть и закрепиться во Франции и Великобритании.

Преступные сети предлагают широкий спектр весьма дорогих услуг для нелегального антропотока. Традиционный набор услуг, аванс за который как правило оплачивается еще на территории стран пребывания нелегальных мигрантов, включает в себя предоставление транспорта, размещение на всем протяжении маршрута, обеспечение поддельными документами и предоставление защиты от других преступных группировок, действующих в рамках антропотока.

Главным логистическим маршрутом нелегальной миграции в Европу является морской маршрут через Эгейское и Средиземное моря с высадкой в Греции или для африканских мигрантов – в Италии. На Грецию в 2015 г. пришлось более 80 % нелегальных мигрантов в Европу с Ближнего и Среднего Востока. В Греции нелегальный антропоток разделяется на две ветви маршрута. Наиболее популярным является транзит через западные Балканы, включая Македонию, Сербию, Косово, Боснию с пересечением границ стран-членов ЕС в Хорватии. Второй, менее популярный, маршрут предполагает транзит через Венгрию.

В конце 2015 г. появился новый маршрут с Ближнего Востока в Европу. Он предполагает переброску беженцев на автобусах через Турцию в черноморские турецкие порты с достижением Европы через Болгарию и Румынию.

Для африканских беженцев абсолютно преобладающим является маршрут через Италию, которая занимает второе после Хорватии-Венгрии место в ЕС по транзиту нелегальных мигрантов. С конца 2015 г. было замечено увеличение восточноевропейского миграционного потока. Это направление миграции, которое пока носит незначительный характер, представляет собой движение с юго-востока Европы, в основном из Румынии, в Польшу с последующей перевозкой нелегальных мигрантов в Швецию и Данию.

Принципиально новым способом транспортировки мигрантов является их перевозка воздухом. Этот вариант логистики доступен только для относительно состоятельных нелегальных мигрантов. Они предварительно доставляются морем в одну из североафриканских стран, преимущественно Египет, Тунис и Марокко. Из этих стран, в том числе с использованием не только гражданской, но и грузовой, авиации, мигранты транспортируются в страны назначения. Случаи доставки групп незаконных мигрантов по воздуху были зафиксированы правоохранительными органами Великобритании, Германии, Франции, Бельгии, Нидерландов, Дании и Швеции.

Горячие точки незаконного ввоза – транспортные хабы – нелегальных мигрантов в Европу совпадают с основными сетями контрабандной логистики. Эти горячие точки локализованы в районах крупных портов, контролируемых криминалом или узлов транспортной инфраструктуры, где организованные преступные группировки длительное время ведут незаконную деятельность.

В настоящее время Европолом выявлены более 230 пунктов, в которых собираются группы нелегальных мигрантов, вливающиеся в антропотоки. В этих пунктах предоставляются пакетные услуги, оплачиваются авансы и определяются натуральные способы оплаты за доставку мигрантов из пункта отправки в пункт прибытия в Европу. Согласно данным ЕВРОПОЛА, основные места локации преступных групп, связанных с нелегальным антропотоком за пределами ЕС являются Амман, Алжир, Бейрут, Бенгази, Каир, Касабланка, Стамбул, Измир, Искендерум, Мисурата, Мерсин, Оран и Триполи.

Преступный контроль и логистика нелегальных антропотоков, а также оперативные штабы и штаб-квартиры преступных сетей, задействованных в этом криминальном бизнесе, внутри ЕС расположены в Афинах, Берлине, Будапеште, Кале, Копенгагене, Франкфурте, Гамбурге, Хук ван Холланде, Лондоне, Мадриде, Милане, Мюнхене, Париже, Пассау, Риме, Стокгольме, Турине, Салониках, Вене, Варшаве и Зеебрюгге. Количество горячих точек и мощность нелегальных финансовых потоков между ними растут в последние годы в геометрической прогрессии. Их питает экспоненциально растущий антропоток.

Мигранты собираются исходно в транспортных хабах – концентраторах, о местоположении которых им заранее сообщается в лагерях беженцев в странах исхода. Как правило, еще до погрузки на морской транспорт, в неевропейских хабах – концентраторах, как правило, крупных городах-портах, мигранты нарушают законы. В период пребывания они участвуют в местных преступных группировках, а также нанимаются на криминальные предприятиях для того, чтобы оплатить свои долги, связанные с перемещением в Европу.

Горячие точки в рамках преступной логистической инфраструктуры выполняют не только функцию концентраторов, но и распределителей и расчетных центров. Именно в этих точках незаконные мигранты получают пакетные услуги, а также принимают на себя обязательства по оплате, либо предоставлению ответных услуг для преступных синдикатов и криминальных сетей.

В настоящее время Европол имеет досье на более чем 40 тыс. лиц, подозреваемых в причастности к незаконному ввозу мигрантов и обслуживанию их антропотока. Только в 2015 г. были открыты досье на более чем 10 тыс. подозреваемых. Кроме того, ЕВРОПОЛ располагает данными на почти 100 сетей и группировок, контролирующих европейский преступный бизнес, связанный с обслуживанием антропотоков. Согласно данным Европола, так или иначе в криминальный бизнес, связанный с нелегальным антропотоком в Европу вовлечены граждане более чем 100 стран. Наибольшее представительство в досье Европола имеют граждане Болгарии, Венгрии, Египта, Ирака, Косово, Пакистана, Польши, Румынии, Сербии, Сирии, Туниса и Турции.

44 % сетей состоят исключительно из граждан стран, не являющихся членами ЕС. 30 % – включают только граждан стран-членов ЕС, и 26 % – объединяют преступников – граждан стран-членов ЕС и криминал из других стран мира. В то же время именно на последнюю четверть сетей приходится, по разным оценкам, от 60 до 80 % всего объема криминального бизнеса, связанного с нелегальным антропотоком. Исключение составляют только скандинавские страны, где весь бизнес, связанный с антропотоком находится в руках граждан этих стран.

Большинство групп подозреваемых имеют достаточно однородный состав. Например, основные преступные группы в Венгрии и Швеции этнически однородны. При этом преступники – граждане Швеции и Венгрии организуют и контролируют бизнес, как в странах прибытия, так и в транзитных странах и даже странах исхода. Это же характерно и для болгарских, румынских и польских сетей.

Приведенные факты заставляют высказать гипотезу, что этническая принадлежность и гражданство в данном случае значительно различаются. Согласно оперативной информации в лагерях беженцев, а также в логистических узлах вне Европы, не замечены венгро-, шведско-, румыно- или польско-говорящие группировки. Граждане других стран, в первую очередь Албании, Косово, ряда центральноевропейских стран и т. п. активно **используют паспорта восточноевропейских стран – членов ЕС.**

Частично также данная ситуация объясняется тем, что восточноевропейские паспорта активно используются криминальными группировками для обеспечения проникновения нелегального антропотока в страны-члены ЕС. Как известно, в соответствии с резолюцией Совета Безопасности ООН № 1244 по Косово, наличие балканского паспорта облегчает возможность нелегальным мигрантам проникнуть на территорию стран-членов ЕС и получить там если не гражданство, то статус беженцев и право на пособие.

Структуры преступных сетей, обслуживающих нелегальные антропотоки, весьма разнообразны и находятся в процессе постоянного изменения. При всем многообразии этих структур можно сделать вывод, что наиболее успешные по состоянию на 2016 г. имеют однородную этническую верхушку. Многие из сетей однородны не этнически, а конфессионально. Лидерами некоторых раскрытых преступных групп являются представители одного и того же течения ислама. Для европейских преступных группировок, действующих в нелегальных антропотоках, за исключением лиц албанской национальности, свойственны большее разнообразие и разнородность руководства.

Преступные сети, имея штаб-квартиру как правило в одной из стран-членов ЕС, обязательно располагают подразделениями в основных точках инфраструктуры нелегального антропотока. При этом, исследования показывают наличие географической локализации по функционалу обслуживания. Ведущие криминальные сети берут на себя функции координации

отдельных узлов инфраструктуры, обеспечения документами и другими услугами, а также получают и обеспечивают основные финансовые потоки.

В то же время, в отличие от более раннего периода, криминальные структуры со штаб-квартирами в странах-членах ЕС, не стремятся брать на себя функции вне территории ЕС, а тем более вне Европы. Причем не только в лагерях беженцев, но и в транспортных хабах-концентраторах.

В течение последних месяцев 2015 г. ведущие группировки перешли на иерархический принцип, где каждый нижестоящий уровень выполняет работу на субподряде у вышестоящего. Так, местные лидеры, контролирующие транспортные хабы, не только выполняют функции субподряда для трансевропейских сетей, но и самостоятельно, с согласия европейских лидеров, обеспечивают безопасность доставки нелегальных мигрантов из районов их проживания к месту транспортировки. Они же отвечают за доставку мигрантов, вплоть до побережья Европы.

В свою очередь их партнеры на нижнем, местном уровне осуществляют первичный отбор нелегальных мигрантов, которые способны оплатить доставку в Европу, вплоть до страны назначения или способны оказать услуги, достаточные для натуральной оплаты маршрута. Именно этот нижний уровень осуществляет доставку, а соответственно получает оплату за транспортировку мигрантов, от места их проживания до транспортного хаба.

В настоящее время на основе обобщения различных данных Европол может представить **типологию лиц, обеспечивающих поставку мигрантов криминальным сетям**. В их число входят оценщики, сборщики оплаты, владельцы, арендаторы и водители транспортных средств, охранные команды, специалисты по работе с местными чиновниками, персонал временных лагерей пребывания, а также менеджеры по логистике и координации.

Организованная европейская преступность постоянно совершенствует свои организационные модели. Отдавая себе отчет, что правоохранительные органы стараются распознать сети и для этого вербуют нелегальных мигрантов в качестве агентов, а также широко используют работу под прикрытием, криминал в последние месяцы стал переходить от постоянных иерархических схем к **гибким адаптивным модульным структурам**. В рамках этих структур можно выделить три уровня.

– Первый – это постоянная штаб-квартира, занимающаяся бизнесом, связанным с размещением, укоренением и использованием мигрантов на территории стран-членов ЕС, а также определением критериев платежеспособности или полезности с точки зрения натуральной оплаты. Штаб-квартиры также имеют контрольно-информационные подразделения в хабах-концентраторах за пределами ЕС и иногда непосредственно в лагерях беженцев и местах отправки в странах исхода.

– Второй уровень составляют преступные группировки, обеспечивающие европейский транзит мигрантов до границ стран ЕС. Эти же группировки, как правило, устанавливают связи со стабильными организованными группами, действующими в хабах-концентраторах вне ЕС. Взаимоотношения между штаб-квартирой и региональными преступными группировками строятся отчасти на подчинении и контроле, отчасти на договорной основе. При этом можно предположить, что штаб-квартиры будут стремиться время от времени обменивать или менять своих локальных партнеров, чтобы повысить гибкость и не допустить раскрытие сетей правоохранительными органами.

– Наконец, третий уровень составляют преступные группировки, работающие вне ЕС, как в хабах-концентраторах, так и на низовом уровне. Поскольку большинство хабов-концентраторов вне Европы расположены либо в несостоявшихся государствах, либо в странах с авторитарным характером правления, для которых свойственно сращивание политики и бизнеса, то здесь действуют другие, нежели в ЕС, законы. Как правило, каждый хаб-концентратор контролируют одна, две, в исключительных случаях более преступных сетей, которые имеют агентские команды на самом низовом уровне – в местах сборки ручейков антропотока.

Ряд исследователей в течение 2015 г. высказали гипотезу о том, что данная модульность является лишь прикрытием и на самом деле антропоток контролируют несколько глубоко законспирированных транснациональных преступных группировок. Остальные же группы, допущены в этот бизнес частично для создания массовости, а частично в целях маскировки. Если в ходе дальнейших исследований будут найдены аргументы в пользу данной позиции, то предстоит задуматься о **возможности сращивания этих лидирующих преступных группировок с государственной властью различных уровней**, как в странах ЕС, так и особенно за его пределами.

Сложность сетей определяется набором преступных бизнесов, реализуемых на антропотоке, длиной и неоднородностью логистики, а также особенностями легализации незаконных мигрантов в странах ЕС. В зависимости от выбранного типа логистики, хаба-концентратора и страны назначения формируются различные типы связей как внутри преступных группировок, так и между ними. Логистика, юридические процедуры и виды бизнеса определяют типологию криминальных сетей. Практически во всех случаях эти сети предполагают наличие постоянного компонента, в качестве которого выступают, как правило, этнически или религиозно однородные на уровне высшего руководства группировки по всему ЕС.

Последнее чрезвычайно важно по той причине, что именно конфессиональная, реже этническая однородность обеспечивает успех в решении ключевой задачи – укоренении нелегального мигранта в той или иной стране пребывания и его немедленное и постоянное использование в рамках криминальной экономики. Религиозные и этнические диаспоры в странах-членах ЕС пронизаны криминальными группировками. Именно диаспоры помогают мигрантам с соответствующими религиозными верованиями или этнической принадлежностью укорениться в стране назначения и осуществить первичную социализацию.

Следует особо отметить, если в XX веке мигранты из стран вне ЕС хотя и старались создать этнические общины и диаспоры компактного проживания в той или иной стране, тем не менее, они активно шли на социализацию и стремились превратить детей в полноправных граждан соответствующей страны, как правило, с ослабленной привязкой к диаспоре. С подъемом исламского фундаментализма ситуация претерпела изменения, особенно для выходцев с Балкан, Северной Африки, Ближнего и Среднего Востока. **Этнические общины стараются сохранить свою не только религиозную, но и социальную однородность, формируя замкнутые, компактно проживающие диаспоры внутри европейских гражданских обществ**.

Члены диаспор – **участники криминальных сетей, являются ключевыми лицами в организации размещения в стране пребывания мигрантов**, обеспечения их работой на черном рынке труда и вовлечении в криминальную деятельность. Средний возраст участников криминальных сетей, специализирующихся на антропотоке, арестованных в 2015 г., составляет 36 лет. При этом возраст лиц, арестованных на территории стран ЕС в рамках борьбы с криминальными группировками, связанными с нелегальной миграцией из числа граждан Сирии, Пакистана и Ирака значительно меньше возраста их подельников с западных Балкан и других государств-членов ЕС.

Среди преступных группировок из числа населения стран ЕС самый молодой возраст у румынских преступников. Они, как правило, не являются руководителями сетей, а выполняют обслуживающие функции, связанные с автомобильной транспортировкой и изготовлением поддельных документов. Иракские, сирийские и афганские арестованные лица практически полностью являются членами преступных группировок вне ЕС, базирующихся на хабах-концентраторах. Они задерживаются в Европе в рамках миссий сопровождения нелегальных мигрантов и при координационных встречах с представителями европейских штаб-квартир.

В ходе арестов удалось установить примерную цену полного пакета транспортировки мигрантов с Ближнего Востока в Грецию и из Северной Африки в Италию. Полный пакет,

включающий доставку из ливийских портов в Италию, оснащение документами и обеспечение приема нелегального мигранта в Италии с размещением в лагере беженцев составляет для взрослых примерно 1000 Евро, а для трех детей – 500 Евро. Таким образом, переброска средней семьи дает преступниками 2500 Евро. Приведенные выше цены не включают в себя оплату признания беженца и его семьи в качестве лиц, имеющих право на получение пособий и возможно предоставление временной работы.

Новым явлением 2015 г. стало использование социальных медиа, шифрованных мессенджеров и даже dark net не только для коммуникаций и обмена информацией между преступными группами, но и в качестве пространства для переговоров с потенциальными беженцами. Понятно, что последнее обстоятельство характерно не для массы нелегальных мигрантов, а лишь для образованной молодежи. Она, хотя и составляет абсолютное меньшинство в антропотоке, по доле в общем количестве мигрантов имеет тенденцию увеличения от месяца к месяцу.

Необходимо отметить, что **криминальные сети, как показали полицейские операции в различных странах-членах ЕС, обязательно имеют IT группу**. Они осуществляют не только информационную поддержку криминального бизнеса, но и ведут целенаправленный поиск информации об активности правоохранительных органов и изменении законодательства стран-членов ЕС. Отмечено, что преступники подчас опережающим образом реагируют в рамках модели ценообразования на ужесточение пограничного контроля или изменение режима транзита в Европе.

В 2015 г. имела место тенденция сращивания преступных сетей, связанных с нелегальным антропотоком, с группировками, специализирующимися на незаконном обороте наркотиков и оружия, проституции, торговле людьми и нелегальном обороте органами для имплантации. Есть основания полагать, что уже в 2016 г. сращивание сменится слиянием преступных сетей и завершится их превращением в многоотраслевые преступные организации.

В 2015 г. криминальные сети, работающие с антропотоком, в 22 % случаев занимались и наркотрафиком, в 20 % – работорговлей и преступностью, связанной с правами собственности, в 18 % – с незаконным оборотом наркотиков. Согласно имеющимся сведениям в 2016 г. корреляция преступности на антропотоке с другими видами тяжелых преступлений увеличится как минимум до 30 %.

Практически теми же темпами как нелегальные антропотоки, в ЕС растет **преступный бизнес, связанный с подделкой документов**. Согласно анализу, наибольшее количество фальшивых документов, используемых нелегальными мигрантами в страны-члены ЕС, изготавливаются в Афинах, Стамбуле, городах Сирии, в Бейруте, а также в азиатских центрах, прежде всего, в городах Таиланда. Лишь меньшая часть мигрантов получает документы в начальном пункте антропотока. Основная часть получает временные проездные документы на каждом определенном этапе транзита из страны пребывания в страну назначения.

В прошлом году была раскрыта крупнейшая в ЕС типография по печати высококачественных европейских поддельных документов, расположенная в Албании. Оборудование лаборатории стоило несколько миллионов Евро. Подпольная типография изготавливала фальшивые документы по запросам посредников, представлявших криминальные сети по всей Европе. Фактически она работала для них по модели аутсорсинга.

Оплата типографских услуг производилась по PayPal и Western Union. Пакеты документов отправлялись из Албании в Турцию, Грецию, Ливию, Сирию, Ливан посредством мелких посылок и курьеров. Максимальное взаимодействие албанской типографии осуществлялось с преступниками, локализованным в таких странах, как Греция, Болгария и Турция. В ходе обыска в типографии были изъяты несколько тысяч пустых бланков визовых документов, видов на жительство, паспортов и даже водительских удостоверений.

В 2015 г. 55 % нелегальных мигрантов, пребывающих в ЕС, составляли женщины и несовершеннолетние дети. В течение 2015 г. на треть увеличилось число несовершеннолетних,

пребывающих в ЕС без сопровождения. Это противоречит норме ЕС об обязательности наличия ответственного взрослого при детских поездках или заверенного консульствами в стране отбытия и одной их стран ЕС заявления обоих родителей о возможности путешествия несовершеннолетнего без сопровождения.

В прошлом году в три раза увеличилась численность несовершеннолетних, обратившихся в органы ЕС с просьбой предоставить убежище. Примерно 50 % несовершеннолетних без сопровождения взрослых были афганские граждане, и лишь 13 % имели сирийское гражданство. В прошлом году в странах-членах ЕС **в несколько раз выросло число исчезновений несовершеннолетних из убежищ или центров приема**.

Правоохранительным органам нескольких стран-членов ЕС, сотрудничающих с ЕВРОПОЛОМ, удалось в 2015 г. парализовать действия пакистанской преступной сети в Европе, которая занималась целевой незаконной миграцией в страны ЕС под заказ конкретных работодателей. Страной размещения пакистанских мигрантов была в течение нескольких лет Испания, где пакистанская рабочая сила использовалась в строительстве и как подсобные рабочие в магазинах и ресторанах.

Некоторая часть нелегальных мигрантов из числа молодых женщин вовлекается криминальными сетями в **проституцию**. Несмотря на то, что статистика по данному направлению в настоящее время отсутствует, по косвенным признакам можно сделать вывод, что речь идет о вовлечении в проституцию десятков тысяч девушек. Например, в таких странах массового размещения мигрантов, как Германия, Австрия, Великобритания, Франция, Швеция и Бельгия на камерах слежения, установленных в злачных районах, на порядки выросло количество девушек ближневосточного и североафриканского типа. Также заметно, во многих городах – на треть и более, упали цены на соответствующие услуги. Это свидетельствует об избытке предложения над спросом.

Существование и нарастание столь мощного нелегального антропотока в страны-члены ЕС стало возможным только при наличии **высокого уровня коррупции как в странах проживания мигрантов, транзитных странах и в странах конечного размещения**. Согласно полицейским данным, наиболее подвержены коррупции, связанной с нелегальным антропотоком в странах-членах ЕС, сотрудники правоохранительных органов, а также работники миграционных служб. В 2015 г. выявлены случаи и пресечена коррупция должностных лиц в военно-морских и сухопутных войсках европейских стран, через которые в Европу прибывают незаконные мигранты. К сожалению, выявлены множественные случаи коррупции среднего и технического персонала консульств и посольств стран-членов ЕС, через которые в руки преступников попадают пустые бланки паспортов, визовых документов и т. п.

Огромный незаконный миграционный поток обеспечил **проникновение в страны-члены ЕС потенциальных террористов** и позволил развернуть на континенте спящие ячейки ИГИЛ и Аль-Каиды. Есть также опасение, что незаконный ввоз мигрантов стал заметным источником финансирования для террористических организаций.

В 2015 г. правоохранительные органы стран-членов ЕС выявили несколько случаев использования миграционных потоков субъектами терроризма. Большинство их этих случаев связано с использованием террористическими сетями сирийских граждан или граждан других стран Ближнего Востока и Северной Африки. Так двое из подозреваемых в Парижских терактах 13 ноября 2015 г. проникли в Европу как незаконные мигранты.

Десятками исчисляются случаи возвращения членов террористических групп ИГИЛ и Аль-Каида, имеющих гражданство ЕС, в массе нелегальных беженцев. Иностранные боевики пребывают в районы расположения террористов обычным легальным порядком, а возвращаются незаметно от правоохранительных органов, растворяясь в потоке мигрантов, часто меняя подлинные документы на поддельные для пересечения границ стран-членов ЕС.

В 2015 г. в целом ряде стран, и прежде всего, в Германии, отмечались случаи актов массового насилия нелегальных мигрантов в отношении гражданского населения. Соответственно **значительно увеличилось и число насильственных нападений на мигрантов во временных лагерях и других местах размещения**. В 12 из 15 стран-участниц ЕВРОПОЛА были зафиксированы такого рода нападения. Случаи поджога центров для мигрантов зарегистрированы в Австрии, Болгарии, Германии, Дании, Финляндии, Швеции, Франции, Греции и Нидерландах, а также в Польше и Великобритании. В подавляющем большинстве случаев прямые нападения, поджоги и пикеты вокруг центров были организованы правыми и левыми экстремистскими группировками и закончились прямыми столкновениями с полицией.

Незаконные антропотоки позволили преступникам создать прибыльный бизнес, через который проходят огромные финансовые средства. Грубая оценка годового оборота этого бизнеса получена путем умножения приблизительного количества мигрантов, достигших ЕС, на стоимость среднего пакета услуг, предоставляемых незаконным мигрантам. Рассчитанный таким образом объем преступного бизнеса составил в 2015 г. по минимум 3 млрд., по среднему уровню – 6 млрд. евро.

По имеющимся данным, значительно возросло число случаев использования малолетних мигрантов для сексуальной эксплуатации и других видов преступлений, связанных с педофилией, а также изготовлением интернет-контента. Ожидается, что в ближайшие годы масштабы этого вида преступности увеличатся на порядки, если на законодательном уровне не будет резко ужесточено наказание не только за привлечение к сексуальной эксплуатации, но и за участие в этой деятельности в качестве пользователя или потребителя видеоконтента.

EMSC (Европейский центр борьбы с нелегальной миграцией) совместно со структурами ЕВРОПОЛА полагают, что в ближайшие годы странам-членам ЕС предстоит заметно ужесточить и унифицировать национальные законодательства в целях недопущения различного уровня жесткости миграционных законодательств стран-членов ЕС. В условиях отмены государственных границ между странами-членами ЕС, отсутствие таких решений и их неукоснительного исполнения уже в ближайшие годы может поставить под угрозу свободное пространство передвижения людей и транспорта в рамках ЕС. Это может стимулировать введение внутренних пограничных процедур, что будет иметь трудно предсказуемые последствия для политической и экономической структуры Евросоюза.

В ближайшие годы страны ЕС без сомнения будут испытывать усиливающееся демографическое давление извне. Этому будут способствовать три независимых группы факторов. Продолжаются и не имеют тенденции к снижению вооруженные конфликты на Ближнем и Среднем Востоке. Возрастают геоклиматические риски для большей части африканского континента. В условиях предстоящего в ближайшие годы всеобщего проникновения интернета даже в самые отсталые районы, все большая доля населения бедных стран, особенно расположенных в зонах конфликтов, сможет воочию увидеть жизнь в Европе. Все эти факторы, без сомнения, подтолкнут межматериковую миграцию.

Организованная преступность и мигранты[30]

Нерегулярная миграция в Европу облегчается и даже стимулируется действиями сетей по переправке мигрантов. Численность мигрантов, прибывших в Европу в результате этих действий, резко выросла в последние годы. Считается, что в настоящее время организованные преступные группы получают больше денег от переправки мигрантов, чем от более традиционной контрабанды – то есть контрабанды оружия и наркотиков, а численность переправщиков, связанных с доставкой мигрантов в Европу, измеряется десятками тысяч человек, которые образуют более или менее структурированные сети со связями по всему континенту и за его пределами, т. е. со странами происхождения и транзита.

Кроме того, переправка мигрантов сопровождается многочисленными вспомогательными видами незаконной деятельности, включая подделку документов, подкуп должностных лиц с целью получения документов, недекларирование водителями грузовиков спрятанных пассажиров при пересечении границ, подкуп сотрудников пограничной и береговой охраны. Группы по переправке мигрантов могут заниматься и сопутствующими видами деятельности, такими как торговля людьми, незаконный оборот наркотиков и отмывание денег. Они и другие организованные преступные группировки также вовлечены, например, в эксплуатацию труда нерегулярных мигрантов и коррупцию, связанную с национальными системами предоставления убежища.

Несмотря на наличие различных международных документов и механизмов, а также усилия национальных властей, на фоне масштабов переправки мигрантов в Европу в последнее время поражает, насколько трудным оказалось обеспечить юридическое преследование и осуждение переправщиков мигрантов. Уже осуществляется сотрудничество между европейскими полицейскими службами, и согласованные действия по ликвидации международных сетей переправки позволили добиться определенных успехов, по крайней мере в том, что касается их европейских элементов. Однако это означает, что каналы переправки перекрываются лишь с одного конца, а учитывая характер этих каналов, не приходится говорить, что их можно перекрыть окончательно или даже нанести им серьезный ущерб на длительную перспективу.

4. Ассамблея приходит к выводу, что для эффективного противодействия организованным преступным группам, связанным с миграцией, исключительно важно наладить международное сотрудничество и обмен оперативной информацией с привлечением максимально широкого круга специалистов и ресурсов для выработки комплексных инновационных подходов. Эти подходы должны быть нацелены на все потенциально уязвимые участки бизнес-моделей этих групп, включая отмывание денег, коррумпирование государственных чиновников и злоупотребление Интернетом. Следует поставить цель использовать все возможные средства для превращения переправки мигрантов и различных зачастую связанных с ней преступлений, из неопасных высокодоходных видов деятельности в деятельность рискованную и не приносящую больших доходов…

7. Ассамблея полагает, что усилия по борьбе с переправкой мигрантов должны быть направлены на ликвидацию глубинных причин вынужденной миграции, которая толкает мигрантов в руки переправщиков. Для того чтобы сократить практику обращения к переправщикам мигрантов, следует разработать адекватные и эффективные программы расселения беженцев, а также организовать безопасные законные каналы миграции.

8. Ассамблея рекомендует государствам-членам: …8.6. разработать и эффективно применять в отношении переправщиков мигрантов широкий спектр следственных методов и методов судебного преследования, включая, в частности:

[30] Парламентская ассамблея Совета Европы. Резолюция 2089. 27 января 2016 года. (Извлечение)

• более эффективное задействование систем обмена оперативной и иной информацией с привлечением как других государств-членов, так и международных организаций;

• более эффективное использование существующих платформ обмена информацией (таких как, Европейское агентство по организации оперативного сотрудничества на внешних границах государств-членов Европейского союза (Frontex) и Европейская система наблюдения за внешними границами (EUROSUR)) для сбора фактической информации о тенденциях, переправке, формах работы, маршрутах и бизнес-моделях;

• повышение эффективности сотрудничества с третьими странами по вопросам сбора доказательных материалов и облегчения экстрадиции;

• обеспечение наделения компетентных органов полномочиями по аресту, конфискации и проведению судебной экспертизы средств, использовавшихся для преступной переправки;

• обеспечение защиты и помощи мигрантам, которые сотрудничают с властями в процессе судопроизводства, включая выдачу временных разрешений на жительство;

• широкое использование перехвата сообщений, в том числе международных, в соответствии с гарантиями, зафиксированными в Европейской конвенции о правах человека (СЕД № 5), как они интерпретируются в решениях Европейского суда по правам человека;

8.6.7. установление подсудности преступлений, совершенных в ходе переправки мигрантов на национальную территорию, даже если совершены они, по-видимому, за ее пределами…

Сети нелегальной миграции[31]

Вступление

Я рад представить этот доклад, подготовленный с использованием объединенных ресурсов Европола и Интерпола в помощь европейским и глобальным правоохранительным органам. Доклад содержит ситуационную оценку роли организованных преступных групп в миграционном кризисе.

Европа сталкивается с беспрецедентным числом нелегальных мигрантов, во все возрастающем количестве пребывающих в Европу, в том числе вследствие активности сложных и безжалостных криминальных сетей. Разведывательная информация, полученная Европолом, указывает на то, что более 90 % всех мигрантов, пересекающих границы Европейского Союза, делают это при помощи сетей организованной преступности.

Сети оказывают услуги по содействию нелегальной миграции как на протяжении всего маршрута, так и в отдельных его ключевых пунктах и отрезках. Вовлеченность организованной преступности в нелегальную массовую миграцию обусловлена, прежде всего, огромными объемами незаконной выгоды, получаемой от организации и обслуживания нелегального антропотока.

Европол находится на переднем крае борьбы с нелегальной миграцией и осуществляет поддержку правоохранительных органов государств-членов ЕС в борьбе с преступными сетями, которые эксплуатируют отчаявшихся мигрантов, стремящихся покинуть зоны вооруженных конфликтов, стихийных бедствий, районы, где их жизнь связана с бедностью, лишениями и преследованиями.

Сети нелегальной миграции являются гибкими, эластичными, быстро приспосабливаются к правоприменительным мерам и способны к мгновенному изменению маршрутов, используемых для незаконного проникновения мигрантов в ЕС. Эти маршруты постоянно диверсифицируются и изменяются. Более чем когда-либо прежде правоохранительные органы стремятся в режиме реального времени получать достоверную разведывательную информацию и обеспечивать ситуационную осведомленность. Решение этой задачи обеспечивается за счет эффективного обмена разведывательной информацией между государствами-членами ЕС при активном участии Европола.

Криминальные сети нелегальной миграции получают огромные преступные доходы от незаконного антропотока. Только в 2015 г. эти сети получили, по оценкам, 5–6 млрд. долларов дохода от своей незаконной активности, связанной с нелегальной миграцией. Эти доходы позволяют наращивать преступные сети, повышать эффективность их деятельности, что оказывает существенное негативное долговременное влияние на экономику Европы.

Нелегальная миграция является глобальным явлением. Однако Европа в настоящее время выступает главным регионом назначения для нелегальной миграции. Для того чтобы понять масштабы и структуру криминальных сетей, Европол и ИНТЕРПОЛ использовали свои уникальные возможности выявления методов, деятельности, маршрутов и организации преступных групп.

Европол смог внести свой вклад в этот доклад, опираясь на разведывательную информацию государств-членов ЕС и других партнеров, а также собственные данные Европейского центра нелегальной миграции (EMSC). Открытый в феврале 2016 г. EMSC представляет собой коллективный ответ правоохранительных органов государств-членов ЕС на возросшую актив-

[31] Объединенный доклад Европола и Интерпола. Май 2016 г. (Извлечение)

ность организованных преступных групп, задействованных в организации обслуживания нелегальной миграции в ЕС.

Роб Вайнврайт, Директор Европола

Интерпол

В последние годы беспрецедентного уровня достиг поток нелегальной миграции в Европейский Союз людей, изгнанных из родных земель нестабильностью, отсутствием безопасности и ужасающей бедностью. Эти трагические обстоятельства породили серьезный гуманитарный кризис и создали многочисленные возможности для транснациональных преступных сетей. Преступники готовы, они ждут миллионы мигрантов из Африки, Ближнего Востока и Азии, чтобы извлечь криминальную прибыль, эксплуатируя потребность людей в помощи и мечты о лучшей жизни.

Преступники обеспечивают незаконное пересечение морских и сухопутных границ, изготовление и предоставление поддельных проездных документов и удостоверений личности, создают сложности для правоохранительных органов в противодействии нелегальной миграции.

Для того чтобы эффективно демонтировать и ликвидировать криминальные сети, эксплуатирующие трагические жизненные обстоятельства отчаявшихся мужчин, женщин и детей, необходимо понимание широкого круга незаконных услуг и методов работы криминальных сетей. В связи с этим Европол и ИНТЕРПОЛ подготовили аналитический доклад о незаконном ввозе мигрантов преступными сетями на территорию ЕС. В докладе дано представление о деятельности, организационных структурах, операционных возможностях, ориентировочной прибыли и географически горячих точках, где работают преступные сети.

Юрген Сток, Генеральный Секретарь ИНТЕРПОЛА

Ключевые результаты

• Более 90 % мигрантов, пребывающих в ЕС, пользуются услугами преступных сетей. Ожидается, что в будущем эта доля еще более увеличится вследствие жестких правоприменительных мер, осуществляемых странами, по территории которых проходит антропоток нелегальной миграции.

• При том, что ключевые миграционные маршруты в течение последних полутора лет использовались как основные коридоры незаконного ввоза мигрантов, они обладают подвижностью и под влиянием таких внешних факторов, как жесткость пограничного контроля или изменение погодных условий, могут меняться. Так как преступники адаптируют свою деятельность к усилению контроля в ЕС, можно ожидать появления новых путей и дальнейшей диверсификации маршрутов. Соответственно появятся новые горячие точки, как в регионах отправки мигрантов, так и в местах высадки мигрантов на европейской территории.

• Преступники и посредники организованы в слабо связанные сети, вытянутые вдоль миграционных маршрутов. В ЕС и за его пределами идентифицированы более 250 точек, связанных с незаконным ввозом мигрантов в ЕС.

• Незаконный ввоз мигрантов представляет собой многонациональный бизнес, в котором участвуют граждане из более чем 100 стран мира, включая страны ЕС и иные государства.

• Базовая структура сетей включает в себя лидеров, которые координируют слабоструктурированные сети по всему маршруту, организаторов, управляющих деятельностью на местном уровне через личные контакты и агентов низового уровня.

• Незаконный ввоз мигрантов является весьма прибыльным бизнесом. Он характеризуется относительно низким уровнем затрат, все возрастающим спросом на преступные услуги и высокими расценками на предоставляемые комплексные или разовые услуги, связанные с нелегальной миграцией. Оценка годового оборота преступных сетей от нелегальной миграции составляет в 2015 г. в среднем от 5 до 6 млрд. долларов. Основным средством платежа остаются наличные.

• Данные разведки, собранные в последние месяцы, показывают стремительное сращивание бизнеса на нелегальной миграции с другими видами криминальной деятельности, в том числе связанными с тяжелыми преступлениями.

• Мигранты, направляющиеся в ЕС потенциально подвержены риску стать участниками незаконного рынка труда или подвергнуться сексуальной эксплуатации, чтобы оплатить преступникам транзит. Ожидается, что криминальные рынки труда и сексуальной эксплуатации значительно увеличатся в ближайшие годы.

• Террористы могут использовать ресурсы преступных сетей и незаконный антропоток для достижения собственных целей. Существует повышенный риск того, что боевики террористических сетей могут использовать миграционные потоки, чтобы проникнуть внутрь ЕС.

Введение

Исключительные масштабы нелегальной миграции в ЕС вызвали принятие беспрецедентных мер на международном уровне.

В 2015 г. Европол и ИНТЕРПОЛ сообщили о стремительном росте числа расследований, связанных с незаконным антропотоком. Также они столкнулись с взрывным ростом числа просьб об оказании оперативной поддержки государствам-членам по купированию последствий миграционного кризиса. Для того чтобы сформулировать адекватный ответ на этот беспрецедентный кризис европейские и международные правоохранительные органы нуждаются в гораздо более полном, чем раньше представлении о деятельности преступных сетей, обслуживающих нелегальную миграцию, действующих в Европе и по всему миру.

Целью данного доклада является повышение осведомленности и добавление новой информации к уже существующим данным по незаконному ввозу мигрантов. В связи с этим главное внимание уделено анализу преступных сетей с целью:

• определения структуры и стратегии сетей;

• анализа их финансовых активов и финансовых потоков, связанных с нелегальной миграцией;

• определения горячих точек, где сети являются наиболее активными;

• предоставления рекомендаций по ключевым оперативным действиям, а также создание дорожной карты повышения эффективности сотрудничества национальных, европейских и международных правоохранительных органов;

• обзора будущих рисков и угроз.

Маршруты нелегальной миграции и их горячие точки в 2015 г.

Европа стала свидетелем беспрецедентного увеличения числа нелегальных мигрантов, пребывающих в ЕС. В 2015 г. масштабы миграционных потоков достигли невиданных высот. Эта тенденция, как ожидается, продолжится в 2016 г. В настоящее время, по оценкам Европола, более 90 % мигрантов, пребывающих в ЕС, используют услуги, оказываемые преступными сетями.

В основном они связаны с транспортировкой и обеспечением размещения в стране пребывания. В большинстве случаев эти услуги предоставляются преступными группами. В этом

криминальном бизнесе участвует большое количество криминальных сетей, а также отдельных преступников. Они получают огромную и все возрастающую прибыль, связанную с нелегальным ввозом мигрантов.

Многие из маршрутов нелегальной миграции в ЕС, включая морские, сухопутные и воздушные, не являются новыми. В течение более 10 лет мигранты западной части Средиземноморья использовали маршрут через Испанию и Португалию. В 2015 г. в общей сложности 7,2 тыс. случаев незаконного пересечения границы, главным образом со стороны гвинейских, алжирских и марокканских граждан на иберийском маршруте. Мигранты, депортирующиеся из Ливии по морскому маршруту через Средиземное море, высаживаются в Италии. Подавляющую часть этих мигрантов составляют жители Магриба и стран Африки. Несмотря на то, что в 2015 г. число мигрантов на этом маршруте снизилось на 12 %, общая численность незаконных мигрантов, зарегистрированных пограничной службой, составила почти 154 тыс. человек.

Из Турции мигранты по юго-восточному маршруту прибывают в ЕС через Грецию или Болгарию морем, сушей или воздухом. Из-за трагических событий в Сирии драматически увеличилось число мигрантов по этому маршруту. Оно возросла в 2015 г. по сравнению с 2014 г. на 1612 %. На этом маршруте было официально зарегистрировано более 885 тыс. незаконных мигрантов. Юго-восточный маршрут через Балканы используется для незаконной миграции в страны Северной Европы.

В 2015 г. начал действовать восточный маршрут. Он предполагает достижение ЕС по внешней границе ЕС с Беларусью, Молдовой, Украиной и Россией. В 2015 г. официально было зарегистрировано на этом маршруте 1920 мигрантов, в основном из Афганистана, Вьетнама и Сирии. В 2015 г. впервые появился северный маршрут, когда мигранты используют Россию для того, чтобы войти в Шенгенскую зону через Норвегию или Финляндию. В 2015 г. более 2000 мигрантов использовали этот маршрут для достижения Шенгенской зоны.

Благоприятно расположенные вдоль маршрутов горячие точки, совпадающие с транспортными хабами, привлекают мигрантов и используются контрабандными сетями. В настоящее время выявлено около 250 таких горячих точек, в том числе 170 в ЕС, и 80 – за пределами ЕС.

Горячие точки располагаются в районах с развитой транспортной инфраструктурой, включая международные вокзалы, аэропорты, порты, точки технического обслуживания для междугородних автобусов и т. п. Наряду с транспортными хабами горячие точки возникают в районах со слабым контролем правоохранительных органов, а также в разрушенных или несостоявшихся государствах. Кроме того, горячие точки расположены в зонах пограничного контроля, особенно в тех местах, где криминальным сетям удалось коррумпировать пограничников, полицейские патрули и подразделения военно-морского флота. Горячие точки расположены также в местах расселения диаспор, сходных по этническому и национальному составу с незаконными мигрантами.

По всей вероятности, структура горячих точек в ближайшем будущем может претерпеть изменения. Наиболее крупные горячие точки, связанные с транспортными хабами, останутся неизменными. В то же время горячие точки, созданные криминальными сетями, за счет коррупции, а также особенностей пограничного контроля могут измениться в результате предпринимаемых правоохранительными органами мер.

Криминальные сети и инфраструктура

Преступные сети, организующие и обслуживающие незаконную миграцию, вытянуты вдоль миграционных маршрутов. Информация говорит о том, что лидерами преступных группировок являются в основном граждане стран, не входящих в ЕС, имеющих то же происхож-

дение или вероисповедание, что и мигранты. При этом в состав сетей входят преступники, являющиеся гражданами не только стран, не входящих в ЕС, но и государств-членов ЕС.

Другой вывод состоит в том, что многие лидеры и активные участники преступных сетей, родившись за пределами ЕС, в последующем стали гражданами или получили вид на жительство в странах ЕС, где они и осуществляют преступный бизнес. За пределами ЕС лидеры и активные участники преступных сетей, как правило, работают с мигрантами того же этнического происхождения, что и они сами.

Типовая структура преступных сетей нелегальной миграции включает в себя лидеров-координаторов, организаторов, которые управляют деятельностью на местном уровне через личные контакты и агентов низкого уровня, которые преимущественно помогают организаторам, а также занимаются подбором преступных кадров и ответственных за информационную работу в регионах, откуда начинаются нелегальные мигрантские потоки. Вышестоящие органы преступных сетей, как правило, работают со значительным числом автономных агентов самого низкого уровня. Агенты самого низкого уровня используются как водители, охранники, организаторы групп мигрантов в районах их проживания и т. п.

Сложность сети, в конечном счете, определяется длиной, степенью риска, разнообразием услуг по нелегальной миграции и интенсивности потока незаконных мигрантов.

Преступные группы осуществляют сотрудничество в тех случаях, когда криминальные сети имеют географическую локализацию. В этом случае возникают сложные сети, объединяющие группы, контролирующие различные участки маршрутов.

С каждым месяцем возрастает количество мигрантов, услуги которым оказывают не временные сети, сконфигурированные из различных локальных групп, а относительно постоянные сети, имеющие устойчивое ядро и временные обслуживающие подразделения. Несмотря на то, что между различными группами имеется определенная конкуренция, с каждым месяцем все более вырисовываются преступные группировки, контролирующие те или иные маршруты практически от страны исхода до страны пребывания. Вместо жестокой конкуренции, свойственной преступным рынкам, возникает феномен олигополии, когда рынок оказывается поделен между несколькими крупнейшими структурами. Это не отменяет конкуренцию, но она происходит среди местных групп в основном низового уровня, а также групп, специализирующихся на определенных услугах, за право работать с господствующими глобальными сетями.

Господствующие глобальные сети, таким образом, работают не только с локальными агентами, но и с преступными группами, специализирующимися, например, на предоставлении транспорта, морских перевозках, коррумпировании чиновников и правоохранительных органов на протяжении маршрута и т. п.

Что касается бизнес-модели преступных сетей, то она построена вокруг увеличения миграционного потока и оказания мигрантам максимума услуг. Если ранее преступные сети обслуживали в основном мигрантов, которые самостоятельно принимали решение о нелегальном проникновении на территорию ЕС, то в настоящее время в лагерях и других местах сосредоточения потенциальных мигрантов работают агитаторы и контролеры. Агитаторы стараются убедить обитателей лагерей и также жителей районов, откуда уже началась миграция, в том, что при оплате деньгами или натурой, они могут быть успешно переброшены в ЕС и закрепиться в одной из стран. Контролеры отбирают из общего числа желающих покинуть места постоянного пребывания тех индивидуальных мигрантов, семьи и роды, которые способны оплатить услуги преступных сетей деньгами или натурой. Все более широко используются для агитации мигрантов социальные медиа, в которых размещается информация о маршрутах, услугах, ценах и пунктах, где можно произвести оплату.

Коррупция является еще одним ключевым фактором, способствующим нарастанию потока нелегальных мигрантов в ЕС. Наиболее восприимчивы к коррупции работники правоохранительных и таможенных органов, лица, осуществляющие пограничный контроль, а также

военные сухопутных и военно-морских сил. Установлено, что оплата им производится либо в зависимости от количества кораблей, автобусов и т. п., которые они допускают на территорию ЕС, либо по оценочному числу мигрантов, пропущенных ими в течение определенного периода времени.

Преступные сети охотно делятся частью прибыли с правоохранителями, таможенниками, военными и чиновниками, поскольку эти коррумпированные сотрудники позволяют криминалу при снижении нормы прибыли заметно увеличить ее массу. Более того, те масштабы нелегальной миграции, которые сложились к настоящему времени, были бы невозможны без высокого уровня коррумпированности правоохранителей, таможенников, пограничников, миграционных чиновников и т. п. в странах, по которым пролегают миграционные маршруты и в странах конечного назначения. Грубая оценка годового денежного оборота преступников за счет незаконного ввоза мигрантов может быть получена на основе оценки численности мигрантов в ЕС в 2015 г. Около 1 млн. человек незаконно оказались в ЕС. Подавляющему большинству из них было оказано содействие в перевозке, транспортировке, проникновении и закреплении в странах пребывания. В среднем мигранты заплатили за услуги от 3,2 до 6,5 тыс. долларов или 3–6 тыс. евро за человека. Указанные цифры позволяют оценить средний оборот преступных сетей в сумму от 5 до 6 млрд. долларов в 2015 г.

В настоящее время используются различные схемы и средства оплаты. В одних случаях незаконные мигранты осуществляют оплату заранее за весь маршрут. В других – расчеты осуществляются поэтапно, на каждом участке пути или по прибытии в промежуточные и заключительные пункты назначения. Также используются различные способы оплаты. Согласно самым последним данным, полученным уже в 2016 г., наиболее распространенными из них являются денежные средства и хавала.

Согласно имеющимся данным преступные сети получают деньги в основном из стран конечного назначения. Это означает достаточно парадоксальный факт, что мигранты, как правило, платят не в начале маршрута, а тогда, когда достигают страны назначения. Фактически, преступные сети своего рода авансируют незаконных мигрантов, поскольку транспортные услуги, а также продвижение по маршруту предполагает предварительные затраты. Преступные сети выступают как своеобразные кредитные учреждения по отношению к мигрантам. Оборотной стороной этого является жесткий контроль миграционного потока на всех его стадиях со стороны преступников с наличием в каждой мигрантской группе контролеров и своего рода охранников, обеспечивающих доставку мигрантов до места назначения в целости. Хавала наиболее широко используется преступными сетями, базирующимися в Турции, Ираке и других странах Ближнего Востока и Азии. В некоторых случаях мигранты тратят несколько недель или месяцев в транзитных узлах для того, чтобы возместить посреднику затраты или накопить деньги на следующий этап путешествия.

Таким образом, можно сделать вывод, что выделяются две существенно разных группы мигрантов – относительно богатое меньшинство, которое рассчитывается деньгами, преимущественно наличными, в конечном пункте назначения и подавляющее – небогатое и нищее – меньшинство, которое оплачивает свой транзит в ЕС поэтапно, в основном используя хавалу. Можно также предположить, что в относительно богатую часть мигрантов входят не только те мигранты и семьи, которые обладают значительным имуществом или средствами в стране пребывания, но и те, кто имеет устойчивые, в том числе родственные, связи в диаспоре страны конечного назначения. На этот вывод наталкивает то, что оплата в стране конечного назначения в основном осуществляется в местах расположения этнических и конфессиональных диаспор.

Хотя незаконный ввоз мигрантов является высокоприбыльным бизнесом, преступные сети сталкиваются с рисками. Данные риски связаны не столько с проблемами неплатежеспособности мигрантов, сколько с необходимостью отмывания преступных денег. В зависимо-

сти от сложности сетей, используется несколько методов отмывания денег. Данная проблема связана с тем, что лишь часть средств инвестируется преступными сетями в развитие инфраструктуры нелегальной миграции, а также другие виды криминального бизнеса. Остальную, значительную, часть средств преступные группы инвестируют в легальную экономику. Разведывательная информация показывает, что криминал все чаще в качестве основного платежного средства, используемого как для платежа, так и для отмывания доходов, выбирает наличные деньги.

Известно, что в Европе действуют курьерские сети специальных денежных мулов, которые осуществляют перевозки больших сумм наличных денег через границы, либо по суше, используя различные тайные хранилища в автомобильном транспорте, или по воздуху. В некоторых случаях, и их число растет, преступники или их родственники владеют законными бизнесами, такими как автосалоны, продуктовые магазины, рестораны и т. п., которые очень удобно использовать для отмывания преступных доходов и обеспечения фасада легитимной деятельности. Преступные доходы особо активно вкладываются в недвижимость, приобретение легального бизнеса в различных странах, а также в инвестиции на финансовых рынках.

Легальные бизнес-структуры активно используются в организации обслуживания нелегальных антропотоков. Тем не менее, не всегда ясно, в какой степени они являются собственностью преступных сетей, а в какой оказывают услуги в результате угроз и насилия со стороны криминала. Наиболее уязвимыми секторами легальной экономики являются предприятия общественного питания, гостиницы, транспортные компании, магазины, туристические агентства и интернет-кафе. Эти предприятия не только используются для обслуживания миграционных маршрутов, но и вносят свой вклад в отмывание преступных доходов от незаконной миграции.

Индустрия нелегальных операционных услуг

Успешное осуществление нелегальной миграции предполагает оказание широкого спектра криминальных услуг. Прежде всего, необходимы подложные документы, позволяющие пересечь различные критические точки маршрутов. Например, в Западной и Северной Европе мигранты широко используют общественный транспорт, включая автобусы и поезда. Доступ на транспортные средства возможен только при наличии документов. Они же позволяют пройти проверки безопасности на борту транспортных средств. Отдельные мигранты, попадающие в поток без содействия преступных сетей, рассказывают, что попытки проникнуть в Италию, Францию, или через Ла-Манш в Великобританию заканчиваются, как правило, неудачей и они обращаются к преступным синдикатам с просьбой предоставить поддельные документы.

На большинстве маршрутов используются комбинированные средства передвижения. Если в начале миграционного бума широко было распространено пешее передвижение, особенно по греческо-балканскому маршруту, то в настоящее время в основном используются автобусы, грузовики или поезда. Мигранты спешиваются и осуществляют небольшие марши лишь для того, чтобы пересечь зеленую границу между странами. Во многих случаях транспортные средства, используемые криминалом, регистрируются с транспортными знаками, отличными от страны проживания их владельца. Широко используются арендованные автомобили. Все это затрудняет работу правоохранительных органов по идентификации структур, оказывающих транспортные услуги криминалу.

По-прежнему действуют морские маршруты, как отрезки доставки мигрантов из Африки и с Ближнего Востока в Европу. Наиболее интенсивно используются юго-восточный – через Грецию, центрально-средиземноморский – через Италию, юго-западный – через Испанию морские маршруты доставки в Европу. Также в транспортную инфраструктуру криминальных потоков входит маршрут пересечения Красного моря через Йемен.

Наиболее широко используемым средством транспорта на коротких расстояниях была в 2015 г. резиновая лодка. Она имеет длину 8-12 метров и вместимость 30–40 мигрантов. Из-за высоких рисков в подавляющем большинстве случаев преступники не сопровождают мигрантов во время морского путешествия из Турции в Грецию на лодках. Они ограничиваются инструктажем и тренировкой мигрантов в части управления лодками. Для доставки наиболее платежеспособных и ценных нелегальных мигрантов преступники используют рыболовные и грузовые суда. Особо активно они используются на центрально-средиземноморском маршруте.

В настоящее время наиболее редко используются транспортировки мигрантов по воздуху. Однако в будущем воздушная логистика получит гораздо более широкое распространение из-за ужесточения контроля на сухопутных и морских путях.

В условиях все более активного использования лоукостеров и развития в Европе сети небольших и малых аэродромов, воздушная транспортировка может стать весьма привлекательным способом доставки мигрантов непосредственно в страны назначения. Преступные услуги по организации воздушны перевозок связаны не столько с заключениями договоров с теми или иными компаниями, сколько с предоставлением особо тщательно изготовленных поддельных документов. Высказывается мнение, что в силу высокого качества поддельных документов и соответственно затрат на их производство, документы могут не предоставляться, а сдаваться в аренду на время воздушной транспортировки.

Для повышения вероятности переброски незаконных мигрантов в ЕС преступники также рассматривают возможность использования сложных маршрутов и необычных приемов. Последние включают покупку билетов в два конца, в том числе обратных билетов, что снижает подозрения, рассматривается тема использования транспортной авиации и соответственно аэропортов, рассчитанных на прием грузов, для доставки мигрантов.

Диверсификация преступности

Данные свидетельствуют: преступный бизнес на нелегальной миграции все теснее сращивается с криминалом, специализирующемся на незаконном обороте наркотиков, подделке документов, имущественных преступлениях и торговле людьми и органами. В 2015 г. было выявлено более 220 случаев, когда преступные сети, занятые нелегальной миграцией, были идентифицированы Европолом, как сети и отдельные преступники, участвующие в более чем в одной области преступности. Из них 22 % были связаны с незаконным оборотом наркотиков, 20 % – с незаконной торговлей людьми, 20 % – с преступлениями против собственности и 18 % – с подделкой документов.

Данные разведки последних месяцев свидетельствуют, что в 2016 г. переплетение бизнеса на незаконной миграции с другими видами криминала будет гораздо выше, чем в 2015 г.

Были выявлены три типа связей между криминалом на нелегальной миграции и ОПГ, специализирующимися на других видах преступлений. Первый тип включает в себя криминальных субъектов, которые добавили к привычным им видам преступности незаконный ввоз мигрантов. Второй тип относится к криминальным группировкам, контролирующим те или иные объекты или маршруты криминальной инфраструктуры. Одни и те же маршруты и объекты используются как для незаконного ввоза мигрантов, так и для незаконного оборота наркотиков и оружия, а также контрабандных поставок различных видов продукции. Третий тип связей базируется на том, что незаконный мигрант является не только плательщиком за преступные услуги, связанные с нелегальным проникновением в ЕС, но и объектом трудовой или сексуальной эксплуатации, потенциальным участником преступных этнических группировок в государствах-членах ЕС.

С географической точки зрения маршруты нелегальной миграции идентичны криминальным логистическим цепочкам, используемым для контрабанды товаров, а также наркотиков, оружия и т. п. В результате группы контрабандистов и наркосиндикаты включаются в бизнес, связанный с нелегальной миграцией. Кроме того, сам нелегальный интенсивный антропоток позволяет увеличить наркотрафик, объемы незаконной торговли оружием, контрабанду различных товаров и т. п.

Поскольку в 2015 г. нелегальный миграционный бизнес характеризовался высокой маржинальностью (прибыльностью), ряд криминальных банд, занимающихся контрабандой обычных товаров, диверсифицировала деятельность и включилась в этот бизнес. Сращивание преступности, обслуживающей нелегальный антропоток с такими секторами криминала, как контрабандисты и наркосиндикаты, связано с тем, что последние за длительное время отработали инфраструктуру переброски контрабандных товаров и наркотиков и для этого коррумпировали пограничников, таможенников, правоохранителей и т. п. Сегодня коррумпированные работники государственных органов получают возможность заработать на дополнительном направлении преступности – нелегальном ввозе мигрантов.

Преступная деятельность, связанная с незаконным ввозом мигрантов, привела к взрывному росту криминала по подделке документов. За 2015 г. доля подозреваемых в подделке документов в странах ЕС в общем объеме подозреваемых по самым различным преступлениям увеличилась с 3 до 18 %.

В настоящее время резко растет не только качество, но и номенклатура поддельных документов, использующихся для нелегальной миграции. Наиболее широко подделываются паспорта, визы, документы, удостоверяющие личность, (например ID карты), подтверждающие документы, (например, водительские удостоверения, карточки беженцев), а также документы, требуемые для получения статуса беженца, (например, свидетельства о рождении, справки признанных ООН благотворительных и миротворческих организаций, записи о браке, документы, подтверждающие наличие родственных связей, трудовые книжки, вид на жительство и т. п.).

Документы определенных стран являются более привлекательными, чем другие, и стоят дороже. Это обуславливается тем, что они позволяют владельцам получить доступ к определенным услугам и пособиям, которые в противном случае оказываются недоступными. В целом, ужесточение контроля, ограничение на поездки и въезд в некоторые страны ЕС, скорее всего, приведет в 2016 г. к возрастанию спроса на поддельные документы, повышению требований к качеству изготовления документов. Это в совокупности неизбежно увеличит цены на поддельные документы.

Злоупотребления легальными каналами является еще одной составной частью инфраструктуры нелегальной миграции. При этом эти каналы зачастую могут быть не связаны с сетями, а находиться под контролем отдельных локализованных преступных групп. Кроме того, такие каналы не носят массового характера и обслуживают преимущественно состоятельных нелегальных мигрантов.

Легальным каналом с наибольшей пропускной способностью, используемым нелегальными мигрантами, является туризм и туристические агентства. Нелегальные мигранты получают туристические визы, и уже прибыв в страну-член ЕС, находят, как правило, при помощи родственников или преступных элементов диаспоры, посредников преступных сетей. Посредники помогают этим мигрантам получить поддельные, либо с нарушениями закона оформить подлинные документы, позволяющие получить статус резидентов.

Наиболее часто встречаются случаи, когда нелегальные мигранты пребывают в ЕС по туристической визе, а затем остаются в странах пребывания после истечения срока действия Шенгенской визы. Такие нелегальные мигранты, как правило, проживают в районах расселе-

ния диаспор, работают на предприятиях нелегальной экономики, либо вовлекаются в преступную деятельность.

Преступные сети включили в орбиту своей деятельности такие легальные институты как временные лагеря и убежища для нелегальных мигрантов в странах ЕС. В силу целого ряда политических, социальных и психологических причин государственные органы многих государств-членов ЕС согласились с временным пребыванием нелегальных мигрантов, не подпадающих под признанный статус беженцев в закрытых лагерях временного проживания на территориях своих стран.

При этом в странах ЕС обеспечиваются питание, проживание и оказание различных услуг лицам, находящимся в подобных лагерях. Кроме того, в некоторых странах отсутствуют законодательно установленные сроки проживания, и нет четких процедур высылки обитателей лагерей за границы ЕС.

Этой легальной двусмысленностью пользуются преступные синдикаты. Они, коррумпируя чиновников и работников благотворительных организаций, обеспечивают относительно приемлемые, тем более по сравнению с ситуацией в стране постоянного проживания, условия жизни нелегальных мигрантов. Кроме того, налажены каналы получения для нелегальных мигрантов в подобных лагерях документов временного вида на жительство и статуса беженца. Все большее распространение в странах конечного назначения приобретает бизнес, связанный с организацией фиктивных браков нелегальных мигрантов с гражданами этих стран, преимущественно той же этнической и религиозной принадлежности.

Нелегальные мигранты уязвимы для криминальных сетей как до, так и после их прибытия в ЕС. В результате сложившихся условий, а также в силу необходимости оплатить транзит, они подвергаются со стороны преступных сетей сексуальной эксплуатации, вынуждены работать на предприятиях криминальной экономики, либо на легальных предприятиях без регистрации, с минимальной оплатой, служить в качестве мулов для перевозки наркотиков, а также участвовать в качестве исполнителей самого низового уровня в деятельности преступных сетей, в том числе связанных с нелегальной миграцией. Имеется статистика о постоянном увеличении доли так называемой «натуральной» оплаты за миграцию. Особо быстрыми темпами это происходит в отношении молодых женщин и несовершеннолетних. Однако и взрослые мужчины, которые не в состоянии покрыть финансовые расходы на оплату нелегального трафика в ЕС, все чаще выполняют поручения для преступных сетей в качестве оплаты.

Нелегальная миграция, терроризм и радикальное насилие

В условиях сочетания миграционного давления и растущего терроризма внутри ЕС проявляется все возрастающая озабоченность тем, что нелегальный антропоток и преступные сети широко используют для инфильтрации в ЕС радикально настроенных иностранных боевиков и членов трансграничных террористических организаций.

Европол установил, что наиболее тесная смычка терроризма и незаконной миграции осуществляется через финансирование терроризма за счет доходов преступных сетей от нелегальной миграции. Несмотря на то, что Европол не получил конкретных данных о том, что террористические организации прямо сотрудничают с организованными преступными группами в своей деятельности, нельзя сбрасывать со счетов следующую возможность.

Она связана с тем, что террористы напрямую используют нелегальную миграцию для инфильтрации в Европу большого числа радикально настроенных мигрантов, которые в последующем разворачивают в странах пребывания как активные, так и спящие ячейки наиболее опасных террористических организаций. В 2015 г. выявлены некоторые случаи взаимодействия террористов с преступными организациями и использования миграционных потоков для инфильтрации террористов. В ходе расследования террористических актов в Париже в ноябре

2015 г. было установлено, что двое из нападавших проникли в ЕС через Грецию в составе потока нелегальных мигрантов из Сирии.

Тренды и риски будущего

– В целом будет происходить увеличение численности мигрантов, пытающихся инфильтрироваться в ЕС. Только в портах Ливии находится в настоящее время около 800 тыс. мигрантов, ожидающих транспортировки в страны ЕС.

– Ожидается, что в 2016 г. более 90 % нелегальных мигрантов в ЕС будут пользоваться услугами преступных сетей. При этом в Европе будут ужесточаться процедуры, а также возможно закрытие национальных границ ряда стран ЕС. Это, с одной стороны, сделает преступные услуги более востребованными для мигрантов, а с другой – приведет к их удорожанию.

– Продолжится процесс формирования олигополий. В результате незаконную миграцию будут во все возрастающей степени контролировать несколько крупнейших преступных сетей, связанных с многочисленными мелкими сетями и группировками, как правило, за пределами ЕС. Этот процесс особенно активно уже идет за пределами ЕС, прежде всего, в Турции, Египте и Ливии. Он будет продолжаться и дальше в Европе.

– Будет продолжаться диверсификация деятельности криминальных сетей, специализирующихся на незаконном ввозе мигрантов. Ожидается, что эти сети вберут в себя фальшивомонетничество, изготовление поддельных кредитных карт и т. п. Все большую роль по мере вовлечения в нелегальную миграцию все менее состоятельных слоев и групп будет играть натуральная оплата услуг преступных сетей. В первую очередь это будет относиться к нелегальной занятости, занятости в теневой экономике и сексуальной эксплуатации в странах конечного назначения мигрантов. Будут укрепляться связи криминала, специализирующегося на незаконном ввозе мигрантов и другими видами преступлений, в первую очередь такими, как торговля людьми, незаконный оборот наркотиками и контрабанда товаров.

– В государствах-членах ЕС возникнет феномен принудительной преступности. Мигранты будут вынуждены заниматься преступной деятельностью как формой оплаты за свою доставку в Европу. Следует ожидать роста преступности, связанной с использованием криминальными сетями и группировками беспризорных несовершеннолетних, которые будут вынуждены участвовать в преступных действиях. Согласно имеющимся данным, преступные группировки будут активно развивать бизнес сексуальной эксплуатации несовершеннолетних.

– Ожидается стремительный рост производства и оборота поддельных документов. Нелегальные мигранты, уже прибывшие в ЕС, породят гигантский, ранее не существовавший спрос на поддельные свидетельства о предоставлении вида на жительство, статуса беженца, фальшивых разрешений на работу и т. п., чтобы закрепиться на постоянное жительство в стране назначения.

– Будет постоянно увеличиваться спрос на проездные и транзитные документы незаконного происхождения. Есть основания полагать, что высококачественные поддельные документы такого рода будут предоставляться мигрантам на основе аренды и использоваться многократно.

– Основные горячие точки миграционных потоков, скорее всего, сохранятся в обозримом будущем. Тем не менее, в соответствии с колебанием потоков, изменением политики или действий правоохранительных органов будут исчезать и появляться горячие точки второго и третьего порядков, играющие подчиненную роль в глобальной инфраструктуре нелегальной миграции.

Рекомендации

– Открытие Европейского центра по нелегальной миграции (EMSC) в структуре Европола является важным шагом на пути усиления борьбы с незаконной миграцией и преступными сетями, осуществляющими эту деятельность. EMSC обеспечит эффективную оперативную и стратегическую поддержку государствам-членам ЕС, в том числе путем развертывания в структуре Европола мобильных следственных групп поддержки (EMIST) и мобильных аналитических групп поддержки Европола (EMAST) в тесном взаимодействии с Интерполом, странами ЕС и другими заинтересованными в партнерстве странами.

– Интерполом создана специальная оперативная сеть против незаконного ввоза мигрантов (ISON). В настоящее время она включает 86 экспертов из 71 страны, включая страны источники, транзитные страны и страны назначения, которая тесно сотрудничает с Европолом. ISON содействует расширению обмена в режиме реального времени информацией между правоохранительными органами по всему миру для более эффективного расследования преступности, связанной с нелегальной миграцией. Странам-членам Интерпола предлагается присоединиться и использовать данную сеть.

– Организация Интерпола INFRA, известная под названием ГИДРА, (международный розыск, отслеживание и аресты) создана для помощи странам-членам в поиске и поимке разыскиваемых преступников, участвующих в торговле людьми, а также в целях содействия глобальному обмену информацией об их местонахождении, укреплении связей между следователями и специализированными подразделениями, а также содействию использования документов и сведений Европола. Она осуществляет свою деятельность в координации с Европолом.

– Правоохранительным органам в странах-членах Интерпола рекомендуется улучшить обмен информацией о преступных сетях, связанных с нелегальной миграцией, а также для оптимального использования инструментов и возможностей, предоставляемых Интерполом и Европолом для дальнейшего улучшения трансграничного взаимодействия в борьбе с преступностью.

Методология

Этот доклад основан на информации, имеющейся в распоряжении Европола и Интерпола, а также почерпнутой из открытых проверенных источников. Выводы, содержащиеся в докладе, базируются на тщательном анализе широкого круга источников и обеспечивают наиболее детальную из когда-либо осуществленных оценку нелегальной миграции. Доклад является уникальным результатом взаимодействия данных разведки ЕС со сведениями, предоставленными странами, не являющимися членами ЕС. Он базируется на:

– 11 500 досье относительно нелегальной миграции, созданных Европолом в 2014 и 2015 гг.;

– разведывательных данных по почти 40 тыс. подозреваемых, 10 тыс. из которых были получены в 2015 г.;

– более чем 1500 международных расследованиях, поддержанных Европолом;

– 1500 файлах, связанных с миграцией, собранных Frontex и государствами-членами ЕС;

– более чем 140000 коммуникациях, осуществленных в 2015 г.;

– оперативных и стратегических докладах, подготовленных Европолом и Интерполом;

– данных опросников, предоставленных центральными национальными бюро Европола;

– географической информации;

– разведывательных данных на более чем 100 подозрительных судов, возможно обслуживающих незаконную миграцию;

– анализе социальных медиа, осуществленном группой интернет-реферирования Европола;

– ежедневных докладах-мониторингах нелегальной миграции, выпускаемых Европолом (EPNT);

– докладах партнерских агентств (Frontex, EASO, UN Agencies);

– разведке по открытым источникам (OSINT).

Для изучения набора данных было использовано сочетание нескольких аналитических инструментов:

– был осуществлен анализ криминальных профилей на более чем 10 тыс. подозреваемых с тем, чтобы определить их происхождение, роль в незаконном ввозе мигрантов, а также связи друг с другом и ранг взаимоотношений;

– был проведен детальный сравнительный анализ на выборке из 522 преступных сетей с целью определения их состава, структуры, системы и характера связей внутри сетей и профилей лидеров;

– в отношении крупнейших преступных сетей с использованием мощного программного обеспечения был проведен социальный сетевой анализ, который позволил установить характер, тесноту и виды связей, как отдельных членов сетей, так и выявленных узлов и паттернов. Было проведено исследование стиля и конкретных форм руководства организациями и связей между лидерами и нижестоящими органами;

– при поддержке Европола было проведено качественное исследование на основе обобщения 490 отдельных исследований для того, чтобы установить контекст и выделить наиболее характерные конкретные примеры;

– географический анализ был использован для выявления ключевых мест и горячих точек, связанных с потоками незаконной миграции.

Часть IV
Экологическая и фармацевтическая мафии

Организованная преступность и криминальная экология: анализ правовых инструментов Европейского Союза[32]

Организованная преступная деятельность в отношении среды обитания является в основном прерогативой организованных преступных групп, зачастую имеющих транснациональный характер. Это требует координации правоохранительных органов отдельных стран с международными институтами ЕС, а также с правоохранительными органами третьих стран.

Организованная преступность наносит значительный ущерб экологии Европы. При этом, результаты обследования и статистика показывает, что масштабы экологической преступности, а также размеры ущерба непрерывно возрастают. При этом, организованные преступные группировки взаимодействуют с легальными акторами, включая рыночных субъектов, различного рода общественные группы и коррумпированных чиновников. Также, наряду с формированием крупных универсальных организованных преступных группировок, одним из направлений деятельности которых является экологическая преступность, становится появление небольших преступных группировок и небольших групп, специализированных на отдельных видах преступных услуг, в том числе в части экологии. С развитием информационных технологий резко возросли возможности преступников устанавливать транснациональные и трансконтинентальные связи между собой и координировать свою деятельность не только в локальном, но и в глобальном масштабах. Не будет преувеличением сказать, что сегодняшняя экологическая преступность в Европе представляет собой сложный иерархо-сетевой феномен. При сохранении центральных, крупных транснациональных группировок, сетевые элементы этого образования легко заменяемы и легко демонтируемы. Между тем, именно с ними преимущественно борются правоохранительные органы европейских стран.

Несмотря на многократные инициативы Европейского парламента, исполнительные органы ЕС пока не подготовили предложений, связанных с законодательным оформлением мер по борьбе с международной организованной экологической преступностью. Особенно недопустимым является промедление в части создания законодательной общеевропейской базы по таким ключевым направлениям, как экологическая преступность, связанная с загрязнением окружающей среды не только промышленными.

Но и энергетическими предприятиями, нефте- и газотранспортирующими и перерабатывающими компаниями, а также АЭС. Кроме того, в отсутствие экологического страхования правоохранительные органы не имеют законодательной базы по борьбе с организованной экологической преступностью, предполагающей нарушение европейского законодательства в сфере продажи немаркированной генно-модифицированной продукции, не сертифицированных материалов для животноводства и земледелия, а также использование на промышленных и иных предприятиях технологий, загрязняющих воздух и воду. Данные виды преступности не только наносят огромный социальный ущерб, но и согласно разным оценкам, наносят прямой ущерб окружающей среде Европы, исчисляемый по разным оценкам суммой от 40 до 70 млрд. долларов ежегодно.

---

[32] *Проект подготовлен в рамках Седьмой рамочной программы ЕС по исследованиям, технологическому развитию и разработкам за счет гранта 320276. Автор: Тереза Фахарда Дель Костильо, профессор университета Гранады, Испания, Февраль 2015.* (Извлечение)

Применительно к экологической преступности, законодательство не отработано не только на уровне ЕС, но и большинства входящих в него стран, особенно новых членов Европейского Союза. Более того, во многих странах борьба с экологической преступностью не относится к ведению министерств внутренних дел, а является прерогативой различного рода контрольных и иных организаций, у которых отсутствуют оперативные и расследовательские функции. Это особенно нетерпимо в ситуации, когда экологическая преступность и криминальное сокрытие экологических преступлений, совершенных легальными субъектами, становится все более значительным и доходным видом деятельности крупнейших национальных и транснациональных преступных группировок.

По мнению европейских институтов, необходимо не только совершенствовать законодательство и расширять возможности уголовно-исполнительной системы по борьбе с экологической преступностью, но и шире использовать административный подход для предотвращения подобных преступлений.

Европол и организованная экологическая преступность

Конвенция Европола последнее время дополнена приложением относительно групп «серьезных форм международной преступности, в отношении которых Европол может осуществлять оперативно-следственные действия». Применительно к экологической преступности это включает в себя:

– незаконный оборот оружия, боеприпасов и взрывчатых веществ, используемых для незаконной охоты и других преступлений в отношении окружающей среды; – незаконный оборот исчезающих или охраняемых видов флоры и фауны; – незаконный оборот отходов, а также незаконное захоронение или хранение отходов; – экологические преступления; – незаконный оборот гормональных веществ, генно-модифицированных образцов и стимуляторов роста. В ноябре 2013 г. ЕВРОПРОЛ впервые в истории представил **доклад по оценке угроз экологической преступности в странах ЕС**. В докладе в частности отмечено, что «наиболее серьезные и крупные по масштабам экологические преступления с участием организованной преступности в странах ЕС связаны с незаконным оборотом и захоронением отходов, преступным сокрытием масштабов и цены экологического ущерба, нанесенного окружающей среде и населению легальными хозяйственными субъектами, а также торговля находящимися под угрозой исчезновения видам флоры и фауны, либо товаров, изготавливаемых из указанных видов».

Торговля исчезающими видами флоры и фауны и изделиями, изготовленными из них.

Европол выявил, что этот вид преступности привлекает организованные группировки, имеющие в своем составе высокоспециализированные, функциональные команды, действующие как самостоятельно, так и подряжающиеся в качестве субподрядчиков в преступные группировки, а также представители неорганизованной преступности в странах, входящих в ареалы обитания исчезающих или на международном уровне охраняемых видов флоры и фауны. По оценке доклада объем мирового рынка составляет по различным национальным международным оценкам от 18 до 26 млрд. евро в год. Ежегодное увеличение рынка составляет 7–10 %. Главным рынком сбыта является Европа, на которую приходится от 50 до 60 % общего объема мирового сбыта.

Исследование выявило, что рынок поделен в основном не по региональному, а по видовому признаку, сообразно отдельным видам животных и растений. В рамках этого рынка сложились и успешно действуют пирамидальные преступные сообщества. На верху пирамиды находятся высокоорганизованные адаптивные. Накопившие опыт в противодействии полиции и судебным органам, специализированные функциональные подразделения крупнейших европейских и транснациональных организаций. В отличие от XX века, когда европейские преступ-

ники лично занимались отловом или охотой на животных и сбором соответствующих растений. А также организовывали их транспортировку, в настоящее время ситуация изменилась. Европейская организованная преступность выполняет штабные, инвестиционные, координирующие и сбытовые функции. Логистические функции берут на себя специализированные международные нелегальные коммуникационные сети, а также легальные системы аэродоставки. Организованная преступность в ареалах обитания видов животных и растений, вовлеченных в рынки, организует на территориях своих стран своего рода транзитные пункты – накопители, куда поступают образцы из различных территорий ареала обитания. Данные накопители действуют либо как филиалы европейских преступных организаций, либо как универсальные криминальные накопители, поставляющие разнообразные грузы одним логистическим средством в конкретный город или страну».

Наряду непосредственно с животными и растениями в число наиболее прибыльных активов относятся полуфабрикаты и изделия из них. Активом, обеспечивающим от 1200 до 1500 % прибыли является слоновая кость и рога носорога пашот, добываемые в Африке и реализуемые в Европе и, особенно, в Китае, где на них имеется огромный спрос. В Африке местные преступные группы, взаимодействующие с накопительными пунктами и европейскими организованными группировками, характеризуются небольшими размерами и чрезвычайно высоким уровнем специализации по отдельным животным и растениям. В то же время в Южной Америке и Азии группы добытчиков и охотников, как правило, интегрированы в повстанческие и террористические сети и в большинстве своем с наркосиндикатами. В докладе выделены основные виды преступности в этой сфере. Это в первую очередь крупные живые животные, которых продают в частные зоопарки с помощью фальшивых документов. Что касается мелких животных, птиц, а также растений, то поставка, как правило, осуществляется в массовом порядке, без каких-либо документов вообще.

Вторым по объему является рынок слоновой кости, рогов носорогов, шкур ценных и исчезающих животных, типа леопарда, а также добытых без лицензий и документов, змеиный яд.

В докладе отмечено, что процветанию этого направления экологической преступности способствует запредельно высоких уровень коррупции во многих государствах, входящих в сферу ареала обитания наиболее ценимых на рынке живых животных и растений, а также изделий из них. В результате во все возрастающем числе случае грузы доставляются в Европе не с фальшивыми, а с подлинными разрешительными документами. Иными словами, государственные чиновники стран Азии, Африки и Латинской Америки становятся цепочкой преступного бизнеса и затрудняют противодействие ему в странах ЕС.

Новым направлением экологической преступности является организация преступными группами в странах ЕС глобального бизнеса по доставке в Китай хищных птиц, животных и растений, широко используемых традиционной китайской медициной и исчезнувших, либо жестко охраняемых в самом Китае.

В своем докладе Европол отметил также новые инновационные решения преступных организаций. Например, в Европе вскрыта сеть выставочных залов, музеев и агентств по организации выставок и экскурсионных туров в замки, являющиеся прикрытием для незаконной торговли животными и изделиями из них. Уже после опубликования доклада стало известно, что в этот бизнес стали входить и государственные, а также частные европейские зоопарки.

В докладе отмечено, что, хотя европейская организованная преступность слабо участвует в преступном экологическом бизнесе, связанным с неразрешенной варварской вырубкой тропических лесов, в мире этот бизнес оценивается в масштабе[6] порядка 70-120 млрд. долларов в год. Главными регионами являются латиноамериканские страны зоны Амазонки и африканские страны зоны Замбези и Великих Водопадов. Главными участниками этого рынка являются латиноамериканские и африканские преступные синдикаты, и соответственно штабные

структуры, расположенные для латиноамериканских структур – в США, а для африканских – преимущественно в Гонконге и приморских районах Китая.

Незаконный оборот и хранение отходов В 2013 г. Европол сделал вывод, что бизнес, связанный с незаконным хранением, захоронением и оборотом отходов растет в геометрической прогрессии как по стоимости рынка, так и по объемам токсичности объемов. По оценкам Европола, среднегодовая норма прибыли в этом бизнесе колеблется между 600 и 900 % годовых. В докладе преступные организации, занятые в этом бизнесе классифицированы по их основным видам. В незаконный оборот отходов в использованном далее широком смысле, включается хранение, захоронении и собственно оборот отходов, осуществляемый без или с нарушением законодательно установленных норм и юридически правомочных решений. В этом виде экологической преступности участвуют как преступные организации, так и легальные компании, ведущие незаконный бизнес. Широкому масштабам этого бизнеса способствуют многочисленные лазейки в законодательстве ЕС, связанном с оборотом отходов, а также разнобой, а в отдельных случаях и прямые противоречия между национальным законодательством стран ЕС по экологической проблематике. Также свой вклад вносят и пробелы, связанные со стандартами и техническим регулированием оборота отходов в странах ЕС. Наиболее распространенным видом экологических преступлений этого типа являются создание несанкционированных хранилищ и захоронений мусора (отходов), а также контрабандная поставка отходов, особенно высокотоксичных из стран с развитым и жестким экологическим законодательством в страны с более льготным законодательным, техническими и экономическим режимами в отношении отходов. В докладе особо отмечено, что по экспоненте растет бизнес, связанный с нелегальным вывозом особенно высокотоксичных компактных отходов из Западно- и Североевропейских стран ЕС за пределы ЕС, в страны Восточной Европы, и прежде всего на Украину и в Россию.

Обязательным компонентом данного бизнеса является широкое использование в нем подложных разрешительных документов и технической документации, а также коррупция среди сертификационных центров, центров технического регулирования и таможенных служб. Внутри ЕС все большее распространение получает так называемая «техника хранения», когда вместо законодательно установленных процедур утилизации отходов путем переработки осуществляется их вывоз на временное хранение с последующей переработкой в страны ЕС и за пределы ЕС, где такие склады созданы.

Практически во всех европейских странах по экспоненте растет объем в метрических тоннах промышленных и урбанистических отходов. Более чем в 70 % европейских городов с населением более 100 тыс. человек и более законодательно разрешенные объемы специально оборудованных мест захоронения мусора и отходов, а также мощности по их переработке в среднем по состоянию на 2013 г. менее чем на 70 % были способны переработать весь объем. Причем, с каждым годом разрыв между имеющимися мощностями и потребностями непрерывно возрастает. В этих условиях даже такие ранее благополучные страны, как Великобритания, Франция и страны Бенилюкса препятствуют на муниципальном и государственном уровнях ужесточению норм, штрафов и наказаний, связанных с незаконным оборотом отходов. Согласно расследованиям средств массовой информации, муниципалитеты в различных районах Европы склонны устанавливать неформальные коррупционные связи с преступными группами в сфере оборота отходов в широком смысле и пользоваться их услугами для избавления соответствующих территорий, либо промышленных площадок от отходов.

В настоящее время только 12 стран ЕС присоединились к законодательству ЕС по пресечению трансграничных перевозок отходов и незаконной торговли ими.

Можно четко выделить два уровня экологической преступности, связанных с незаконным оборотом и утилизацией отходов. Первый уровень идентифицируется структурами мафиозного типа, тесно связанными не только с бизнес-структурами, но и с высокопоставленными чиновниками в муниципальных органах власти, включая крупные и крупнейшие города ЕС.

Подобные структуры ведут деятельность на трансграничном уровне и занимаются преступным бизнесом с отходами не только в ЕС, но и за его пределами, создавая сложные технические, организационные и логистические цепочки, охватывающие многие страны. Как правило, подобные структуры занимаются всеми видами отходов, делая особый упор на особо экономически выгодную деятельность с такими отходами. Как отходы химических производств, радиоактивные отходы, отходы биоинженерных предприятий медицинской промышленности, а также отходы, связанные с вредными металлами, такими как ртуть, свинец и т. п.

На втором уровне, который развит повсеместно, действуют организованные группы в составе 3-10 человек, имеющие локальную сферу деятельности. Эти незначительные в глобальном масштабе преступные группы специализируются, как правило, на городских отходах, а также на вышедших из эксплуатации автомобильных аккумуляторов и шин.

Практически повсеместно в экологическую преступность по направлению отходов вовлечен и законный бизнес. Вовлеченность имеет двоякий характер. С одной стороны, законный бизнес предоставляет преступникам услуги, связанные с финансами, поставкой оборудования для переработки отходов, или сам является покупателем отходов для дальнейшей переработки по заниженным ценам, имея в виду преступное происхождение своего сырья. С другой стороны сращивание легального бизнеса с экологической преступностью идет по линии активного участия организованной экологической преступности. в основном первого уровня, для сокрытия различного рода экологических происшествий, ЧП, ЧС, связанных с выбросами вредных промышленных веществ в окружающую среду, загрязнение вод и воздуха, а также нарушение санитарно-эпидемиологических норм. Имеется много свидетельств, что за последние годы преступные синдикаты все чаще решают проблемы легального бизнеса для того, чтобы не допустить привлечения к уголовной или административной ответственности за преступления против окружающей среды, используя для этого коррумпированных чиновников и правоохранителей.

Еще одним фактором, способствующим экспоненциальному росту преступности, связанной с отходами, является отсутствие согласованности в законодательных и технических нормах, в части отнесения веществ и материалов к отходам или к сырью для вторичной переработки. Дополнительным фактором является неотработанность европейского законодательства в отношении не потребительской продукции «секонд хэнд». В результате в течение последних 10 лет, начиная с 2005 года постоянно растет преступный экспорт в страны Восточной Европы и постсоветского пространства, прежде всего, Украину, Белоруссию, Россию списанный в наиболее технически развитых странах ЕС техники, включая транспортные средства, строительную технику, станки и оборудование. В ЕС они оформляются как отходы, т. е. выведенное из эксплуатации оборудование, подлежащее вторичной переработке. Соответственно, компании, списывающие это оборудование, в соответствии с законодательством ЕС и различных стран освобождаются от налогов на продажу устаревшей техники, и более того, получают налоговые вычеты и иные льготы от государств, как стимул обновления. В страны Восточной Европы и постсоветского пространства вывозимая из Европы как отходы для последующей переработки техника реализуется в этих странах, как секонд хэнд.

Особо быстро развивающимся направлением экологического бизнеса является переработка электронных токсичных отходов. В настоящее время на роль ключевого транзитного пункта для трансконтинентального транзита электронных отходов претендует Италия. Эта система действует следующим образом. На Западных Балканах концентрируются токсичные электронные отходы из Западной, Северной и Центральной Европы. Затем они перебрасываются в Южную Италию и оттуда морским путем транспортируются в Африку или Азию для их последующей переработки с извлечением ценных металлов, включая металлы платиновой группы, а также захоронение той части отходов, которые не подлежат переработке. В отличие от других видов бизнеса, бизнес, связанный с электронными отходами, осуществляется неболь-

шими организованными группами, не превышающими 20 человек. раньше картина была иная и с 60-х гг. Прошлого века этот бизнес пыталась подмять под себя организованная преступность первого уровня. Однако в результате успешных операций правоохранительных органов в конце 80-х и в 90-е гг. прошлого века транснациональные синдикаты были разбиты. В результате в XXI веке на этом рынке стали преобладать транснациональные адаптивные, связанные лишь логистикой и финансовыми расчетами сети, состоящие из небольших преступных групп. Также как в любой другой области и в сфере криминала с сетями бороться весьма затруднительно.

Евроюст и организованная экологическая преступность

Для того, чтобы усилить борьбу с серьезной организованной преступностью, на сессии Европейского Совета в Тампере от 15–16 октября 1999 г. было принято решение о создании ЕВРОЮСТА, в состав которого вошли прокуроры, судьи и высокопоставленные представители полиции стран-членов ЕС. В статье 3 постановления ЕС от 28 февраля 2002 г. было указано, что ЕВРОЮСТ в числе своих важнейших задач имеет:

• координацию расследований и полицейских преследований правонарушителей в тех случаях, когда правонарушения имеют отношение к двум или более членам государств-членов ЕС. При этом Евроюст должен:

• стимулировать и улучшать координацию между компетентными органами государств-членов ЕС в части расследований и судебных преследований на основе любого запроса, исходящего из компетентного органа одной из стран-членов;

• совершенствовать сотрудничество между компетентными органами государств-членов путем содействия оказанию взаимной правовой помощи и практической реализации просьб от экстрадиции;

• оказывать любую необходимую помощь компетентным органами государств-членов при проведении ими международных расследований и уголовного преследования преступников, совершивших правонарушения в более чем одной стране.

В отношении организованной экологической преступности Евроюст принял ряд важных инициатив в 2013 г. В ноябре 2013 г. Евроюст и европейская сеть прокуроров по охране окружающей среды провели встречу «На пути к улучшению координации судебного преследования экологического криминала в ЕС и роль Евроюста в Гааге». Целью встречи была дискуссия по обмену опытом и выработке наилучших практик в борьбе с международной экологической преступностью. На встрече было отмечено. что несмотря на экспоненциальный рост экологической преступности и ее возрастающие международные масштабы, судебные органы должным образом не перестроили свою работу, уровень которой не отвечает потребностям. предъявляемым к судебным органам народами Европы. особо была отмечена необходимость резкого улучшения работы в сфере создания совместных баз данных, разведывательных систем и т. п.

В апреле 2013 г. колледж Евроюста утвердил **стратегический проект по экологической преступности**, разработка которого была завершена в ноябре 2014 года. В настоящее время в качестве основных направлений исследовательской и образовательной деятельности колледжа Евроюста выделены:

• оценка состояния сотрудничества в судебной сфере;

• выявление препятствий, мешающих распространению в рамках ЕС лучших практик борьбы с экологической преступностью, накопленных в тех или иных странах;

• анализ правовых документов в части борьбы с экологической преступностью и наказания за соответствующие преступления, как в масштабах ЕС, так и сравнительный анализ юридической практики отдельных стран.

В ноябре 2014 г. Евроюст одобрил окончательный вариант стратегического проекта по борьбе с экологической преступностью. В докладе дано определение экологической преступности как «тяжкие преступления, часто совершаемые организованными преступными группами, включающие в себя, прежде всего, незаконный оборот отходов, незаконную торговлю охраняемыми, исчезающими видами флоры и фауны, загрязнение воды, почвы и воздуха». В докладе в качестве основных видов экологической преступности были признаны: незаконный оборот видов, находящихся под угрозой; незаконный оборот отходов и загрязнение среды обитания.

Применительно к этим трем видам экологической преступности в стратегическом докладе выделены следующие важнейшие аспекты:

• сложность и непроработанность законодательства, касающаяся экологической преступности;

• недостаточный уровень штрафов и продолжительности тюремного заключения за особо опасные для общества и природа экологические преступления;

• недостаточная координация компетентных органов на национальном и международном уровнях;

• трансграничный характер экологической преступности;

• сочетание иерархических и сетевых структур в организованной экологической преступности.

В качестве «возможных решений» отмеченных выше задач ЕВРОЮСТ должен способствовать:

• теснейшему международному сотрудничеству, как в масштабах ЕС, так и между отдельными его членами;

• созданию совместных следственных групп и их взаимодействию с совместными оперативными группами;

• обмен правовой информацией и практикой кодификации экологических преступлений;

• стандартизации интерпретации законодательных актов ЕС в отдельных странах Союза, и сближению размеров штрафов за аналогичны преступления.

Политические последствия и выводы

Экологическая организованная преступность часто имеет транснациональные измерения. Это требует сотрудничества государств-членов ЕС с третьими странами и международными организациями. Экологическая преступность является новым видом преступности, которая меняет традиционное понимание организованной преступности и расширяет его собственно с криминальных элементов на легальные юридические лица, систематически совершающие экологические преступления и маскирующие их тем или иным способом.

Организованная преступность в сфере экологии имеет две основных формы. Во-первых, внутри крупных преступных синдикатов, типа мафии и других организованных преступных группировок, зачастую носящих трансграничный характер, сформированы функциональные группы и подразделения, специализирующиеся на экологической преступности. В этом случае организованная преступность по форме действует подобно трансграничным многоотраслевым корпорациям, где единые командные, финансовые, контрольные, логистические и иные структуры обслуживают специализированные силы деятельности внутри корпорации или преступной организации. Во-вторых, организованные преступники действуют как брокеры, предоставляя узкоспециализированные услуги для многофункциональных международных и страновых преступных организаций для легальных физических и юридических лиц. Экспансия организованной преступности в сферу экологии мотивирована высокой нормой прибыли и относительно низким уровнем риска по сравнению с другими высокодоходными видами высокотех-

нологичной преступности. До сих пор, не говоря об Африке, Азии и Латинской Америки, даже не во всех странах ЕС предусмотрена конфискация активов и доходов от экологических преступлений.

ЕС пока не принял должных мер по борьбе с экологической организованной преступностью. Это, безусловно, важнейшее упущение Союза, поскольку статья 83 договора о функционировании ЕС позволяет его органам принимать директивы в области особо тяжких преступлений, имеющих трансграничное измерение. В будущем Союз может единогласно принять решение относительно добавления серьезных экологических преступлений в список особо тяжелых трансграничных преступлений.

Особый разнобой наблюдается в национальных законодательствах, поскольку международное законодательство отсутствует, по сути, вообще, относительно определения экологической преступности и установления уголовной и административной ответственности за преступления такого рода.

Разведка, базирующаяся на кооперации и сотрудничестве

Успехи в борьбе с трансграничной национальной преступностью решающим образом зависят от создания эффективных информационно-аналитических и разведывательных систем, обладающих максимально полной информацией на преступные, организованные группы, непостоянные преступные группы, преступников-одиночек, а также юридических и физических лиц, прямо или косвенно связанных с ними. Создание такой единой в масштабах ЕС базы требует максимального сотрудничества и кооперации всех стран-членов ЕС, усилий международных органов ЕС и максимально полного использования уже созданных и имеющихся баз данных, информационных систем, компьютерных программ и передовых практик. В настоящее время максимальную эффективность в том направлении продемонстрировали такие страны, как Великобритания, Нидерланды и Италия.

Укрепление институтов, упрочение сетей и повышение эффективности инструментов

В настоящее время ЕВРОЮСТ, ЕВРОПОЛ и Европейская сеть прокуроров по охране окружающей среды ведут свою работу по гармонизации и повышению эффективности взаимодействия правоохранительных и судебных органов, структур прокуратуры в профилактировании, предупреждении и, преследовании и наказании организованной, в т. ч. экологической преступности. В ходе этой работы особое внимание обращается на:

– гармонизацию национального законодательства, за которую отвечает ЕВРОЮСТ;

– вовлечение в борьбу с организованной преступностью других органов государственной власти на всех уровнях, в том числе таможенного и налогового контроля. Эта работа также относится к компетенции Евроюста;

– улучшение действующих практик борьбу с организованной преступностью. Главным направлением является дальнейшая отработка организации и обеспечения эффективной деятельности следственных групп на основе сочетания их действенности и результативности с обязательным соблюдением принципов законности и подотчетности деятельности. За эту работу несет ответственность в первую очередь Европол;

– дальнейшее совершенствование информационных сетей, информационно-аналитических систем и баз данных применительно к организованной преступности вообще и экологической организованной преступности в частности;

– решение вопросов, связанных с рассекречиванием документов по борьбе с организованной преступностью. Поскольку в настоящее время значительные массивы наиболее важных документов в этой области не доступны для научного анализа, а также использования в практике обучения специалистов правоохранительных, судебных и прокурорских органов.

Защита международной цепи поставок медикаментов от угрозы проникновения контрафактных препаратов[33]

По данным Всемирной организации здравоохранения (ВОЗ), распространенность поддельных, ложномаркированных, фальсифицированных или контрафактных лекарственных средств или средств, известных под аббревиатурой SFFC (поддельные/ ложномаркированные/фальсифицированные/контрафактные), выпуск, упаковка и неправильная маркировка которых преднамеренно осуществляется обманным путем, – это растущая тенденция мирового масштаба, которая представляет угрозу для безопасности пациентов и подрывает доверие населения к системам здравоохранения и регуляторным органам, призванным обеспечивать надзор и контроль.

Лекарственные средства SFFC обнаруживаются во всех уголках мира. Они могут быть разными, начиная от случайных смесей вредных токсических веществ и заканчивая неактивными, неэффективными препаратами. Некоторые из них содержат задекларированный, активный ингредиент и обладают таким сходством с подлинным продуктом, что вводят в заблуждение как специалистов здравоохранения, так и пациентов. Но в каждом случае источник лекарственного средства SFFC неизвестен, а его содержание сомнительно. Лекарственные средства SFFC, при всех обстоятельствах, являются нелегальными. Они способны привести к безрезультатному лечению или даже к смерти. Устранение этих средств является в значительной мере сложной задачей для общественного здравоохранения.

О контрафактных препаратах

С проблемой контрафактных препаратов общество впервые столкнулось в середине 80-х годов прошлого века, когда контрафакторы начали копировать легкие препараты, «улучшающие качество жизни», которые использовались для борьбы с ожирением, облысением и т. п., за чем вскоре последовало тиражирование рецептурных препаратов широкого потребления, например, препаратов для предупреждения беременности, лекарственных средств от нарушения эрекции, диабета, гипертонии, повышенного уровня холестерина в крови, а также вакцин, антибиотиков и противомалярийных средств.

Более чем 25 лет спустя объем фальсифицированных препаратов увеличился до такой степени, что стал охватывать дорогостоящие препараты, пользующиеся высоким спросом, а также жизненно важные препараты для лечения рака, ВИЧ/СПИДа, серьезных сердечно-сосудистых заболеваний и даже средств для поддержания органов-трансплантатов. В настоящее время нет такого препарата или лечебного средства, которого бы не коснулось несанкционированное тиражирование. К целевым лекарственным средствам теперь относится целый ряд как фирменных и незапатентованных препаратов (генериков) – от недорогих незапатентованных обезболивающих средств и антигистаминных препаратов до дорогостоящих препаратов, являющихся лидерами продаж, а также специальных лекарственных средств для лечения состояний, представляющих угрозу для жизни. Не избежали фальсификации даже инъекционные лекарственные средства и медицинские устройства.

Согласно статистическим данным ВОЗ, собранным в 2000 году:

---

[33] World Courier; AmerisourceBergen. Июнь 2014 г. (Извлечение). Компания World Courier входит в состав корпорации AmerisourceBergen, является самым крупным и самым опытным поставщиком специализированных курьерских услуг на международной арене. Она позиционируется как единственная в своем роде компания, которая удовлетворяет самым строгим требованиям отрасли по организации международных перевозок скоропортящихся и термолабильных фармацевтических продуктов и исследуемых лекарственных препаратов как для продажи, так и клинических исследований.

• 32,1 % обнаруженных контрафактных препаратов не содержали активных ингредиентов;

• 20,2 % обнаруженных контрафактных препаратов содержали неправильное количество активных ингредиентов;

• 21,4 % обнаруженных контрафактных препаратов содержали неправильные ингредиенты;

• 5,6 % обнаруженных контрафактных препаратов содержали правильные ингредиенты, но имели поддельную упаковку;

• 8,5 % обнаруженных контрафактных препаратов имели высокое содержание примесей;

• 1 % обнаруженных контрафактных препаратов представляли собой копии подлинного продукта.

Последствия применения поддельных препаратов для пациентов могут существенно отличаться от случая к случаю: от неэффективного лечения незначительных симптомов до неэффективного лечения тяжелых заболеваний и до резистентности к лекарственным средствам вследствие продолжительного воздействия активных ингредиентов в уменьшенном количестве и даже до летальных исходов. По разным статистическим данным, от контрафактных препаратов ежегодно умирает от 100 000 до 1 миллиона человек. Выпущенные на объектах, не соответствующих установленным требованиям, где практически отсутствует контроль качества, эти поддельные лекарственные средства содержат ряд сомнительных ингредиентов, в частности, кофеин, крысиный яд, крахмал, мел, гипс, муку, сахар и даже ацетаминофен, используемый для понижения температуры, и порождают представление об эффективном действии препарата.

Распространенность контрафактных препаратов с учетом географических регионов

В современной глобализированной фармацевтической отрасли бытует мнение, что 10 % всех лекарственных препаратов, распространяемых по всему миру, являются контрафактными. Примерно 80 % этих контрафактных лекарственных препаратов производится за границей, а ведущими поставщиками таких препаратов являются Индия и Китай. По подсчетам ВОЗ ежегодно во всем мире продается контрафактных препаратов на сумму свыше 75 миллиардов долларов США, а, по некоторым источникам, годовая рыночная стоимость таких препаратов приближается к 200 миллиардам долларов США. Вполне предсказуемо, что получить точные данные сложно.

Развивающиеся страны исторически были главной мишенью для контрафакторов, отчасти по причине низкого уровня импорта и более слабой инфраструктуры регуляторной системы, но также и в связи со слабостью экономики и отсутствием возможности широкого доступа к дорогостоящим препаратам у значительной части населения. В то время как Азия, население которой составляет 60 % жителей всего мира, в настоящее время представляет собой крупнейший рынок для контрафактов, Африка, Америка и регионы, дестабилизированные в политическом и экономическом отношении, аналогичным образом являются привлекательными мишенями для распространения такой фальшивой продукции. По оценкам ВОЗ, примерно 30 % препаратов, распространяемых на территории этих регионов, являются контрафактными. По приблизительным данным в некоторых странах такие препараты составляют до 60 %. Более того, рост коммерческих продаж лекарственных средств через Интернет – как продукции, предназначенной для развивающихся стран, так и продукции, выходящей из развивающихся стран, – попросту способствовал усугублению данной проблемы.

В промышленно развитых странах, например, в США, Канаде, большинстве стран Евросоюза, Австралии, Новой Зеландии и Японии, где средний доход населения выше, цепь поставок медикаментов лучше защищена более надежной системой таможенных органов, импортного контроля и регуляторного надзора, а деятельность правоохранительных органов является более активной, частота случаев контрафактной деятельности, согласно статистическим данным, сократилась до 1 % или меньше.

Несмотря на то, что этот процент может показаться незначительным, реальные цифры помогают лучше увидеть реальную ситуацию. В одних только Соединенных Штатах количество рецептов, выписанных в 2011 году, составляло более 4 миллиардов, по более чем 40 миллионам из которых были получены контрафактные лекарственные средства. Согласно результатам исследования, проведенного в 2010 г. в 14 странах Европы фармацевтической компанией Pfizer, более 10,5 миллиардов евро (14 миллиардов долларов США) ежегодно тратилось на рецептурные препараты, поставляемые из нелегальных источников, в том числе на средства для похудения, лечения гриппа и нарушения эрекции; многие из этих препаратов были контрафактными. В ходе этого же исследования было отмечено, что количество контрафактных препаратов, обнаруженных в странах, граничащих с Евросоюзом, увеличилось от 560 598 изделий в 2005 году до 4 081 053 изделий в 2007 году.

Судя по всему, данная ситуация будет усугубляться в перспективе и, несмотря на то, что в настоящее время ее проблематичность признали на международном уровне, контролировать эту ситуацию представляется крайне сложной задачей. Например, в 2013 году благодаря совместным действиям международных правоохранительных органов и усилиям почти 100 стран было изъято больше 10 миллионов потенциально опасных лекарственных средств на сумму 36 миллионов долларов США, в связи с чем было арестовано 213 лиц разных национальностей.

Помимо этого, было обнаружено и заблокировано порядка 14 000 веб-сайтов, созданных нелегальными интернет-аптеками, а также проверено более 530 000 упаковок таможенными и регуляторными органами. Из этого количества было изъято почти 42 000 упаковок, в которых содержались все препараты от антибиотиков, лекарственных средств для лечения онкологических заболеваний и антидепрессантов до лекарственных средств при нарушении эрекции и пищевых добавок.

Международное сотрудничество

В 2006 году была создана Международная оперативная группа по борьбе с контрафактной деятельностью в сфере лекарственных препаратов (International Medical Products Anti-Counterfeiting Task Force, IMPACT), партнерское образование, в состав которого вошли представители 193 государств-членов ВОЗ, целого ряда международных и неправительственных организаций, правоохранительных органов, ассоциаций производителей фармпродукции и регуляторных органов. В сферу ее компетенции входит работа со странами и отраслью, направленная на обеспечение более высокого уровня обнаружения поддельных препаратов и защиты от их широкого распространения, а также на минимизацию преступной деятельности посредством более надежной и ориентированной на сотрудничество системы международных правоохранительных сил.

Вместо послесловия
Преступность будущего уже здесь

Преступность как кривое зеркало отражает те социальные, экономические, политические процессы, которые проходят в современном обществе. Отражает самые уродливые формы этих процессов. Криминологи на основе методов математического анализа научились прогнозировать тенденции преступности, сопрягать ее с теми или иными социально-экономическими факторами, на этой основе планировать меры предупреждения преступности. Но одновременно какой-либо структурированный взгляд на образ будущей преступности практически отсутствует. В отечественной криминологии за последние годы можно найти буквально единицы статей, где присутствуют футурологические аспекты. Можно констатировать, что концепции будущей преступности в нашей стране мы не имеем. Да и в целом в мировой криминологии этим проблемам уделяется явно незначительное внимание. Несмотря на то, что сама футурология как наука о предсказаниях будущих тенденций развития представлена весьма значительными исследованиями.

Попытка представить будущее преступности реализована в двух крупных монографиях, изданных в Соединенных Штатах. Одна из них называется «Будущие насилия» (авторы – Бенджамин Уайтс и Габриэлла Блум), а другая – «Будущее преступности», автор последней Марк Гудман длительное время работал в структурах Национального бюро Интерпола США и ФБР, а теперь является одним из главных разработчиков проблем безопасности в «Гугле». Если суммировать эти две книги, то основной принцип можно охарактеризовать фразой американского писателя Уильяма Гибсона о том, что «***будущее уже наступило, просто оно еще неравномерно распределено***». В названных работах подробным и доступным образом рассказано о всех новых тенденциях киберпреступности, преступности в сфере новых технологий в целом. Безусловно, эти работы представляют большую ценность и должны быть изучены всеми криминологами, которые думают о том, как на основе научных знаний усовершенствовать уголовную политику. Для первой стадии футурологического анализа это, безусловно, необходимый элемент. Но дальше мы упираемся в проблемы методологии.

Можно, конечно, бесконечно анализировать те или иные технологические тренды и на их основе смотреть, каким образом отдельные преступники либо преступная организация будут использовать те или иные технологии. Но разве это достаточно для криминологического анализа в его широком научном понимании?

Например, выдающийся американский изобретатель и футуролог Рэй Курцвейл, выступая в апреле 2015 года в Детройте на международном конгрессе по инновациям, подробно, до 2099 года спрогнозировал развитие технологий. От появления системы виртуальной реальности, формирующей изображение непосредственно на сетчатке глаза людей в 2019 году, до наступления эры технологический сингулярности, которая распространится за пределы Земли вместе с человечеством. Имеется в виду эра, где люди и машины сливаются на всех уровнях бытия и над всем этим господствует искусственный разум или искусственный интеллект. Если учесть то обстоятельство, что все предыдущие прогнозы Рэя Курцвейла были осуществлены за последние 15 лет практически год в год, то криминологи безусловно обязаны применительно к такого рода прогнозам выстраивать хоть какое-то подобие прогнозов криминологических.

Можно идти и более широким путем, исходя из познания тенденций развития новой промышленной революции в XXI веке.

Вопросы четвертой промышленной революции, как известно, были главной темой обсуждения на последнем заседании Всемирного экономического форума в Давосе в январе 2016 года. В докладе президента Всемирного экономического форума профессора Клауса Шваба

красной нитью проходит идея о том, что человечество стоит на пороге технологической революции, которая полностью изменит наш образ жизни, работы и коммуникации. По его мнению, первая промышленная революция использовала для механизации производства силу воды и пара. Вторая промышленная революция использовала для конвейерного производства электричество. Третья – автоматизировала производство с помощью электроники и информационных технологий. Четвертая промышленная революция опирается на Третью – с середины прошлого века длится цифровая революция во всех областях жизни. Технологии сливаются, и границы материального, цифрового и биологического миров стираются.

Надо сказать, что до Шваба первыми идею новой промышленной революции в XXI веке развили Джереми Рифкин в своей книге «Третья промышленная революция» и Крис Андерсон в книге «Новая промышленная революция». Неважно, как назвать новый этап промышленного развития. Важно, что это уже не является чисто теоретическим размышлениями, это реальность. В Германии реализуется программа «Индустрия 4.0», которая представляет собой прикладную модель новой промышленной революции. Аналогичные программы разрабатываются во всех развитых государствах, в том числе и в России.

Все названные исследователи отмечают, что человечество никогда в своей истории не наблюдало настолько быстрого технического прогресса. В сравнении с прошлыми промышленными революциями, развивающимися в основном линейно, масштаб новой революции увеличивается в экспоненте. Эта революция влияет на индустрию каждой страны в мире. Глубина и широта вызванных ей изменений требует трансформации целых систем производства, менеджмента и управления. На основе этой новой революции совершаются все новые прорывы в таких областях, как искусственный интеллект, робототехника, интернет вещей, автономный транспорт, 3D-печать, нанотехнологии, создание новых материалов, новых батарей, развитие квантовых вычислений и создание квантовых компьютеров.

В Давосе отмечалось, что новая промышленная революция может глобально поднять мировой уровень жизни. Но в то же время эта же новая революция с большой степенью вероятности усилит финансовое и социальное неравенство в мире, нарушит работу рынков труда. Автоматизация производства приведет к тому, что роботы вытеснят с рынка множество людей.

По прогнозам ученых больше всех от инноваций выиграют интеллектуалы и капиталисты – инноваторы, акционеры и инвесторы. Но одновременно это создаст финансовую пропасть между теми, кто живет за счет труда, и теми, кто живет за счет капитала. Поэтому исследователи предупреждают, что технологический прогресс, как это ни парадоксально, может стать одной из главных причин стагнации, иногда и снижения уровня доходов большей части населения развитых стран. В итоге может образоваться ситуация, когда востребованы будут либо суперспециалисты в новых технологиях, либо совершенно неквалифицированные люди. Что касается середины или то, что называется средним классом, то эта часть населения переживет наибольшее потрясение. Это в свою очередь, по мнению экспертов Давоса, породит распространение экстремистских идей, идеологий. Новая промышленная революция кардинальным образом изменит саму природу национальной и международной безопасности, повлияет как на вид конфликтов, так и на их природу. Границы между войной и миром, солдатом, полицейским, гражданским человеком и даже насилием и ненасилием могут оказаться пугающе размытыми.

Какой мы видим будущую криминальную ситуацию через призму последствий новой промышленной революции? Это следующий этап познания для криминологов в осмыслении образа будущей преступности и разработке мер по готовности действовать в таких условиях.

Но и это еще не конечный результат для футурологического осмысления преступности. Разработчики концепции новой промышленной революции безусловно идут дальше в социальном осмыслении будущего человечества в сравнении с учеными, которые ограничиваются только прогнозированием развития новых технологий.

Для криминологов здесь важны социальные последствия новой промышленной революции. Но можно ли на этом останавливаться? Без целостного прогнозирования социальной реальности будущего? И есть ли такие прогнозы, на которые могут опираться криминологи? Конечно, есть. Достаточно назвать работы известного экономиста и политического деятеля Жака Аттали, особенно его книгу «Краткая история будущего», которая опубликована еще 10 лет назад. Или книгу ведущего аналитика Национального совета по разведке США Мэтью Барроуза «Будущее рассекречено, или Каким будет мир в 2030 году». Когда эти книги появились, особенно работы Аттали, их просто воспринимали как околонаучную фантастику или апокалиптические фильмы Голливуда. Но прошло не так много времени и мы видим, что казавшиеся самыми невероятными негативные сценарии реализуются в жизни. Например, Аттали дает три сценария развития человечества. По первому сценарию, который он называет *гиперимперией* рыночных богатств, деньги покончат со всем, что может помешать их торжеству, включая сами государства, которые они постепенно уничтожат. Все станет частным, включая армию, полицию, судебную власть. Большинство людей превратятся в артефакт для производства и продажи. Если человечество отшатнется от такого будущего, прервет глобализацию силой, наступит варварская эпоха, мир погрязнет в разрушительных войнах. Государства, религиозные объединения, террористические группировки и пираты, используя новейшее оружие, будут истреблять друг друга. Такой ход событий Аттали называет *гиперконфликтом*. Гиперконфликт – это и гиперкриминал на планете. По сценарию Аттали на месте стран, которые распадутся под давлением рынка, появятся пиратские государства и негосударственные образования, зоны беззакония. Ими будут управлять лидеры вооруженных банд, контролирующие регионы, порты, нефтепроводы, дороги и сырье. Пиратские государства будут вести себя по модели обычных государств, сражаться против традиционных государств, обеспечивать свое существование за счет использования труда интеллектуалов. По существу, реализацию этого сценария мы уже видим на примере ИГИЛ, структур Талибана, мексиканских и латиноамериканских картелей. Да и в целом сегодняшняя мировая экономика и политика становятся все в большей мере мафиозной федерацией.

Как пишет Марк Гудман в книге «Будущее преступности», уже сейчас в общей сложности на долю транснациональной преступности приходится от 15 до 20 % мирового ВВП, как чисто преступный оборот, и не менее 25 дополнительно, как легальный оборот, контролируемый преступными группировками. В общем и целом преступные группы контролируют не менее трети, а скорее ближе к половине мирового оборота всех видов товаров, услуг, активов и финансов. С учетом того, что концентрация собственности в преступном мире гораздо выше, чем в легальном бизнесе, можно сделать вывод о том, что крупнейшими собственниками активов и держателями ресурсов на планете являются именно преступные синдикаты.

Между современной и старой преступностью существует не только антагонизм, но и сильная разница в методах и организации преступных синдикатов. Современные группировки в основном отказываются от традиционных иерархических структур времен дона Карлеоне и Тони Сопрано, а представляют собой подвижные сетевые структуры. Они активно используют аутсорсинг, коллективное предпринимательство, платформенные решения и т. п. Одним словом, если преступники до середины XX века плелись в хвосте технических, организационных и финансовых технологий, то сегодня они, несомненно, находятся в авангарде.

К примеру, добыча одного среднего киберпреступника, по данным нью-йоркской киберполиции, в семь раз превышает добычу обычного преступника. В том же Нью-Йорке раскрываемость обычных преступлений составляет в разные годы от 40 до 60 %, а киберпреступлений – 4 %. Иными словами, киберпреступность – это высокодоходная и мало рискованная криминальная деятельность.

Третий сценарий развития Аттали называет *гипердемократией*. Суть которой заключается в приостановке глобализации, в создании единого мирового правительства и нескольких

региональных центров власти. Это наиболее позитивный сценарий развития человечества, при котором каждый человек с помощью новейших технологий сможет жить в достатке, справедливо, беречь окружающей мир и т. п. То есть общество всеобщего благоденствия.

Думается, последний сценарий человечества при жизни ближайших поколений наименее вероятен. Поэтому профессия криминолога еще долгое время будет оставаться востребованной, а криминологические знания входить в систему образования любого вида и любой направленности. Но это лишь при том условии, что криминологи будут адекватно оценивать социальные процессы настоящего и прогнозировать их изменение в будущем.

* * *

Мы живем в ситуации, когда новые формы преступности, связанные с новыми технологиями, уже присутствуют в нашей жизни, а основная полицейская мощь по-прежнему обращена в прошлое.

Это совершенно не означает, что традиционные виды преступности сходят на нет. Наоборот, кризисные явления в экономике, непростые, иногда фатальные миграционные процессы могут порождать и порождают рост так называемой обычной корыстно-насильственной преступности. Да и бытовое насилие, сопровождающее человечество на протяжении всей его истории, сходить на нет не будет. А все это – основная масса регистрируемой преступности. Но, как показывают исследования последнего времени, ущерб и катастрофические последствия применения новых технологий криминальными структурами часто не сопоставим с негативными последствиями преступности традиционной.

В материалах XIII конгресса ООН по предупреждению преступности и уголовному правосудию, который проходил в Катаре в апреле 2015 года, содержатся результаты общемирового исследования, которые показывают, что для населения в целом ***уровень виктимизации в результате киберпреступности существенно выше, чем уровень виктимизации в результате «обычных форм» преступности***.

Делать ставку только на кибербезопасность и полагать, что специалисты кибербезопасности спасут мир, это уже подход из прошлого. Мы имеем дело с гораздо более сложным явлением – ***комплексными высокотехнологическими угрозами***. Информационные технологии являются своего рода платформой для развития всего остального – робототехники, нанотехнологии, биотехнологии, синтетической биологии. Многие исследователи отмечают, что все перечисленные технологические новации могут быть использованы не только террористическими организациями, но и иными криминальными структурами. Ведь грань между терроризмом, гибридными войнами и уголовной преступностью в последние годы стирается. И силовым структурам, обеспечивающим безопасность своих государств, уже порой трудно понять, что первично – действия террористов, мафиозных структур или реализация чьих-либо политических проектов. Фактически стираются юридические границы между войной, терроризмом и преступностью. Ясно одно, что современная технология позволяет относительно небольшим группам террористической, политической или криминальной направленности овладеть разрушительными силами, которые всегда ранее были монополией государства. При этом любой человек, любая финансовая или политическая структура могут быть внезапно атакованы в любое время, в любой точке мира вне зависимости от своего статуса.

Особое распространение новые технологии получают в структурах организованной преступности. С одной стороны, сами сообщества хакеров часто организуются как мафиозные структуры. А с другой стороны, действующие мафиозные структуры переквалифицируются на высокотехнологическую преступность. На уже указанном конгрессе ООН в Катаре отмечалось, что свыше 80 % выявленных в мире киберпреступлений связаны с организованной преступностью.

Европол вообще в своих последних докладах о тенденциях организованной преступности прогнозирует, что в ближайшие годы практически все виды мафиозной деятельности будут опираться на цифровые структуры.

Есть все основания полагать, что несмотря на постоянное самовоспроизводство традиционных видов преступлений, ближайшее криминальное будущее будет коренным образом отличаться от криминального настоящего. В этой связи нельзя не привести результаты исследования бывшего руководителя Департамента политики Министерства внутренней безопасности США Стюарта Бейкера (они опубликованы в вышедшей в этом году в Америке книге «Будущие насилия. Роботы и термиты, хакеры и дроны. Новая эра конфронтации»). Бейкеру на основе компьютерного анализа удалось рассчитать цикл зависимости социальных волнений от появления и развития новых технологий. В основе его цикла находится два параметра: снижение цены коммерческого использования технологии и масштабы ее распространения. Выяснилось, что последние 120 лет прослеживается прямая зависимость между этими двумя параметрами и количеством преступлений (а также их вредоносностью), совершаемых с использованием соответствующей технологии.

В соответствии с циклами Бейкера мир и особенно промышленно-развитые страны ждет просто вал высокотехнологической преступности и близких к ней негативных явлений. Либерально-настроенные американские ученые в этой связи приходят к неожиданному для них самих выводу о том, что пока этот вал не накрыл всех с головой, необходимо изменить политику, законодательство, отказаться от многих привычных ценностей, включая свободы и неограниченный рынок. Девиз нового времени – это контроль, превентивность, распределенность функций и полномочий на всех уровнях.

Это не означает, что кто-то предлагает сдерживать технологический процесс. Если технологии не развиваются, то общество деградирует, какой бы жесткий режим в нем ни был установлен. Поэтому вся сложность ближайшего времени и в мире, и у нас в стране будет заключаться в том, что одновременно необходимо будет интенсифицировать процесс развития новых технологий, без которых немыслима начавшаяся новая промышленная революция. И одновременно жестко сдерживать террористические и криминальные угрозы, сопутствующие этим технологиям.

Теперь о нескольких конкретных прогнозах для нашей страны.

Первое. Кризисные явления в экономике, сложности вхождения в новую промышленную революцию увеличат напряженности на рынках труда, межнациональных отношениях, в мигрантской среде. Все это не может не повлиять негативным образом на рост как традиционных, так и нетрадиционных видов преступлений. Никуда не уйдет, а только будет возрастать доля корыстных и корыстно-насильственных преступлений в общей структуре преступности. Не только в ближайшие годы, но и в ближайшие десятилетия.

Второе. Правоохранительным органам в условиях дефицита финансовых средств на их существование придется вести борьбу на этих двух направлениях – традиционном и нетрадиционном. Причем, уже ясно сейчас, что вся правоохранительная система будет постоянно запаздывать в своих ответных действиях на технологизацию преступного мира. Чтобы это запаздывание не было столь явным, необходима коренная перестройка всей системы подготовки кадров правоохранительных структур, их набора. По существу в ближайшее десятилетие вся полиция должна стать одновременно киберполицией, использующей новейшие достижения в работе с Большими данными в передаче информации, ее визуализации.

Третье. Следует при раскрытии преступлений совершенно изменить систему использования новых технических средств получения объективной информации о виновности того или иного подозреваемого лица. Использовать под врачебным и прокурорским надзором медицинские средства, которые в журналистской среди получили название «сыворотка правды». Активно применять детекторы лжи нового поколения. Современная нейробиология уже сейчас

позволяет практически на 100 % устанавливать правдивость тех или иных показаний. Пытки, психологическое давление, унижение, следственные комбинации во многих случаях должны быть заменены технологическими инновациями.

Четвертое. Должны уйти архаичные, пещерные способы расследования уголовных дел, написание и чтение сотен томов этих дел, без машинной обработки, особенно по делам экономической направленности, организованной преступной деятельности.

Пятое. Необходима революция в экспертной деятельности. Уже сейчас новейшие открытия по целому ряду направлений науки требуют их использования в той сфере, которую мы традиционно называем криминалистической экспертизой.

Шестое. Технологическая революция предполагает, что сами правоохранительные органы должны перестраивать свою работу с учетом новых технологий. Требует самого пристального внимания ***работа с Большими данными***. Как известно, аналитика Big Data позволяет вычленить из потока самой разнообразной информации необходимые точечные сведения для принятия решений в сфере обеспечения безопасности. С помощью технологий Big Data возможно вычленять информацию о готовящихся терактах, отслеживать вспышки насилия и этнические конфликты, искать преступников с помощью анализа видеопотока с камер наблюдения. Как известно, в Соединенных Штатах и Европе уже функционируют так называемые системы упреждающей полиции, работа которой все больше основывается на развитии интеллектуальных систем по анализу Больших данных, которые самостоятельно сопоставляют релевантную информацию и делают из нее выводы о повышении криминальной активности в тех или иных районах или о связях определенных людей с теми или иными криминальными организациями.

Для внедрения таких систем прежде всего требуется наведение порядка в криминальной статистике, использование для подготовки алгоритмов принятия решений всего потока информации о заявлениях и сообщениях о преступлениях и иных правонарушениях.

Седьмое. Борьба с высокотехнологическими преступлениями требует постоянного укрепления международного сотрудничества. Особенно важным в этом отношении может оказаться участие в координации поддержки транснациональных расследований таких структур, как ***Глобальный инновационный комплекс Интерпола, открытый в 2015 году в Сингапуре и Европейский центр по борьбе с киберпреступностью Европола***.

Восьмое. Не может оставаться такой архаичной судебная система. Приговоры по конкретным делам должны одновременно основываться на глубоком психолого-психиатрическом исследовании всех обвиняемых с составлением прогнозов их индивидуального постпреступного поведения. И только на этой основе в XXI веке могут назначаться те или иные виды наказаний. Пока наше уголовное судопроизводство, система исполнения наказаний практически никак не сопряжены с технологической реальностью.

В скором времени мы можем оказаться в ситуации, когда преступники будут использовать квантовые исчисления, а мы по-прежнему прокалывать дыроколом и подшивать многотомные уголовные дела.

В. Овчинский, доктор юридических наук