В.Н.Трофимов

Применимость международного права к киберпространству: иллюзия или реальность?

Москва
ЮСТИЦИНФОРМ
2021

Центр международной информационной безопасности
и научно-технологической политики МГИМО (У)
МИД РФ

УДК 341
ББК 67.91
Т 76

Т 76. **Трофимов В.Н.,** действительный член РАЕН, д.ю.н.
Применимость международного права к киберпространству: иллюзия или реальность? / В.Н. Трофимов. – М.: Юстицинформ, 2021. – 182 с.

ISBN 978-5-7205-1729-8

Решение Генассамблеи ООН о разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях вызвало серьезные споры о принципиальной возможности урегулирования порядка использования Интернета с помощью международно-правовых средств. Данная книга посвящена детальному исследованию возможностей регулирования международных отношений, в том числе применительно к информационной среде, с помощью различных средств, как силовых, так и правовых. По мнению автора, повышению эффективности использования международного права мешают некоторые неточности в понимании его места среди других средств регулирования международных отношений.

Отдельный раздел в книге посвящен исследованию угроз, связанных с использованием информационных технологий. По мнению автора, в определенной мере пока еще недооцениваются угрозы, возникающие из самого факта использования ИКТ. Видимо, основные заблуждения касаются оценки природы естественного интеллекта при создании искусственного интеллекта.

УДК 341
ББК 67.91

ISBN 978-5-7205-1729-8

Связь с автором: dialog-partner@list.ru

Оглавление

Введение

Информационно-коммуникационные технологии (ИКТ) решительно вошли в нашу жизнь. Интернет, телевидение, мгновенная связь через континенты, приборы самого разного назначения. При этом такие технологии стали доступны для самого широкого круга пользователей, они перешагнули государственные границы и, без преувеличения, вошли почти в каждый дом. Преимущества использования устройств, действующих на основе информационно-коммуникационных технологий, очевидны: для того чтобы найти нужную книгу, не надо идти в библиотеку. Мало того, можно воспользоваться книгами из библиотек других государств. Можно играть на бирже, не выходя из дома. Есть возможность поставить диагноз и проконсультироваться с врачом, не покидая квартиры или даже не вставая с постели. Совсем иным стало освоение Космоса. Нелишне сказать и о возможностях, которые используются при решении военных задач.

Однако вместе с преимуществами, связанными с ИКТ, пришли и новые проблемы. Возможностями Интернета стали пользоваться террористы и иные преступники. Некоторые государства, используя такие технологии, активно вмешиваются во внутренние дела других стран, организуя беспорядки, "цветные" революции. Совсем иными стали технологии шпионажа, кражи государственных и коммерческих секретов. Тут уместно упомянуть слова Президента России В. Путина, высказавшегося в отношении искусственного интеллекта: это не только будущее человечества, но и колоссальные угрозы. И тот, кто станет лидером, тот будет властелином мира.

В наше время сложилась определенная асимметрия доступа к научным достижениям, которая ведет к закреплению неравенства в мире, порождает яростную борьбу за обладание передовыми технологиями. Как пример: "цифровой разрыв" – неравномерное развитие информационных технологий между различными странами, географическими регионами.

Конечно, государства принимают меры, чтобы противодействовать нежелательному использованию ИКТ, разрабатываются новые законы, внедряются в жизнь технологии противодействия преступникам и террористам. Идет активная подготовка специалистов соответствующих профилей, способных эффективно бороться с новыми угрозами.

При этом усилий на национальном уровне явно недостаточно, ИКТ легко пересекают границы, позволяют преступникам действовать быстро и анонимно. Актуальными стали коллективные действия государств, использование возможностей международных организаций. На повестке дня стоят вопросы разработки новых многосторонних международных соглашений, позволяющих объединить и скоординировать усилия многих стран для защиты своих интересов от нежелательных и тем более преступных попыток злоупотреблять ИКТ.

Определенные успехи тут уже есть: в ООН регулярно обсуждаются проблемы Интернета, ИКТ в целом, принят целый ряд резолюций ГА ООН. В двусторонних отношениях приняты декларации, в которых сформулированы ориентиры международного сотрудничества на ближайшие годы. Россия заключила двусторонние соглашения с рядом государств, касающиеся информационной безопасности. Заключены многосторонние договоры в рамках международных организаций, в которых участвует Россия. Наконец, в декабре 2019 года принята резолюция ГА ООН о разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Так каковы же дальнейшие направления и перспективы противодействия угрозам злоупотребления ИКТ? Какова может быть тут роль международного права, международных договоров? Данная монография посвящена именно этой теме. Однако нельзя эффективно использовать международное право без предварительного внимательного изучения самого предмета регулирования: ИКТ. Что это за явление по своей природе? Насколько такие технологии безопасны сами по себе? Нет ли тут специфических скрытых угроз, способных нанести серьезный ущерб как интересам государств, так и отдельных людей? Исследованию этих вопросов также посвящен отдельный раздел монографии. При этом автор считает уместным ссылаться не только на уже общепризнанные теории и концепции, но и на гипотезы, пока не получившие общего признания. Такой подход, по мнению автора, позволит принять во внимание более широкий круг проблем, связанных с обеспечением безопасности использования ИКТ.

Глава 1. Международное право

1. Высшие инструменты регулирования международных отношений

Прежде чем обозначить роль международного права при обеспечении безопасности использования ИКТ (в том числе и безопасность в киберпространстве), представляется необходимым более внимательно рассмотреть некоторые общие вопросы, касающиеся международного права. От правильного понимания этих вопросов будет во многом зависеть и успешное использование международного права как средства обеспечения информационной безопасности. Является ли вообще международное право высшим инструментом регулирования международных отношений, или его роль более скромная и ограниченная? Как представляется, в научном сообществе в отношении этого вопроса нет окончательной ясности. Попробуем разобраться.

Нередко последовательность шагов по выработке международно-правовых норм в ситуации, когда применялась сила (в том числе вооруженная сила), следующая: в международных отношениях возникает проблема, и государства пытаются ее решить, в том числе прибегая и к силовым методам. В конце концов, наступает какая-то более или менее стабильная ситуация (по итогам войны подписан акт капитуляции; силовые действия прекращены в связи с тем, что ни одна сторона не может добиться полной победы; попытки решить проблему силой не увенчались успехом; шантаж и давление, в том числе угроза применения силы не сработали и т.д.). В результате представители государств садятся за стол переговоров и вырабатывают некие правила поведения применительно к возникшей проблеме. Эти правила могут быть сформулированы в виде международного договора, нередко подлежащего ратификации. Вот, казалось бы, и торжество международного права, сыгравшего завершающую роль в урегулирования проблемы, которую первоначально пытались решить с использованием силы. Роль, действительно, завершающая. Но не решающая, что важно. Весь описанный процесс вовсе не доказывает, что международное право – это высший инструмент регулирования международных отношений.

2. ООН

Рассмотрим еще одну, на этот раз не предполагаемую, а вполне конкретную ситуацию: закончилась Вторая мировая война, нацистская Германия и ее союзники потерпели сокрушительное поражение. По итогам войны у государств-победителей сформировался более или менее общий подход, как дальше регулировать международные отношения и не допустить новой мировой войны. Этот общий подход был оформлен, в частности, в виде Устава ООН[1]. При этом была создана международная организация (ООН), которой государства-члены делегировали часть своих полномочий. В рамках ООН был создан Совет Безопасности ООН, который может применить силу в целом для поддержания международного мира и безопасности и в частности – против конкретного государства-агрессора. При этом ясно, что у ООН есть собственная правосубъектность, которая отличается от правосубъектности отдельных государств[2]. Внешне все выглядит так: существуют отдельные государства со своими правами и обязанностями, а отдельно существует международная организация со своей правосубъектностью, способная применить силу на основе коллективной воли государств-членов и стоящая в результате как бы выше отдельных государств. Если какое-то государство противоправно применит вооруженную силу, совершив тем самым акт агрессии, в таком случае собирается Совет Безопасности ООН и принимает соответствующее решение. Это могут быть, например, экономические санкции, но не только: СБ ООН может принять решение применить против такого государства-агрессора и вооруженную силу. При этом вооруженные силы ООН будут формироваться из вооруженных сил государств-членов, но будут иметь статус международных сил. Казалось бы, вот оно, торжество высшей силы международного права, нашедшее свое выражение в виде Устава ООН.

Попробуем подробнее разобраться в этой ситуации. Международное право в целом запрещает применение вооруженной

---

[1] Устав Организации Объединенных Наций и Статут Международного Суда. М., Международные отношения, 1998.

[2] *Крылов С.Б.* Материалы к истории Организации Объединенных Наций: Создание текста устава Организации Объединенных Наций. М., Л.: Изд-во АН СССР, 1949. Вып. 1. 343 с.

силы, особо обозначая противоправность агрессии. Помимо Устава ООН, Генассамблея приняла, в частности, резолюцию "Определение агрессии", которая более или менее подробно описывает, какие именно действия следует рассматривать как акт агрессии[3]. Более того, резолюция констатирует право государств на индивидуальную и коллективную оборону в случае агрессии.

Тем не менее, несмотря на упомянутые международно-правовые документы, некоторые страны время от времени прибегают к применению вооруженной силы, причем далеко не всегда в целях самообороны, при этом игнорируют возможность использовать процедуры и действия, предусмотренные применительно к СБ ООН. В этой связи можно упомянуть бомбардировки Югославии в 1999 году, а также так называемую операцию "Буря в пустыне" в 1991 году, проведенную в отношении Ирака. Таких примеров, к сожалению, немало, но ограничимся этими двумя, этого будет достаточно. Обе военные операции не были санкционированы Советом Безопасности ООН, то есть по международно-правовым меркам были противоправными. Однако СБ ООН не принял в этой связи никаких решений в целях пресечения указанных действий и наказания государства-нарушителя.

Итак, с одной стороны, международное право запрещает подобное применение вооруженной силы. С другой стороны, несмотря на запрет, сила используется. Мало того, в конечном итоге в этих двух описанных случаях к странам, прибегшим к применению вооруженной силы в обход механизмов, предусмотренных Уставом ООН, не применялись никакие санкции, то есть эти страны, по сути, не понесли никакой международно-правовой ответственности.

3. Особое положение некоторых стран. Постоянные члены СБ ООН

Важно отметить, что в двух упомянутых примерах вооруженная сила применялась Соединенными Штатами Америки и их союзниками, в том числе по военному блоку НАТО. Это важное обстоятельство, которое следует учитывать для правильного понимания ситуации.

---

[3] *Бухмин С.В.* Агрессия: международно-правовые аспекты // Вестник ТГУ, серия Гуманитарные науки. Вып. 4 (36). 2004. С. 96.

Значит ли это, что США, в отличие от других государств, имеют право безнаказанно применять вооруженные силы, пренебрегая требованиям Устава ООН? Какова же в таком случае роль международного права? Может быть, оно – обязательное для любых государств, кроме США и их союзников?

Конечно же, международное право устанавливает обязательные правила, в том числе и по вопросам международной безопасности, распространяющиеся на любые страны, в том числе и на США с союзниками. Но при этом международное право является лишь одним из инструментов регулирования международных отношений, но вовсе не высшим инструментом. В качестве такого высшего инструмента, к сожалению, пока выступает применение силы, в том числе вооруженной, а также угроза ее применения[4]. Хорошо это или плохо, отдельный вопрос. Но пока человеческое общество устроено именно так. Применение силы является крайним средством, к которому подчас прибегают субъекты международных отношений.

Что следует понимать под "крайним средством"? Например, перед государством стоит серьезная проблема, которую оно вынуждено решать. Если не решать, может возникнуть, например, внутренняя политическая напряженность и даже нестабильность. Но многократные попытки решить эту проблему с помощью международного права и предусмотренных им механизмов не дают никаких результатов. Что делать? Безвыходная ситуация? Есть крайнее средство: война. Тут важно отметить, что применение силы является крайним средством вне зависимости от того, являлось ли такое применение силы правомерным или нет. Правомерные случаи применения силы – это, в частности, самооборона и справедливая война. Если государство подверглось агрессии, у него может не быть альтернативы в виде использования механизмов международного права. Нередко единственное (крайнее) эффективное средство остановить агрессора – это тоже применение вооруженной силы.

Конкретный, возможно, не самый удачный, но свежий пример: война Азербайджана и Армении осенью 2020 года за Нагорный Карабах. Переговоры и попытки урегулировать эту проблему в рамках международного права длились десятилетия, но оказались безуспешными. А внутри Азербайджана тем временем нарастала политическая напряженность в связи с ее нерешенностью. Наконец

[4] *Трофимов В.Н.* Военная и экологическая безопасность. Международное право и сила. М.: Прометей, 1991. С. 106–114.

руководство Азербайджана решило, что дальше тянуть нельзя. При этом у Азербайджана оставалось единственное и крайнее средство – применить вооруженную силу, вне зависимости от того, будут ли такие действия признаны правомерными или нет.

Действительно, было ли такое применение вооруженной силы правомерным? СБ ООН не санкционировал подобные действия. При этом не исключено, что еще не были до конца исчерпаны средства, предусмотренные международным правом. Однако следует учитывать, что Азербайджан не просто пытался захватить вооруженным путем Нагорный Карабах и прилегающие к нему территории, он их возвращал в свой состав после того, как они были отторгнуты другим государством с помощью силы. Иными словами, вряд ли можно было говорить об акте агрессии. Но был ли это случай справедливой войны? Наверное, на этот вопрос нет однозначного ответа. Турция поддерживала азербайджанские вооруженные силы. Значит, с точки зрения Турции, война была справедливой. Однако многие государства требовали прекратить вооруженные действия. Значит, с их точки зрения, война не была справедливой и это не была самооборона.

Важно подчеркнуть, что использование запрещенных международным правом средств регулирования международных отношений не является универсальной и общепризнанной практикой. Такие действия иногда позволяют себе только те государства, которые полагают, что к ним не удастся эффективно применить какие-либо средства принуждения или наказания. Именно поэтому чаще всего в такой роли выступают США. Экономический и военный потенциал, наличие большого числа военных союзников позволяют этой стране почти безнаказанно вмешиваться в дела других государств, угрожать применением силы, а то и применять ее. Через механизмы ООН невозможно принять решение о применении к США мер принуждения, учитывая формальные возможности этой страны в Совете Безопасности ООН (статус постоянного члена и право "вето").

По сути, в такой ситуации запрещенные международным правом действия против других государств могут позволить себе и ближайшие союзники США, полагающиеся на соответствующую поддержку в СБ ООН (например, действия ряда европейских государств против Ливии[5]).

[5] См., например: *Репешко Е.А.* Подход НАТО к разрешению ливийского кризиса в событиях "Арабской весны" // Вестник МГИМО. 2014. № 1 (34). С. 172–176.

Попробуем подробнее разобрать ситуацию, касающуюся соотношения права и силы. Допустим, какое-то государство прибегло к применению вооруженной силы, причем явно противоправно. То есть формально с точки зрения международного права – это государство-агрессор. По этому поводу собирается Совет Безопасности ООН. Для того чтобы формально признать указанное государство агрессором и применить в отношении него санкции или даже вооруженную силу, СБ ООН должен принять решение. Для этого необходимо набрать простое большинство голосов членов СБ ООН, но ни один из постоянных членов СБ ООН не должен возражать. Таким образом, если государство-нарушитель само не является постоянным членом СБ ООН или не является близким союзником постоянного члена СБ ООН, в отношении него в полном соответствии с требованиями международного права (в соответствии с Уставом ООН) будут предприняты какие-то меры принуждения.

Если же государство-нарушитель само является постоянным членом СБ ООН, то этот орган по вполне понятным причинам (право "вето") никогда не сможет признать его агрессором. Как известно, постоянных членов СБ ООН пять: США, Китай, Франция, Великобритания и Россия. Точно так же если одно из государств – постоянных членов СБ ООН сочтет, что страну-нарушителя не следует наказывать с помощью средств, предусмотренных в Уставе ООН, Совет Безопасности и в этом случае не сможет принять никакого решения. Иными словами, по формальным причинам СБ ООН не сможет принимать обязательное решение в отношении государства-нарушителя, если таким нарушителем является одна из стран – постоянных членов или кто-то из ее союзников.

Подчеркнем, что мы выше описали формальную ситуацию, которая может не совпадать с фактическим положением вещей. Статус постоянного члена СБ ООН не является чем-то бесконечно незыблемым. Если один из постоянных членов СБ ООН будет слишком злоупотреблять своим статусом, может сложиться ситуация, когда остальные страны придут к выводу, что такой статус следует отменить. Хотя такого прецедента еще не было, но исключать подобную возможность никак нельзя. Если четыре постоянных члена СБ ООН выступят за отмену такого статуса, а остальные члены ООН их поддержат, такое решение может быть принято. Грубо говоря, в таком случае полицейский у входа просто перестанет пускать в соответствующее помещение ООН представителя такого государства,

вот и все. И такому государству останется только возмущаться и рассылать дипломатические ноты в разные инстанции. Никакого реального способа изменить такое решение у него не будет.

Конечно, пока расклад сил в ООН таков, что угроза лишиться статуса постоянного члена существует, пожалуй, только в отношении России. Китай – слишком крупная держава. США, Франция и Великобритания и вовсе являются союзниками по блоку НАТО. Возможно, когда-нибудь потом расклад сил может измениться, но пока ситуация именно такая. Это значит, что выходить за пределы требований международного права могут не только США, но и Россия. Но ей при этом, дабы не рисковать потерять статус постоянного члена (а так вопрос уже ставился, пусть и неформально), желательно предварительно заручиться поддержкой хотя бы еще одного постоянного члена СБ ООН, например, Китая[6].

А какой была бы ситуация, если представить на мгновение, что Организация Объединенных Наций вообще не существует? Видимо, особо существенных изменений не будет. Если какая-то страна совершит акт агрессии, остальное сообщество государств сможет наказать нарушителя, применяя силу или экономические рычаги, лишь в том случае, если это в принципе будет возможно. А возможно это будет только тогда, когда агрессор не обладает значительным военным или экономическим потенциалом, чтобы дать отпор другим государствам. А иначе агрессор просто проигнорирует экономические санкции или даже эффективно на них ответит. Ситуация будет аналогичной, даже если страна-нарушитель будет слабой в военном или экономическом плане, но окажется близким союзником, например, сверхдержавы, которая окажет ей покровительство. А если сверхдержава по каким-то причинам заступится за страну-нарушителя, не являющуюся ее союзником? И в этом случае агрессия, скорее всего, останется безнаказанной.

[6] См., например: *Хоу Лицзюань.* Сотрудничество России и Китая в рамках ООН // Вестник Московского университета. Серия 12. Политические науки. 2010. № 5. С. 114–115; *Ян Юйхэн.* К вопросу о сотрудничестве КНР и РФ в ООН в XXI в // Гуманитарные, социально-экономические и общественные науки. 2015. № 8. С. 101–107.

4. Ядерное оружие

Значительный военный потенциал – это не только большая армия. Некоторые страны обладают ядерным оружием, и тут показателен пример: КНДР[7]. Страна экономически не слишком большая, армия у нее по численности тоже не выдающаяся. Не исключено, что против этой страны могли быть применены не только экономические санкции, но и вооруженная сила. Но этого не случилось, скорее всего, именно потому, что КНДР обладает ядерным оружием и способна нанести неприемлемый ущерб тому, кто попытается прибегнуть к военным методам[8].

Подведем итог: человечество осуждает силовые методы решения международных проблем и регулирования международных отношений. Это осуждение ясно зафиксировано в соответствующих международно-правовых документах, в том числе имеющих обязательную силу. Но обеспечить, чтобы все государства соблюдали этот запрет, пока невозможно. Некоторые страны противоправно нарушают запрет, понимая, что наказания не последует. При этом остальные государства не могут действовать подобным образом, не обладая достаточными для этого политическими, военными или экономическими возможностями.

Итак, фактически силовые методы пока стоят выше других способов регулирования международных отношений, в том числе и международно-правовых. Грубо говоря, пока, к сожалению, сила стоит выше права[9]. Следует также понимать, что сила является крайним, хотя нередко противоправным средством, к которому государство может прибегнуть для решения каких-то проблем.

Вышеприведенные примеры касаются только вопросов применения к государству-правонарушителю вооруженной силы и экономических санкций. Но, конечно же, это не единственные средства для подобных ситуаций. На государство-агрессора можно пытаться воздействовать и

---

[7] *Дьячков И.В.* Влияние ядерной проблемы КНДР на безопасность в Северо-Восточной Азии // Вестник ТГУ. 2012. № 5. С. 308–314.

[8] *Боженова О.О.* Американо-северокорейские отношения на рубеже XX–XXI веков в контексте денуклеаризации Корейского полуострова // Столыпинский вестник. 2020. № 2. С. 483–488; *Поленова А.Л.* Внешняя политика КНДР в децентрализованной системе международных отношений // Восточная Азия: прошлое, настоящее, будущее. 2020. № 7. С. 124–132.

[9] *Трофимов В.Н.* Военная и экологическая безопасность. Международное право и сила. М.: Прометей, 1991. С. 17, 105.

иначе, например: создать информационное давление, принимать в рамках ООН документы, не имеющие обязательной силы (резолюции ГА ООН), использовать судебные механизмы и т.д. Тут, однако, надо понимать, что эти другие средства, как правило, являются менее эффективными, нежели вооруженная сила и экономические или политические санкции.

Применение вооруженной силы – это крайнее средство. Кроме нее государства пытаются регулировать международные отношения с помощью достаточно широкого набора других способов и инструментов. Среди них как традиционные общепризнанные (например, международное право, международные переговоры), так и достаточно специфичные, при этом либо прямо запрещенные международным правом, либо не запрещенные, но осуждаемые международным сообществом. Например: информационная война, недружественные акции, санкции, вмешательство во внутренние дела других государств, угроза применения силы, проба сил, применение силы (помимо применения вооруженной силы), подкуп и шантаж иностранных должностных лиц, ложные обещания, использование агентов влияния, двойные стандарты[10] и др. Часть из этих средств нередко обозначается термином "мягкая сила".

Понятно, что в тех ситуациях, когда некоторые государства противоправно применяют вооруженную силу, избегая какой-либо ответственности, они точно так же используют и иные средства из вышеприведенного списка, запрещенные международным правом. К сожалению, современная международная практика именно такова. Сила стоит выше права, и происходит это из-за злоупотребления соответствующими государствами своим политическим, экономическим или военным статусом.

5. Стабильное состояние международных отношений и международное право

Нужно учитывать, что международные отношения в различные периоды времени находятся в разном состоянии. Если это состояние

[10] *Ковалев В.В., Магомедов М.Г., Самыгин С.С.* Практика двойных стандартов в мировой политике: угрозы национальной безопасности России // Гуманитарные, социально-экономические и общественные науки. 2016. № 6–7. С. 55–60; *Ноздрин А.В.* Политика двойных стандартов в международных отношениях // Актуальные проблемы современных международных отношений. 2013. № 1. С. 79–83.

стабильное, причем достаточно продолжительное время, то участники международных отношений действуют, как правило, в соответствии с взаимно согласованными нормами международного права. В такие периоды может сложиться впечатление, что именно международное право и является высшим инструментом регулирования международных отношений. Такое стабильное состояние возможно, например, тогда, когда складывается более или менее устойчивый баланс сил между основными игроками (сверхдержавами, группами государств) [11].

Когда соотношение сил из-за каких-то причин меняется, начинается передел сфер влияния, изменение в целом мирового порядка. В такие периоды времени на первый план могут выйти силовые методы, вплоть до применения вооруженной силы, которые и будут определять новый международный порядок.

6. Переговоры

Конечно же, верховенство вооруженной силы вовсе не означает, что по любому поводу соответствующие государства прибегают именно к военным методам. В современную эпоху благосостояние наций определяется не столько захватнической политикой, сколько эффективностью экономики. Промышленное и сельскохозяйственное производство, торговля, в том числе и международная, конечно же, требуют стабильного состояния, более или менее предсказуемой ситуации на какой-то разумный по продолжительности период времени. В этой связи те или иные государства, полагающиеся на свою экономическую или военную мощь, тем не менее, как правило, не прибегают немедленно к применению вооруженной силы, а используют другие средства, служащие той же цели, но не связанные с непосредственным применением оружия. Среди этих средств можно назвать следующие: международные переговоры, проба сил, угроза применения силы. Рассмотрим эти средства поподробнее.

---

[11] См., например: *Будаева С.В., Дэцзидэма.* Баланс сил как общий принцип равновесия в современных международных отношениях // Вестник ЗабГУ. 2014. № 9. С. 73–79; *Лукин А.Л., Литтл Р.* Баланс сил в международных отношениях: метафоры, мифы и модели (реферат) // Полит. наука. 2011. № 2. С. 258–265; *Богданов А.Н.* "Американская однополярность" и системный баланс сил в начале XXI в // Вестник Санкт-Петербургского университета. Политология. Международные отношения. 2015. № 2. С. 96–07; *Трофимов В.Н.* Военная и экологическая безопасность. Международное право и сила. М.: Прометей, 1991. С. 103–105.

Нередко международные переговоры рассматриваются как часть процесса согласования тех или иных международно-правовых договоренностей. Но переговоры могут быть использованы и в иных целях[12]. Например, какое-то государство намерено изменить международную ситуацию, но ссылки на международно-правовые нормы не помогают. Или же претензии на такие изменения никак не следуют из международно-правовых норм, а то и противоречат им. Тогда такое государство может предложить соответствующей стране или странам провести международные переговоры. В ходе таких переговоров оно будет пытаться убедить других участников, что сложившееся соотношение сил таково, что им лучше уступить, не доводя до применения вооруженной силы. Конечно, в какой-то мере такие попытки можно рассматривать как международный шантаж и угрозу применения силы. Но возможны переговоры и без угроз и шантажа, а лишь как способ довести до других стран свою позицию и реальную расстановку сил.

7. Проба сил

Конечно, переговоры в силу разных причин могут оказаться безрезультатными. Либо другие страны усомнятся в реальной возможности применить к ним силу, либо будут надеяться на помощь других государств, либо просто будут переоценивать свои возможности. В таком случае страна, все еще полагающаяся на силовые методы, может применить так называемую "пробу сил". Суть такой пробы сил заключается в том, что сила реально применяется, но в ограниченном масштабе. В результате другие страны в ходе достаточно ограниченного конфликта могут, например, убедиться, что союзники их не поддерживают, а сами они не способны противостоять военному нажиму. В результате такой пробы сил можно добиться существенных уступок, не прибегая к полномасштабной войне.

Нужно иметь в виду, что применительно к пробе сил речь может идти не только о попытках ограниченными силовыми методами (в том числе с использованием вооруженных сил) прощупать возможности

[12] *Щербак И.Н.* Международные переговоры в контексте глобального управления // Современная Европа. 2017. № 3 (75). С. 143–145; *Лебедева М.М.* Международные переговоры как социальный и гуманитарный ресурс в мировой политике // Полит. наука. 2020. № 3. С. 98–113.

противника. Возможны и иные формы этого метода. Например, в 2019 году США попробовали не выдавать въездные визы некоторым членам российских делегаций, направлявшихся в Нью-Йорк для участия в мероприятиях, проводимых в рамках ООН[13]. Казалось бы, речь шла просто о явно неправомерных недружественных действиях, направленных против России. Ведь, как известно, Соединенные Штаты при создании ООН приняли на себя обязательства обеспечить дипломатам стран-членов этой организации беспрепятственный доступ в ее штаб-квартиру. Невыдача виз прямо противоречила таким обязательствам. Но не исключено, что такие действия не были просто недружественными. Возможно, что таким способом США пытались прощупать реакцию других стран на возможность ограничения прав России в Организации Объединенных Наций. Если бы другие страны не осудили США, это показало бы, что есть практическая возможность и вовсе пересмотреть статус России в ООН, а точнее – статус постоянного члена СБ ООН.

8. Несовершенство принимаемых человеком решений. Ошибка

Тут в качестве небольшого отступления нужно отметить, что в идеальном случае война вообще не существовала бы как явление, если бы стороны потенциального конфликта могли точно оценивать ситуацию и при этом действовали рационально. Поясним, что имеется в виду. Итак, начались переговоры. Государство, предполагающее, что оно сильнее, подробно разъясняет новую расстановку сил, описывает состояние своей армии и экономики. И предлагает изменить существующий порядок, установив какие-то новые правила. Другая сторона в такой ситуации теоретически могла бы реально оценить свое положение и свои шансы отстоять старые правила. Если таких шансов практически нет, то не имеет смысла дальше сопротивляться и усугублять противостояние, а тем более доводить дело до военных действий, ведь ясно, что война в любом случае будет проиграна.

Но описанное мирное изменение существующего порядка, к сожалению, происходит не так часто. Причины кроются в самой природе человека. Во-первых, человеку свойственно ошибаться

[13] BBC News. Русская служба. Российской делегации не дали визы для участия в Генассамблее ООН. 24 сентября 2019 г. // URL: https://www.bbc.com/russian/news-49807656.

(рискованное поведение[14]). Применительно к данному примеру конкретные люди, оценивающие на описанных переговорах свои и чужие силы, могут ошибиться в расчетах, полагая, что их страна способна отстоять свои позиции. В результате они не уступят, а дело, скорее всего, дойдет до вооруженного столкновения.

Во-вторых, человеку свойственно не только ошибаться, но и действовать нерационально, в силу самоуверенности, самонадеянности, фанатичной веры в свое население, в свою армию, в совершенство своего оружия, в преимущества государственного строя и т.д. Конечно, и в этом случае, по большому счету, речь идет об ошибке. Но тут это не ошибка точных расчетов, а, скорее, склонность к эмоциональному поведению.

Конечно же, человеку подчас свойственны и иные состояния: агрессия, злоба, зависть, лень. Понятно, что и они время от времени играют свою негативную роль в неспособности найти мирное решение в изменившейся ситуации и пойти на разумный компромисс.

Как нетрудно заметить, история человечества – это постоянные конфликты и войны. То есть, судя по всему, до сих пор человеческий фактор превалировал при принятии ключевых решений и вел к эскалации противостояния вплоть до вооруженного конфликта.

Представляется уместным в качестве примера сложности предварительных расчетов сослаться на ситуацию вокруг Великой Отечественной войны. Перед войной чисто арифметический подсчет сил нацистской Германии и СССР вовсе не говорил о подавляющем преимуществе немцев. Однако немецкие стратеги полагались, видимо, на учет дополнительных факторов: на неожиданность нападения, на высокую степень организации немецкой армии, на боевой опыт. Однако, как известно, Германия войну проиграла в силу целого ряда неучтенных причин. По некоторым оценкам, главный просчет заключался в том, что немцы не оценили возможности консолидации и мобилизации советского общества, его готовности пойти на значительные жертвы. Не нужно также сбрасывать со счетов то, что объективно не было должным образом оценено состояние дорог Советского Союза. Трудно было предвидеть низкие температуры зимой двух первых лет войны. Кроме того, вмешался и субъективный

[14] *Власенко Р.Я., Лосева Т.Н.* Риск как самостоятельный компонент системной организации целенаправленной деятельности субъекта // Рос. мед.-биол. вестн. им. акад. И.П. Павлова. 2014. № 2. С. 145–152.

фактор, в результате силы немецкой армии не были использованы достаточно концентрированно и рационально.

Почему же Германия не пыталась предварительно договориться с СССР об ином устройстве международных отношений, не прибегая к войне? Вообще-то, наверное, можно считать, что такие переговоры в определенной форме имели место[15]. Например, немцы в разных ситуациях ставили вопрос о союзнических отношениях против Франции и Великобритании. В результате какое-то сотрудничество имело место, но в достаточно ограниченных пределах. Но этого Германии было мало, немецкое руководство полагало, что оно было вправе претендовать на принципиально иной порядок. То есть, надо полагать, в конечном итоге немецкие политики пришли к выводу, что СССР не пойдет на военный союз с Германией. Возможно, именно в результате этого и последовало нападение на Советский Союз.

Еще один, уже упоминавшийся выше пример: конфликт вокруг Нагорного Карабаха. Как известно, в октябре-ноябре 2020 года конфликт перерос в вооруженное столкновение, в ходе которого армия Азербайджана добилась определенных успехов. Этому военному столкновению предшествовало несколько десятков лет мирных переговоров, однако в их ходе Азербайджан не смог убедить другие заинтересованные стороны, в частности, силы самообороны Карабаха и Армению, что он способен с помощью вооруженной силы восстановить контроль над этой территорией. Таким образом, мирным путем найти решение не удалось, началась война.

9. Мягкая сила

Понятно, что помимо использования военной силы могут быть использованы и другие методы по сути силового давления. Спектр таких методов очень широк, он шире так называемой "мягкой силы"[16], то есть давления в рамках международного права. Перечислим лишь некоторые из этих методов: экономические и политические санкции,

---

[15] Например, речь идет об операциях "Тибет" и "Аманулла". См.: *Трофимов В.Н.* Коллаборационисты: мнимые и настоящие. Субхас Чандра Бос, Махатма Ганди, Шарль де Голль, Андрей Власов, Михаил Горбачев. М., 2015. С. 31–37.

[16] *Трофимов В.Н.* Военная и экологическая безопасность. Международное право и сила. М., Прометей, 1991. С. 24; *Харитонов А.И.* "Мягкая сила" с китайской спецификой // Вестник РГГУ. Серия: Политология. История. Международные отношения. 2017. № 1 (7). С. 113–120.

обман, информационная война, подкуп и шантаж должностных лиц других государств, вербовка и использование агентов влияния, организация акций протеста, финансовая, информационная или иная поддержка оппозиции в другом государстве, вплоть до поставок оружия, в целом вмешательство во внутренние дела. К ним же относятся прямая засылка вооруженных банд, попытки организовать "цветные революции", физическое устранение неугодных политических деятелей и т.д. Но к этим же методам надо отнести также переговоры, пробу сил, использование ложных юридических конструкций (псевдоправо), недружественные акции.

Понятно, что вышеперечисленные методы либо прямо запрещены международным правом, либо аморальны. И спорным является вопрос, можно ли вообще их использовать. Как уже было показано выше, сверхдержавы, постоянные члены СБ ООН, некоторые другие государства подчас используют такие методы вопреки международно-правовым запретам, не особо опасаясь негативных для себя последствий. Например, США, как правило, не очень ограничивают себя в вопросах применения силы или угрозы ее применения, не очень заботясь о последствиях. А другие страны? **В любом случае подчеркнем, что мы поднимаем тут вопрос о соотношении права и силы и рассматриваем различные ситуации применения силы не для того, чтобы пропагандировать подобные действия, а в первую очередь, для того, чтобы понимать действия других государств и грамотно противодействовать им.**

10. Россия

Итак, рассмотрим вопрос, может ли, например, Россия угрожать применением вооруженной силы и даже применять ее? Тут нет однозначного ответа. Видимо, следует учитывать несколько следующих обстоятельств. Подобные действия чреваты тем, что Россия может приобрести негативную репутацию государства, пренебрегающего международным правом и даже разрушающего его, репутацию государства-агрессора[17]. Однако отказ от использования таких методов в условиях, когда против России они широко применяются, безусловно, поставит страну в заведомо невыгодное

[17] См., например: *Кошкин П.Г.* Формирование нового образа России в прессе Запада с 2014 по 2019 г. // Вестник Санкт-Петербургского университета. Политология. Международные отношения. 2019. № 4. С. 477–499.

положение, может в конечном итоге привести к смене политического режима, к фактической или даже формальной потере суверенитета, к распаду государства. Изложенное означает, что в условиях реальной угрозы для безопасности государства использование силовых методов возможно, даже если это прямо запрещено международным правом. При этом, что касается России, желательно предварительно заручиться поддержкой других дружественных влиятельных государств.

Например, в вопросе о присоединении Крыма целый ряд государств полагает, что имел место акт аннексии, то есть Россия, якобы, совершила агрессивные действия[18]. России предъявляют претензии, что она, если и не использовала свои вооруженные силы в боевых действиях, однако тем не менее создала ситуацию, которую можно трактовать как угрозу их применения. В результате против РФ были приняты экономические и политические санкции. Но, во-первых, эти санкции по понятным причинам не были одобрены СБ ООН. Во-вторых, санкции были введены лишь частью международного сообщества, то есть политическая и экономическая изоляция России не увенчалась успехом. В-третьих, санкции, как правило, оказались малоэффективными. Изложенное означает, что, наверное, в описанном случае действия России, даже если представить на миг, что они противоречили международному праву, тем не менее являлись оправданными.

Примерно такая же ситуация касается и роли и действий России применительно к событиям на Донбассе и Луганске[19]. Прямое применение вооруженной силы со стороны России не было доказано. Точно так же не были убедительно доказаны факты поставок оружия, поощрения участия добровольцев в вооруженной борьбе против регулярных вооруженных сил Украины. Санкции против России были введены, но с таким же результатом и последствиями, как и в вопросе присоединения Крыма.

Можно привести и другие примеры: недоказанное вмешательство России в выборы в США и в других странах, предполагаемые

---

[18] *Гаврилов И.А., Гаврилов А.А., Щербинин А.И.* Присоединение украинского Крыма Россией как причина апории со странами Запада // Вестник Томского государственного университета. Философия, Социология, Политология. 2015. № 3 (31). С. 93.

[19] *Бабенко В.Н.* Образ России на Украине: от "Братского народа" до "Государства-агрессора" // РСМ. 2015. № 3 (88). С. 184–195.

покушения на жизнь Яндарбиева, Литвиненко, Скрипаля, якобы организованное крушение самолета с наиболее антироссийски настроенными политическими деятелями Польши в Катыни, информационная война, в том числе с использованием RT. В некоторых из этих случаев отдельные страны вводили против России политические и экономические санкции, предпринимали иные действия, например, поддерживали, как политически, так и финансово и информационно, деструктивные силы в РФ, вели информационную войну, совершали, по сути, диверсионные действия с использованием киберпространства. Однако пока, по счастью, все эти действия не привели к существенным отрицательным последствиям для России.

Значит ли все вышеизложенное, что Россия, которая является постоянным членом Совета Безопасности ООН и обладает достаточно значительным экономическим потенциалом, тем не менее должна воздерживаться от подобных злоупотреблений? Вопрос это достаточно сложный. С одной стороны, подобные действия будут размывать доверие к международному праву. С другой стороны, вряд ли разумно ограничивать себя в ситуации, когда международная практика складывается иным образом. Да, эта практика противоправна и аморальна. Но если другие страны к ней прибегают, то ограничивать себя – значит ставить свою страну и свое население в заведомо проигрышную ситуацию. Задача внешней политики – в первую очередь защищать интересы именно своей страны и своего народа, а выбор средств для достижения этой цели зависит от конкретной ситуации.

Итак, может показаться, что все страны – постоянные члены СБ ООН, опираясь на свое право "вето", могли бы прибегать к использованию всего арсенала средств регулирования международных отношений, в том числе и неправомерных. Но, как выясняется, на практике это не так (не совсем так). Например, уже упомянутые выше действия России в отношении Крыма и Донбасса не привели к принятию в СБ ООН решений о применении к РФ каких-либо средств принуждения. Но и без СБ ООН другие государства, используя свои экономические и политические возможности, применяют в отношении России те или иные санкции. Учитывая достаточно ограниченные экономические возможности России, эти санкции хоть и не радикально, но все равно как-то влияют на экономическую и политическую ситуации внутри страны.

11. Право и сила

Чтобы окончательно прояснить вопрос о соотношении права и силы в международных отношениях, приведем еще некоторые условные чисто теоретические примеры. Так, иногда в иностранной научной литературе в качестве условного примера используется случай такого литературного персонажа, как Робинзон Крузо, который согласно сюжету соответствующего приключенческого романа попал на необитаемый остров. Этот пример, как правило, касается тех или иных экономических моделей и в таком качестве подвергается обоснованной или необоснованной, но критике[20]. Попробуем, однако, использовать этот пример применительно к вопросу о соотношении права и силы в международных отношениях. Итак, Робинзон попал на необитаемый остров. У него есть огнестрельное оружие (ружье), и он достаточно комфортно обустроил свой быт. В силу обстоятельств его партнером по пребыванию на острове становится туземец Пятница.

Далее – эпизод, которого не было в романе. Робинзон использует свои знания как цивилизованный человек, обучает некоторым приемам Пятницу и устанавливает определенные правила взаимного поведения. Согласно одному из этих правил с утра Пятница готовит завтрак на двоих, а Робинзон читает христианскую молитву. Какое-то время это правило взаимно соблюдается и устраивает каждую из сторон. Однако однажды утром Робинзон просыпается и обнаруживает, что ружье пропало. Он выходит из хижины и видит Пятницу, который сидит неподалеку с пропавшим ружьем. Пятница объясняет, что он теперь сам хорошо понимает христианство. Поэтому теперь с утра не Пятница, а Робинзон будет готовить завтрак на двоих, а Пятница будет читать молитву.

Конечно же, такое изменение правил явно сопровождалось угрозой применения силы (ружье лежало на коленях у Пятницы). Как может дальше поступить Робинзон? Он может либо подчиниться угрозе, либо наброситься на Пятницу и в борьбе попытаться отнять у него ружье. Еще один вариант: притвориться, что согласен, и потом хитростью вернуть контроль над ружьем.

В данном условном примере каждый из двух человек выступает источником права точно так же, как отдельные государства в

20 *Прокофьев Д.* Робинзон Крузо как бизнесмен и экономист. Economy Times, 18 декабря 2020.

международных отношениях. Одна из сторон хочет изменить прежние формальные правила, используя угрозу применения силы. Угроза применить силу реализуется в ходе переговоров Пятницы и Робинзона. Итог таких действий может быть разным, как это происходит и в реальных международных отношениях. Сила (вооруженная сила) в этом примере стоит выше права и является способом поменять существующие правила (у кого ружье, тот и прав). Пример, конечно, в определенной мере противоречит нормам современной морали, поскольку демонстрирует верховенство грубой силы над установленными формальными правилами. Однако надо понимать условность моральных норм, поскольку то, что не одобряется в современных международных отношениях, вполне может быть нормой для необитаемого острова и двух людей, над которыми нет ни полиции, ни суда, ни какой-либо иной высшей власти, а также нет правил поведения, устоявшихся в современном человеческом обществе. Робинзон может пытаться навязать свои правила поведения, как он их понимает, будучи цивилизованным человеком. Но Пятница тоже с тем же успехом может насаждать свои туземные правила, опираясь на грубую силу. И нет никакого критерия, который определял бы, что в условиях ограниченного пространства правила цивилизованного общества лучше правил туземцев-людоедов.

12. Обман[21]

Итак, вопрос о соотношении права и силы выше в какой-то мере рассмотрен. А как быть с соотношением международного права и других методов регулирования международных отношений? Например, как соотносятся международное право и обман (недоговороспособность[22])? Для этого рассмотрим еще один

[21] См. например: *Черных А.В.* Политическая ложь как механизм удержания власти // Власть. 2014. № 12. С. 105–108; *Петрищев Е.В., Цыбаков Д.Л.* Деструктивное информационно-психологическое воздействие в современной мировой политике: субъекты и технологии // Известия ТулГУ. Гуманитарные науки. 2018. № 2. С. 8; *Хорина Г.П.* Власть, политика, нравственность: проблема взаимодействия // Знание. Понимание. Умение. 2013. № 4. С. 49–56.

[22] *Мусаелян Л.А.* Девальвация международного права. Статья вторая: цивилизационные, формационные и геополитические факторы кризиса международного права // Вестник Пермского университета. Философия. Психология. Социология. 2015. № 1 (21). С. 20.

умозрительный условный пример. Допустим, что к берегам вновь открытой земли причалил корабль с европейцами. Назовем их руководителя условно Колонизатором. Как выясняется, вновь открытая земля уже заселена туземцами. Туземцы настроены насторожено к пришельцам и готовы защищать свою территорию с оружием в руках.

Колонизатор и его товарищи хотели бы обосноваться на новой земле. Но пока это невозможно, туземцы готовы относиться к ним как к гостям, но не готовы делиться территорией и ресурсами. Как может поступить Колонизатор? Силой отвоевать территорию он пока не в состоянии. И он прибегает к обману.

Колонизатор поступает следующим образом. Он предлагает вождю туземцев (условно назовем его Туземцем) вступить в переговоры. В ходе переговоров он подробно рассказывает о себе и о своей стране. При этом подчеркивает, что и он, и вся его страна живут по цивилизованным правилам. То есть в стране установлены и согласованы справедливые правила поведения, в том числе по вопросам бизнеса. Эти правила четко выполняются всеми жителями, и это основа основ их существования. Если заключается договор, то он неукоснительно выполняется. А если договор нарушается, то государство и ее органы заставляют нарушителя либо выполнить договор, либо показательно его наказывают.

Туземец внимательно слушает Колонизатора, задает много вопросов и, в конце концов, приходит к выводу, что все сказанное – чистая правда. И это действительно правда, Колонизатор пока не прибегает к обману.

Далее Колонизатор предлагает Туземцу строить взаимные отношения также на цивилизованной основе. Туземец в целом не против, ему понравились рассказы про страну, где все ведут себя строго по правилам. Итак, Колонизатор предлагает Туземцу заключить договор аренды. По договору Туземец предоставляет Колонизатору в аренду на двадцать лет небольшой участок земли прямо на берегу. Колонизатор может там жить и строить дома. При этом Колонизатор в обмен дает Туземцу самые разные товары: бусы, зеркальца, ткани. Мало того, Колонизатор дает Туземцу даже ружья. И не только ружья, но и патроны к ним. Каждый год Колонизатор будет давать дополнительные патроны, не говоря уж об уже упомянутых зеркальцах и бусах.

Конечно, Туземец считает, что сделка выгодная. Он получил огнестрельное оружие и, главное, патроны к нему. Запас патронов будет пополняться в течение всего срока аренды. А через двадцать лет срок аренды кончится, и Колонизатор вернет Туземцу арендованную землю. Исключительно выгодная сделка!

Колонизатор все двадцать лет исправно выполняет договор, ремонтирует ружья, поставляет патроны, передает иные товары. То есть пока все хорошо. Наконец проходит двадцать лет, и договор заканчивает свое действие. И тут выясняется следующее. Колонизатор в соответствии с договором строил на арендованной земле строения. Мало того, обнес их частоколом. И завез туда большой запас оружия и боеприпасов, а также запас продовольствия. В зданиях живет много людей. Причем это не просто люди, а солдаты. При этом формально Колонизатор действовал в полном соответствии с условиями договора аренды, он мог строить здания и селить там людей. И построил, и поселил. В итоге получился хорошо оборудованный форт, способный выдержать любую осаду.

Понятное дело, что после окончания договора аренды Колонизатор и не думает освобождать землю. Мало того, он использует форт для того, чтобы совершать набеги на туземцев и шаг за шагом дальше отвоевывать у них куски территории.

В чем заключался обман? Колонизатор не обманывал Туземца в отношении того, что в его государстве заключенные договоры неукоснительно соблюдаются. Он также до последнего дня неукоснительно выполнял договор аренды. И лишь по окончании договора не выполнил последнее условие: освободить территорию, срок аренды которой завершился.

Обман заключался в том, что Туземец не имел возможности воспользоваться правовыми механизмами, чтобы принудить Колонизатора выполнять условия договора аренды. Более того, в какой-то мере можно считать, что Колонизатор заключил с Туземцем договор, похожий на международный. Он при этом в качестве примера ссылался на договоры, заключаемые внутри государства. Выполнение таких договоров обеспечивается всей полнотой власти и силовых возможностей государства. А в международных отношениях нет вышестоящего механизма, принуждающего стороны соблюдать договоры (хотя, конечно, в международном праве предусмотрена целая система обеспечения выполнения международных договоров, весь вопрос только в том, насколько она действительно

эффективная[23]). В международных отношениях стороны формально равны между собой, и только они и являются источником как права, так и силы (силовых механизмов принуждения).

Итак, в вышеприведенном условном примере обман оказался более действенным средством регулирования отношений между субъектами, чем договор. Более действенным и эффективным, но, конечно же, несправедливым, по мнению Туземца.

13. Международные судебные органы

Конечно, участники международных договоров могут договориться и делегировать свои полномочия какому-то органу, который будет выполнять как функции суда, так и функции органа, принуждающего выполнить решение суда. Более того, такие суды существуют: Международный Суд ООН, Международный Трибунал по морскому праву, Международный уголовный суд, Европейский суд по правам человека и др. Существуют международные арбитражные органы, занимающиеся рассмотрением гражданских исков. Но нужно понимать, что такие судебные органы совсем не эквивалентны внутригосударственным судебным органам. Существование международных судов совсем не означает, что сообщество государств превратилось в некое подобие сверхгосударства.

Международные суды сильно отличаются от внутригосударственных судов. Государство должно признать компетенцию международного суда, причем, как правило, применительно к каждому отдельному судебному делу. Если судебное решение вынесено не в пользу государства-участника разбирательства, это совсем не означает, что это решение будет выполнено. Исполнение решения международного судебного органа – это отдельная сложная проблема. Иногда практикуется арест имущества соответствующего государства как мера обеспечения вынесенного решения. Но понятно, что если речь идет о сверхдержаве, о крупном государстве, о постоянном члене СБ ООН, то тут не существует механизмов, чтобы навязать ему что-то силой, против его воли.

[23] *Ильинская О.И.* К вопросу о способах обеспечения выполнения международных договоров // Актуальные проблемы российского права. 2011. № 3. С. 238–243.

Мало того, судьи международных судебных органов сами являются гражданами каких-то государств, они только формально свободны в своих решениях, а на практике могут занять и нередко занимают необъективную политизированную позицию.

14. Обман и право

Вернемся, однако, к нашему примеру с Колонизатором и Туземцем. Ясно, что Колонизатор, отказавшийся освободить арендованную землю, опирается при этом на угрозу применить силу для защиты своих притязаний. В этом примере обман стоит выше права и позволяет не соблюдать достигнутые договоренности именно потому, что он подкреплен силой. К сожалению, в современных международных отношениях обман – достаточно часто встречающееся явление, имеющее самые разные формы.

Есть и еще один достаточно существенный аспект в приведенном примере с Колонизатором и Туземцем. Колонизатор не заинтересован в том, чтобы Туземец понимал существование как проблемы соотношения права и силы в международных отношениях, так и проблемы соотношения международного и внутригосударственного права – иначе Туземец изначально будет осознавать опасности, связанные с заключением каких-либо договоров с Колонизатором. Поэтому Колонизатору проще отдать Туземцу ружье, порох и патроны, чем книгу, правдиво описывающую фактические методы регулирования международных отношений. Это замечание касается, например, СССР, в библиотеках которого по каким-то причинам фактически отсутствовали многочисленные научные работы западных специалистов, посвященные как силовым моделям поддержания международного порядка, так и в целом проблеме соотношения силовых и юридических методов регулирования международных отношений.

15. Санкции[24]

Рассмотрим некоторые другие способы регулирования международных отношений. Часть из них достаточно тесно связана с

[24] *Семенов А.В.* Политико-экономические санкции в современных международных отношениях // Власть. 2015. № 7. С. 67–72.

возможностью применить силу. Например, недружественные действия, санкции, вмешательство во внутренние дела, экспорт "цветной революции", засылка диверсантов могут быть расценены как casus belli, то есть как повод применить в ответ вооруженную силу, объявить войну. Нередко именно США вмешиваются во внутренние дела других государств, объявляют те или иные экономические или политические санкции, совершают самые различные недружественные действия. Но за этими действиями всегда стоит возможность Соединенных Штатов Америки применить вооруженную силу. Соответственно, эти действия не приводят к военному конфликту, а государства, которые стали жертвой подобных действий, вынуждены искать иные выходы, не связанные с применением вооруженной силы (например, ответные санкции).

Россия была подвергнута самым различным санкциям в связи с событиями вокруг Крыма, Донбасса и Луганска. США также предприняли ряд санкционных мер, полагая, что Россия вмешивалась в американские выборы в 2016 году. Российская Федерация ввела ответные санкции, но в целом пошла по пути не столько ответных мер, сколько минимизации ущерба. Другие страны вмешивались в чеченский конфликт, открыто поддерживая сепаратистов оружием, финансами и инструкторами. Во всех перечисленных случаях международного военного конфликта не случилось именно потому, что и США, и Россия обладают огромным военным потенциалом и способностью нанести противнику неприемлемый ущерб даже в случае ответного, а не первого удара.

Гипотетически можно представить ситуацию, когда во внутренние дела США будет вмешиваться достаточно небольшое государство. Или такое государство будет предпринимать меры, ограничивая поставки нефти в США или его союзникам в Европе (например, блокада Ормузского пролива). С большой вероятностью Соединенные Штаты в таком случае в ответ вместо санкций или иных подобных мер (на самом деле полумер) могут прибегнуть к применению вооруженной силы.

16. Коллаборационизм, вербовка агентов влияния

Использование агентов влияния, ведение информационной войны, подкуп и шантаж должностных лиц другого государства, шпионаж, предоставление убежища перебежчикам другой страны – также

достаточно часто используемые приемы в международных отношениях, но они не так тесно связаны с возможностью той или иной страны применить силу. Например, США не раз предоставляли убежище перебежчикам из спецслужб СССР и России, а РФ в свою очередь поступила подобным же образом в отношении американца Сноудена. По мнению автора, и не только его, Горбачев умышленно действовал в интересах других государств (коллаборационизм), ослабляя СССР, а в конечном итоге и развалив его (именно он приказал спустить флаг над Кремлем, тем самым дав сигнал, что согласен с распадом страны)[25]. Вербовка руководителя другого государства – достаточно редкий случай, но и такое случается в международной практике.

17. Международный правопорядок и международный порядок

В связи с существованием двух принципиально различных способов регулирования международных отношений – правовых и силовых – можно предложить использовать два различных понятия: "международный правопорядок" и "международный порядок". Международный правопорядок – это состояние международных отношений, обусловленное международным правом. А международный порядок обеспечивается всем комплексом существующих средств, в том числе и силовых[26]. На самом деле, в научной литературе уже достаточно давно можно встретить именно такое толкование этих терминов.

Итак, желательно различать понятия "международный порядок" и "международный правопорядок". Первое обеспечивается с помощью всего арсенала доступных инструментов, в том числе и неправомерных, а второе – в основном с помощью международного права. Как правило, все государства стремятся к определенной стабильности в международных отношениях, к международному порядку. Но при этом международный порядок включает в себя и ситуации, когда одни страны ущемляют права других государств

---

[25] *Трофимов В.Н.* Коллаборационисты: мнимые и настоящие. Субхас Чандра Бос, Махатма Ганди, Шарль де Голль, Андрей Власов, Михаил Горбачев. М. 2015, С. 143–194.

[26] *Трофимов В.Н.* Военная и экологическая безопасность. Международное право и сила. М.: Прометей, 1991. С. 20, 101–106.

(например, колониализм, неравноценный экономический обмен, поддержка непопулярных, но союзнических режимов в других странах). Такая несправедливая, но стабильная ситуация – это тоже "международный порядок".

18. Доминирование

Существуют определенные силовые модели поддержания международного порядка и безопасности, при этом используются, например, такие методы, как поддержание баланса сил или обеспечение полного доминирования. И баланс сил, и полное доминирование могут на какое-то время обеспечить сохранение стабильной ситуации.

Коснемся чуть подробнее вопроса, что же такое "доминирование"[27]. Видимо, одной из причин Второй мировой войны стали претензии Германии и Японии на изменение своего статуса и желание контролировать (поработить) другие государства. Наверное, можно утверждать, что одной из причин, по которым США не ликвидируют свои военные базы на территории этих государств, – это желание полного военного доминирования и недопущения попыток нового пересмотра существующего мирового порядка с использованием вооруженной силы.

Доминирование может проявляться и в иных формах. Например, США, как правило, не стремятся держать свои воинские контингенты на территории стран Латинской Америки, однако понятно, что они легко могут прибегнуть к применению силы в случае, если сочтут, что в этом регионе происходит существенное изменение сложившегося порядка. То есть тут доминирование предполагается и по большому счету не оспаривается.

---

[27] *Озерова Е.Г.* Геополитическое доминирование Америки: информационно-аналитический аспект // Вестник СПбГУ. Язык и литература. 2008. № 1-II. С. 319–324; *Бакина А.* США: к вопросу о "мягкой" и "жесткой" силе в условиях глобального доминирования // Власть. 2007. № 7. С. 92–97; *Ницевич В.Ф., Ницевич М.Ю.* Геополитическое доминирование как безусловный императив национальной безопасности: методологические основания // Известия ТулГУ. Гуманитарные науки. 2017. № 1. С. 62–67.

19. Пересмотр баланса сил. Карибский кризис

Хороший пример поддержания стабильности в международных отношениях – это баланс сил между СССР и США в период "холодной войны". При этом имели место локальные пробы сил, например, войны в Корее, во Вьетнаме, Афганистане, Карибский кризис, размещение ракет "Першинг" в Турции. В результате стороны приходили к выводу о реальном соотношении сил и не претендовали на какие-то глобальные изменения. Можно упомянуть в этой связи и компромиссные решения по итогам таких проб сил, например, взаимопонимание о неразмещении "Першингов" в Турции в обмен на неразмещение советских ракет на Кубе. Это взаимопонимание не приняло форму международного договора, заключенного в письменном виде, однако несомненно, что оно является частью именно международного права. Таким образом, в ходе Карибского кризиса сначала путем реальной пробы сил было выяснены как возможности каждой из сторон прибегнуть к угрозе применения силы (может быть, и к применению вооруженной силы), а главное, решимость перейти к применению силы. По итогам этой пробы сил сформировался как новый международный порядок, так и новый правопорядок ("Першинги" в обмен на ракеты на Кубе[28]).

20. Пересмотр и расторжение заключенных договоров

Понятно, что соотношение сил (баланс сил) на международной арене время от времени меняется. Государства, которые стали сильней в военном, политическом отношении или увеличили свой экономический потенциал, начинают претендовать на изменение порядка по каким-то вопросам. Нередко это значит, что те страны, которые стали относительно слабее, должны уступить часть своих прав. Формально это может быть сделано за счет пересмотра имеющихся международных договоров.

Таким образом, пересмотр уже заключенных международных договоров – естественное последствие изменения реальной международной ситуации. Хороший пример – это Договор об

[28] *Малахов В.Т.* Карибский кризис 1962 года: история и современность // Вестник Московского государственного лингвистического университета. Общественные науки. 2016. № 2 (767). С. 115.

ограничении ракет средней и меньшей дальности (ДРСМД)[29]. Указанный договор был заключен с США от имени СССР Михаилом Горбачевым и рассматривался многими как неравноценный, ущемлявший оборонные интересы Советского Союза. С помощью ракет средней и меньшей дальности наземного базирования СССР мог нанести ответный удар по европейским странам, входящим в блок НАТО. В свою очередь Соединенные Штаты, планируя удар по СССР, полагались как на стратегические ракеты, так и на ракеты средней дальности морского базирования, не подпадавшие под действие договора. Таким образом, США никак не сокращали свой военный потенциал, нацеленный на СССР, а Советский Союз сокращал ракеты, игравшие сдерживающую роль применительно к европейским военным союзникам США.

Договор просуществовал до 2019 года, когда США обнаружили, что Россия смогла разработать крылатые ракеты средней дальности морского базирования, способные нанести ответный удар по Западной Европе. Получалось, что договор больше не защищал европейские страны НАТО, но сдерживал США в производстве и продаже ракет средней дальности наземного базирования. То есть практическая ситуация существенно изменилась: договор, ранее ущемлявший оборонный потенциал как СССР, так и России, изменил свою роль и стал сдерживающим фактором уже для военно-промышленного комплекса Соединенных Штатов. В результате США, несмотря на серьезную международную критику, вышли из договора[30].

Нужно упомянуть и Договор об ограничении систем противоракетной обороны (Договор по ПРО), заключенный между СССР и США в 1972 году. Как только Соединенные Штаты пришли к выводу, что этот договор сдерживает их, в 2002 году они отказались и от него[31].

---

[29] *Ознобищев С.К.* Американские (русские) горки европейской безопасности // АПЕ. 2020. № 3. С. 23, 30–34.

[30] *Иванов О.П.* Модернизация стратегии НАТО и Россия. Современная Европа, 2020, № 3. С. 117–127.

[31] *Буторов А.С.* Односторонний выход США из Договора по ПРО 1972 г. и его глобальные последствия. Вестник РУДН, серия Международные отношения, март 2016. Т. 16. № 1. С. 153–164.

21. Неравноценность прав при заключении международного договора

Международный договор далеко не всегда является средством, взаимовыгодным для его участников. Нередко страны, участвующие в разработке очередного международного договора, всяческими способами стремятся включить в него положения, выгодные для них, и исключить выгодные для другой стороны. Подчас в итоге баланс зафиксированных в договоре интересов (прав и обязанностей) является достаточно спорным. Размен может касаться разных по своей природе интересов. Например, заключая Конвенцию ООН по морскому праву, крупные военные державы получили свободу судоходства через международные проливы и право мирного прохода через чужие территориальные воды. В свою очередь, прибрежные государства смогли зафиксировать свои права на весьма обширные прибрежные пространства (морские экономические зоны до 200 морских миль и континентальный шельф)[32]. То есть в этом случае произошел размен военных интересов на экономические. Прибрежные государства достаточно быстро смогли легализовать свои претензии на ресурсы экономической зоны и континентального шельфа, сразу же получая доход от их эксплуатации. А военные державы лишь в принципе зафиксировали свои права на свободу военного судоходства, то есть защитили свои потенциальные военные интересы, которые, может быть, никогда и не будут реализованы.

Еще один пример – это Договор о запрещении размещения на дне морей и океанов оружия массового уничтожения. Ясно, что у США, а также у значительной части европейских стран экономический потенциал расположен именно по морскому побережью. У СССР (а сейчас у России), наоборот, экономический потенциал расположен, как правило, далеко от морского побережья. Некоторые исключения – это Владивосток на берегу Тихого океана, Санкт-Петербург на Балтике, Мурманск на берегу Баренцева моря. Подрыв термоядерной бомбы даже в центре Атлантики вызывал бы разрушительный цунами для восточного побережья США и западного побережья Европы. При этом такая же угроза для территории СССР практически не существовала. Тем не менее, СССР согласился на заключение

[32] *Молодцов С.В.* Международное морское право. М., Международные отношения, 1987. С. 207–211.

Договора о запрещении размещения на дне морей и океанов оружия массового уничтожения.

В чем-то сходная ситуация касалась и Договора о принципах деятельности по исследованию и использованию космического пространства, включая Луну и другие небесные тела. Статья IV указанного договора запрещает выведение на орбиту Земли ядерного оружия. А если бы такого запрета не было? В таком случае выведенное на околоземную орбиту ядерное оружие каждый час пролетало бы над потенциальной целью на территории предполагаемого противника (например, над Вашингтоном или Нью-Йорком). Конечно же, точно так же такая же бомба была бы запущена в ответ на орбиту и этим потенциальным противником. В результате возможность нанести ответный удар была бы равной для любого ядерного государства, способного вывести заряд на орбиту Земли, вне зависимости от его военного и экономического потенциала. Такое положение сводило бы к нулю преимущества, которые могли извлечь США из своего особого военного и экономического статуса. Договор был заключен, запрет был установлен. В результате Соединенные Штаты, имея возможность затрачивать на военные цели значительные финансовые средства, разработали новые виды оружия, ставящие их в преимущественное положение к подавляющему числу других стран.

Конечно, последний пример не лишен недостатков. Ядерное оружие на орбите, в конце концов, сгорало бы в атмосфере, заражая радиоактивными отходами значительные пространства. Это было невыгодно для всех стран, в том числе и для СССР. Тем не менее, из этого примера понятно, как именно рассчитывают свои интересы те или иные страны, предлагая заключить новый международный договор.

Еще один пример – это Конвенция о сохранении морских живых ресурсов Антарктики[33]. Исторически так сложилось, что в СССР развитие получило не столько разведение рыбы, сколько ее вылов, причем нередко в морях, не прилегающих к территории Советского Союза. В результате был создан довольно значительный промысловый флот. Однако во второй половине двадцатого века многие прибрежные государства, как уже было отмечено выше, стали претендовать на двухсотмильную рыболовную зону. Промысел рыбы в ней стал платным. Для советских промысловых судов деятельность

[33] *Трофимов В.Н.* Международно-правовой статус Антарктики. М.: Прометей, 1990.

по вылову рыбы у чужих берегов стала экономически намного менее выгодной. Образовался неиспользуемый резерв промысловых судов. Однако в этот период выяснилось, что в морях, непосредственно примыкающих к Антарктиде, имеются колоссальные запасы так называемого криля, арктического рачка небольшого размера. Советский промысловый флот, практически не имея конкурентов, мог начать вылов криля, добывая тем самым большое количество почти чистого протеина. Тотчас же другие государства, претендующие на те или иные части Антарктики, предложили заключить Конвенцию о сохранении морских живых ресурсов Антарктики, согласно которой лов в антарктических морях очень существенно ограничивался. Советский Союз по каким-то причинам согласился на участие в этом международном договоре, тем самым сам добровольно ограничивая свои промысловые возможности.

При заключении международного договора бывают и просчеты, которые трудно заранее предвидеть. Например, СССР, становясь участником Конвенции ООН по морскому праву, сделал очень определенные оговорки в отношении компетенции Международного трибунала по морскому праву в случаях, связанных с обеспечением национальной безопасности и военными кораблями. Однако все эти оговорки оказались бесполезными. Несмотря на них, указанный судебный орган принял к рассмотрению заявление Украины в отношении ее кораблей и экипажей, арестованных Россией при попытке пройти из Черного моря в Азовское без соблюдения формальных процедур, касающихся безопасности. Мало того, Трибунал в итоге вынес решение против России, и никакие ссылки на оговорки и положения Конвенции не помогли. Оказалось, что Трибунал далеко не всегда является беспристрастным судебным органом, действующим в соответствии с нормами международного права.

Все вышеизложенное говорит о том, что, как правило, международный договор не заключается на вечные времена. В момент заключения он отражает сложившийся баланс сил, сложившуюся политическую или экономическую ситуацию. Бывает, что международный договор заключается в результате ошибки, просчета или обмана. Это значит, что если баланс сил меняется, экономическая и политическая обстановка претерпевает существенные изменения, обман или просчет становится очевидным, необходимо ставить вопрос либо об изменении соответствующего международного договора,

либо об отказе от участия в нем. Конечно, изменение договора – сложный процесс. Как правило, другие участники договора, которым он был выгоден, активно препятствуют этому. И выход из договора не всегда бывает легким, в результате можно попасть под серьезную международную критику, под обвинения в разрушении международного права. В таком случае надо предварительно просчитывать все плюсы и минусы, выяснять, какие последствия для страны будут менее губительными – от участия в договоре или от выхода из него.

22. Злоупотребление правом

Особый случай регулирования международных отношений – это использование заведомо ложных юридических конструкций или злоупотребление правом. Для краткости можно назвать этот прием "псевдоправом". Дело в том, что прямое использование силовых методов имеет определенный побочный негативный эффект: подобные действия далеко не всегда встречают одобрение как у отдельных государств, так и в целом у мирового сообщества. Дабы снизить этот негативный эффект, соответствующие силовые действия нередко маскируются с помощью правовых конструкций, формально признаваемых мировым сообществом, как то: национально-освободительное движение, право наций на самоопределение, революция и др. Например, Косово было насильственно отторгнуто от Сербии. Однако формально эти действия прикрывались ссылками на национально-освободительное движение, голосование в парламенте (то есть, якобы, народное волеизъявление), на право нации на самоопределение, на решение международного суда[34].

Еще один пример: отделение прибалтийских республик от СССР. Общеизвестно, что западные страны активно поддерживали и поощряли сепаратистские настроения в этих республиках, не признавая их вхождение в состав Советского Союза. Республики приобрели независимость без соблюдения юридических процедур, предусмотренных для подобных случаев в законодательстве СССР, с использованием силовых методов. Во многом этим событиям способствовали действия лично М. Горбачева, которые подчас

[34] *Строева А.С.* Проблема признания Косова // Актуальные проблемы российского права. 2011. № 4. С. 275–282.

квалифицируются специалистами как прямой коллаборационизм. Однако формально в западной литературе отделение прибалтийских республик преподносится как восстановление независимости после советской оккупации в результате правомерной борьбы.

Несомненно, что действия западных стран в Ливии и свержение Каддафи имели насильственный характер. Но формально такие действия оправдывались ссылками на гражданскую войну, а боевиков называли революционерами. Более того, Международный уголовный суд заявил, что действия Каддафи могут быть квалифицированы как преступления против человечности. СБ ООН принял резолюцию о санкциях в отношении Каддафи, а также резолюцию о бесполетной зоне в Ливии (Джамахирии). В результате в рамках этой последней резолюции, но явно с нарушением ее пределов, страны – члены НАТО стали наносить авиаудары по территории Ливии, поддерживая боевиков.

Нередко вмешательство во внутренние дела других государств, вплоть до засылки банд и поддержки оружием оппозиции, оправдывается ссылками на необходимость поддержки процессов демократизации, защиты прав человека. Вторжение в Ирак оправдывалось Соединенными Штатами необходимостью не допустить создание оружия массового уничтожения.

Конечно же, страны Запада квалифицируют действия России в отношении Крыма как акт агрессии, ссылаясь на "аннексию" (является формой агрессии). Россия, в свою очередь, ссылается на право нации на самоопределение, указывая на то, что народ Крыма сам определил свою судьбу на референдуме[35]. Понятно, что западный мир не соглашается с российской квалификацией, рассматривая ее как попытку придать насильственным действиям правомерный вид, то есть как злоупотребление правом (как попытку необоснованно расширительно толковать понятие "нация"). Учитывая это, не исключено, что России следовало немного иначе мотивировать свою позицию, например, ссылаться на то, что в международном праве пока не сформировались нормы, регулирующие выход из состава государства его части, и пока только идет процесс формирования таких норм в виде складывающейся конкретной практики. Когда практика окончательно сложится, будут сформулированы и соответствующие нормы права.

---

[35] *Пряхина Т.М.* Признание факта принятия в Российскую Федерацию Республики Крым // Вестник СГЮА. 2015. № 5 (106). С. 16–22.

23. Борьба за мир

В связи с изложенными соображениями относительно соотношения права и силы в международных отношениях представляет интерес рассмотрение политики, проводимой некоторыми государствами и формулируемой как "борьба за мир"[36]. Подобную политику, например, широко декларировал СССР. Для правильного понимания этого феномена важно различать реальные цели внешней политики и публично декларируемые цели, являющиеся частью пропаганды и информационной войны.

Конечно, война – это страдания и смерть многих людей, уничтожение материальных ценностей. Ясно, что это не может восприниматься как положительное явление. Однако важный вопрос: какими именно методами можно реально снизить угрозу войны и массовой гибели людей. Просто призывать не воевать – это, конечно, утопия. Невозможно уговорами и агитацией заставить другие государства не прибегать к крайнему средству защиты их интересов – к силе. Более реальный способ предотвратить войну – это использовать такие методы, которые убедили бы других участников международных отношений, что у них нет шансов победить с использованием вооруженной силы, что баланс сил сложился не в их пользу, и им разумнее уступить, не доводя до полномасштабной войны. Например, можно использовать переговоры. Но они не будут успешными, если на них не будут представлены убедительные доказательства существенного военного превосходства. Однако как без реальных боевых действий доказать свое военное превосходство? Тут уместны ссылки на значительный военный бюджет, на численность и вооруженность собственной армии. Существенное значение имеют военные учения, практика заключения военных союзов. Важны пробы сил, например, в форме локальных конфликтов, которые на практике покажут реальное соотношение сил. Значительную роль играют также пропаганда и другие методы информационной войны.

Итак, декларировать, что внешняя политика государства преследует цель борьбы за мир во всем мире – вполне допустимый и

[36] Вопрос всех вопросов: Борьба за мир и исторические судьбы человечества / ред. коллегия: В.В. Загладин, И.К. Пантин, Т.Т. Тимофеев. М.: Политиздат, 1985. С. 20–52.

оправданный прием. Но при этом надо понимать, что подобные публично декларируемые цели не совпадают с реальной ситуацией в вопросе регулирования международных отношений. Наверное, тут можно говорить об использовании во внешней политике двойных стандартов.

24. Российская внешняя политика и силовые модели обеспечения международной безопасности. СНВ-2

Что касается российской внешней политики, то, наверное, можно констатировать, что ни в научном сообществе, ни среди практиков, занимающихся международными отношениями, пока не сложилось системное понимание проблемы соотношения права и силы в международных отношениях. Соответствующие силовые акции предпринимаются, но их оправданность и необходимость осознается, видимо, скорее, на интуитивном уровне. Тут можно привести следующий достаточно показательный пример[37]. В самом конце 1993 года президент России Б. Ельцин и президент США Д. Буш подписали Договор о сокращении стратегических наступательных вооружений (СНВ-2). Согласно Конституции России в то время высшим органом государственной власти в стране был не президент, а Съезд народных депутатов (парламент). Конечно же, такой значительный договор, касавшийся разоружения, должен был быть предварительно согласован на всех уровнях власти. Однако этого не произошло, Б. Ельцин решил не показывать депутатам проект договора, сразу согласившись с американцами на его подписание. После того как договор был вынесен на ратификацию, Верховный Совет России стал запрашивать у исполнительных органов власти соответствующие обоснования. В частности, в МИД России был направлен официальный запрос Комитета по международным делам Верховного Совета России, в котором содержалась просьба разъяснить, как сочетается СНВ-2 с силовыми моделями поддержания международного порядка, используемыми Соединенными Штатами. В запросе содержалась также просьба изложить, как именно США используют такие силовые модели в своей внешней политике. МИД России не смог ответить на этот запрос. Как выяснилось, там не было никакой системной информации по данной теме. То есть

[37] *Трофимов В.Н.* Саботаж. М.: Делибри, 2018. С. 544–576.

исполнительная власть России заключила СНВ-2, не имея никакого представления о теоретических и практических основах формирования внешней политики США по вопросам применения силы и поддержания международного порядка. В лучшем случае речь шла об интуитивном понимании этого вопроса.

25. Глобальное потепление, информационная безопасность

Вопрос о соотношении силы и права в международных отношениях совсем не праздный, он имеет важное практическое значение. Как именно следует применять на практике науку международного права? Казалось бы, ответ очевиден: возникает международная проблема, специалисты ее описывают. Юристы разных стран собираются вместе и вырабатывают совместные взаимоприемлемые правила, которые позволяют эту проблему решить. Правила принимают форму международного договора, который торжественно подписывают и ратифицируют. Договор на века!

Действительно, именно так достаточно часто и случается. Это касается в первую очередь проблем, которые имеют универсальный характер, то есть создают примерно одинаковые сложности или даже угрозы для всех стран без исключения. Например, это касается распространения опасных болезней, борьбы с определенными формами терроризма, защиты каких-то видов живых существ от вымирания.

Однако проблемы далеко не всегда имеют такую форму. Например, глобальное потепление – несомненно, проблема универсального характера. Но она совсем не одинаково затрагивает интересы разных стран. Государства, которые расположены ближе к полюсам, не будут страдать от избыточной жары. Конечно, в чем-то глобальное потепление отрицательно скажется и на них (распространение тропических болезней, катастрофические природные явления: наводнения, засухи). Но в целом такие страны попадут в более благоприятную климатическую зону, смогут осваивать ранее недоступные полярные области, получат выгоды в области сельского хозяйства. В какой-то мере это касается, например, России и Канады[38].

[38] *Котликофф Л.Д., Казакова М.В., Нестерова К.В.* Проблема глобального потепления и последствия борьбы с ней для российской экономики // Российское предпринимательство. 2017. № 4. С. 633–640.

Борьба с глобальным потеплением – это, в первую очередь, снижение выбросов в атмосферу от промышленных предприятий (борьба с парниковым эффектом). И тут государства с развитой промышленностью далеко не всегда заинтересованы в ограничении производства. Сокращение выбросов – это дополнительные расходы, то есть подорожание продукции и снижение ее конкурентоспособности. Кроме того, ограничение использования промышленных грязных, но дешевых технологий – это снижение темпов экономического роста, утрата возможности догнать другие промышленно развитые страны. Значительные выбросы в атмосферу происходят, например, на территории Китая[39]. Но снижение темпов экономического роста и потеря конкурентоспособности – серьезная проблема для этой страны, возможно, сейчас более серьезная, чем в целом обеспечение благоприятных условий существования для собственного населения, а также засухи и наводнения.

Промышленность США также существенно загрязняет атмосферу. Но дополнительные издержки от использования природоохранных технологий – это тоже снижение темпов роста и потеря конкурентоспособности. А это для США чревато не просто экономическими потерями, а утратой лидирующего положения в мировой экономике, проигрышем в экономическом соревновании с Китаем.

Изложенные обстоятельства сказались на позиции этих стран (Россия, Китай, США) по отношению к разработке новых соглашений по борьбе с изменением климата и к введению новых ограничений на выбросы парниковых газов в атмосферу. Интересы этих стран не совпали с интересами других государств, что серьезно затормозило переговорный процесс. Неучастие ключевых мировых игроков и проблемы с разработкой новых международных норм означали, что чисто юридическими методами не удается достичь взаимоприемлемых результатов. Помимо международного права существенную роль тут в скрытой форме стала играть в том числе и сила. Внешне это выглядит так: какое-то государство не соглашается с предлагаемыми ограничениями на выброс вредных веществ и продолжает грязное промышленное производство. Если это сверхдержава (США, Китай), то его невозможно заставить силой ввести такие ограничения. Невозможно потому, что такая

[39] *Толоконникова Е.В.* Экологические проблемы Китая // Вестник ГУУ. 2014. № 1. С. 60–63.

сверхдержава сама полагается на свои политические, военные и экономические преимущества. Да, она прямо не прибегает к использованию силы. Но полагается именно на свою силу, проводя промышленную политику, которая наносит ущерб интересам других стран, и не опасается, что ее за это накажут.

Еще одна категория международных проблем – это те, которые в той или иной форме затрагивают вопросы безопасности. Это не только проблемы урегулирования военных конфликтов и ограничения вооружений. К ним относятся и проблемы обеспечения безопасности в области использования ИКТ (информационная безопасность, кибербезопасность). Тут интересы разных стран еще более не совпадают. Мало того, в таких вопросах на первый план в прямой форме выходит сила, а также угроза применения силы и иные факторы, так или иначе связанные с использованием силы. Какова тут роль международного права? Можно ли тут использовать только средства международного права, не обращаясь к иным средствами регулирования международных отношений, в том числе и к силовым моделям поддержания международного порядка? Видимо, нет.

26. Как реагировать на применение силы? Pacta sunt servanda

Представим себе следующую умозрительную ситуацию. Существует система международных договоров, которые призваны обеспечивать мир и порядок. Но вдруг одна из сверхдержав нарушает этот порядок и вопреки всем международным договорам применяет силу (вооруженную силу). Что делать, как реагировать? Какие средства надо применять, чтобы уменьшить для себя ущерб от такой ситуации? Предположим, что государственный деятель, отвечающий за формирование международной политики своей страны, решил обратиться за советом к юристу-международнику. Воспроизведем тут этот диалог между Политиком и Юристом, который на самом деле вполне мог иметь место в реальности:

Политик: "Страны НАТО вопреки всем международным договорам бомбят Югославию (Ливию, Ирак и т.д.). Что делать?"

Юрист: "Pacta sunt servanda. Договоры надо выполнять! Страны НАТО действуют неправомерно".

Политик: "Я и без вас понимаю, что неправомерно. Мы-то что должны делать?"

Юрист: "Надо побудить страны НАТО соблюдать международные обязательства".

Политик: "Как побудить?"

Юрист: "Вести разъяснительную работу среди стран, не согласных с такими действиями. Призвать мировое сообщество осудить действия НАТО. Поставить вопрос на Совете Безопасности ООН".

Политик: "Призвать и разъяснять – это все хорошо, только малоэффективно. В СБ ООН вопрос поставить можно. Но ведь ясно, что страны НАТО, имеющие статус постоянных членов, заблокируют все наши проекты резолюций. Это все бесполезно. Делать-то что нам?"

Юрист: "Надо вынести вопрос на Генассамблею ООН".

Политик: "Резолюции ГА ООН не являются юридически обязательными. Даже если мы сможем добиться принятия такой резолюции, толку от нее будет мало, страны НАТО просто проигнорируют ее!"

Юрист: "Все равно такая резолюция будет способствовать консолидации всех прогрессивных сил против агрессора".

Политик: "Консолидация – это хорошо. Но это туманная маловероятная перспектива. Может, и нам прибегнуть к силе? Хотя бы продемонстрировать, что мы тоже не лыком шиты?"

Юрист: "Нельзя ни в коем случае! Это будет противоречить международному праву! Договоры надо соблюдать. Pacta sunt servanda. Мы тогда сами будем ослаблять международное право. А на что мы тогда в следующий раз будем ссылаться, когда агрессор опять на кого-нибудь нападет?"

Политик: "Если следовать вашей логике, то мы всегда будем в проигрышном положении, если им можно применять силу, а нам нельзя, потому как это вредит международному праву".

Юрист: "Так устроен современный мир. Надо вести борьбу за повышение эффективности международного права!"

Политик: "А что, если тоже применить силу? Я слышал, существуют модели обеспечения международного порядка не только с помощью права, но и силы!"

Юрист: "Применение силы запрещено международным правом!"

Все! На этом диалог, несомненно, завершится. Юрист-международник не смог предложить ничего дельного. Мало того, юрист дважды ввел политика в серьезное заблуждение. Он утверждал, что современный мир устроен так, что международное право нельзя

нарушать, а кто нарушает, тот поступает плохо, но с этим ничего поделать нельзя. Вот позиция юриста: "pacta sunt servanda", "надо бороться за повышение эффективности…", "надо поставить вопрос…", "надо решительно осудить…", "надо призвать все мировое сообщество…". Более того, юрист совершенно необоснованно поставил право выше силы ("применение силы запрещено международным правом"), тем самым лишив политика возможности эффективно противостоять действиям других стран и защитить интересы своего государства.

Диалог между политиком и юристом по вопросам безопасности информационных технологий (цифровых технологий, кибербезопасности) будет еще менее содержательным:

Политик: "Другие государства явно злоупотребляют возможностями Интернета и информационных технологий, вмешиваются в наши внутренние дела, открыто ведут антироссийскую пропаганду, а по сути, информационную войну, беззастенчиво воруют чувствительную информацию, шпионят за нашими гражданами. Что делать?"

Юрист: "Дело в том, что деятельность государств в киберпространстве, в Интернете еще мало кодифицирована. Практически нет никаких универсальных международных договоров, которые устанавливали бы соответствующие правила. Существуют региональные соглашения, позволяющие координировать действия в киберпространстве и обмениваться информацией, и то не любой, а только применительно к уголовным преступлениями и терроризму. Есть двусторонние соглашения, регулирующие сотрудничество спецслужб. Есть Будапештская конвенция, но мы в ней не участвуем. Можно говорить о применимости соглашений, касающихся выдачи преступников. Приняты некоторые резолюции ГА ООН, но они не носят обязательного характера. В целом же работа ведется пока только на уровне выработке принципов деятельности в киберпространстве. Но тут противоречия между участниками достаточно существенны. К тому же даже те принципы, по которым уже найдено согласие, не могут применяться непосредственно, они должны быть инкорпорированы в соответствующие международные договоры. Следовательно, нам надо вести разъяснительную работу, объяснять, что хаос в киберпространстве не выгоден никому. Надо предложить проект резолюции для ГА ООН. Можно попробовать поднять вопрос в СБ ООН. Можно попробовать применить уже

существующие нормы международного права, например, гуманитарное право, общие принципы международного права, договоры, в целом регулирующие международную безопасность. Но норм, признаваемых всеми государствами и прямо регулирующих деятельность в киберпространстве, человечество пока не выработало. Надо подождать..."

Политик: "Сколько надо ждать?"

Юрист: "Ну, это никто не знает. Может быть, несколько лет. Или десятилетий. А пока придется мириться с хаосом и беспорядком в киберпространстве…"

Однако если бы рядом с юристом-международником стоял также специалист по вопросам применения силы в международных отношениях, обсуждение могло бы выглядеть иначе, например, так:

"Договоров нет, поскольку неясно, каково реальное соотношение сил в киберпространстве. Никто не хочет себя заранее ограничивать, рассчитывая, что именно он, опираясь на свои высокоразвитые технологии, может извлечь из деятельности в киберпространстве односторонние преимущества в ущерб интересам других стран. Идет настоящая гонка вооружений, только виртуальных. Порядок, конечно, когда-нибудь возникнет, но не сразу. Если мы хотим ограничить вредоносную деятельность других стран в нашем киберпространстве, то это можно делать двумя путями. Первый путь – принимать собственное законодательство и вводить те или иные ограничения в Интернете. Что-то удастся ограничить или запретить, но такие запреты и ограничения далеко не всегда будут эффективны. Специфика Интернета такова, что существует, например, система переадресации, размещение анонимной информации, использование паролей, защищающих группы участников, и др. Все это позволяет так или иначе, но обходить установленные государством национальные запреты. Другой путь – самим развивать информационные технологии, и нравится нам это или нет, но поступать так же в отношении других государств, как они поступают в отношении нас. То есть используя киберпространство, вмешиваться в их внутренние дела, вести шпионаж, информационную войну, красть чувствительную информацию. Конечно, это вызовет серьезное сопротивление и международные осложнения. Но иного эффективного пути нет. Пока другие страны не поймут, что мы тоже можем злоупотреблять Интернетом, никто там не согласится ни на какие международные договоры и ограничительные меры, ни на какой

международный правопорядок. До тех пор, пока соответствующая другая страна не поймет, что мы можем извлечь из использования Интернета больше преимуществ в ущерб их интересам, они не согласятся ни на какие международные договоры. А пока порядок в киберпространстве будет обеспечиваться с помощью практических действий, то есть, по сути, с применением силы, причем нередко путем размена в виде взаимного ущерба".

27. Междисциплинарность

Таким образом, если политик пытается получить хороший совет от научного сообщества, то ему в сложной ситуации надо советоваться одновременно не только с юристом-международником, но и со специалистом в области силовых моделей поддержания международного порядка. А лучше, если юрист-международник сам освоит вопросы, связанные с соотношением права и силы в международных отношениях. Иными словами, для того, чтобы научные советы и рекомендации имели хоть какую-то практическую значимость, необходимо использовать междисциплинарный подход.

Итак, междисциплинарный подход[40]. Реальная жизнь далеко не всегда совпадает с научной теорией, она намного многообразней, изобилует противоречиями, исключениями и парадоксами. Научные же исследования нередко ведутся с высокой степенью специализации, что вполне объяснимо: для того чтобы глубоко изучить предмет, приходится вести исследование в узко специальном направлении. В результате международными отношениями, помимо юристов-международников, занимаются еще историки, политологи, специалисты по вопросам применения силы, а также в какой-то мере представители и иных научных направлений. Каждый из них хорошо знает свой предмет и в пределах своих знаний способен дать соответствующие советы. Но государственному деятелю, принимающему конкретные решения, нужен не просто совет, а совет, имеющий хоть какое-то практическое значение. Если международная проблема имеет несколько аспектов (в нашем случае международно-правовой и силовой), то нужны несколько специалистов, которые при этом должны быть способны договориться между собой и выработать

[40] *Ветров Ю.П., Калинин И.В.* Синергия междисциплинарности // Высшее образование в России. 2012. № 8–9. С. 155–158; *Афанасенко И.Д., Борисова В.В.* Междисциплинарность в логистическом знании // Известия СПбГЭУ. 2017. С. 12–15.

единую практическую рекомендацию. А лучше, если советы будет давать один человек без узкой специализации, обладающий профессиональными знаниями по нескольким дисциплинам. Это и есть междисциплинарный подход, то есть выработка рекомендаций и окончательных решений на основе знаний, относящихся к разным научным дисциплинам.

Формально в любом случае, как в высшей школе, так и на уровне среднего образования, учащиеся изучают широкий круг дисциплин. Казалось бы, тем самым закладывается основа для междисциплинарного применения полученных знаний. Однако это далеко не всегда так. После высшей школы начинается специализация выпускников. И эта специализация нередко предполагает совершенствование знаний в пределах одной определенной дисциплины. Что касается международного публичного права, то тут ситуация имеет дополнительную специфику. Соответствующие правовые нормы регулируют определенный конкретный предмет (международное морское право – использование морей и океанов, международное космическое право – использование Космоса, договоры в области разоружения – определенные виды оружия и его использование, международное гуманитарное право – снижение негативных последствий военных конфликтов, международное дипломатическое право – права и обязанности государств и дипломатов в процессе дипотношений, право международных договоров – порядок заключения, исполнения и расторжения международных договоров и т.д.). Иными словами, юрист-международник, занимающийся определенным направлением (отраслью) международного права, в любом случае глубоко изучает не только юридическую технику, но и предмет и объект, который подвергается регулированию.

Казалось бы, юрист-международник, занимающийся проблемами безопасности в той или иной области международных отношений (в том числе и проблемы безопасности использования информационных технологий), само собой, изучает те или иные угрозы. Но одно дело – угрозы, и другое – использование, например, силы для достижения определенных результатов, для регулирования международных отношений. В этом последнем случае сила, угроза применения силы выступают способом регулирования отношений, точно так же, как и международное право. То есть сила выступает как инструмент регулирования.

Сила может выступать и как объект научного исследования. Но в таком случае предметом выступают способы ее применения. А если предмет исследования – способы обеспечения международного порядка, то тут применение силы, наряду с международным правом, – это уже один из инструментов для обеспечения такого порядка.

Вышеизложенное означает, что на соответствующих этапах подготовки специалистов (в рамках высшей школы и после нее) желательно не замыкаться на узкой специализации, точнее, обеспечивать специализацию сразу по нескольким дисциплинам. На практике междисциплинарный подход предполагает подготовку специалистов сразу по нескольким дисциплинам. Например, готовить не юристов-международников, а политологов, которые будут изучать не только международное право, но и иные дисциплины. Или формально готовить по специальности юриста-международника, но при этом исходить из необходимости глубокого изучения других дисциплин, помимо дисциплины международного права.

Глава 2. Информационно-коммуникационные и цифровые технологии

Для целей этой главы желательно определиться с некоторыми терминами. В данной работе используются два термина: информационно-коммуникационные технологии (ИКТ) и цифровые технологии. Понятие "ИКТ", пожалуй, шире, чем "цифровые технологии", по крайней мере, ИКТ включает в том числе и аналоговые технологии.

Хорошо было бы оперировать только одним термином: ИКТ или цифровые технологии. Но так не получается. Вопросы, связанные, например, с борьбой с использованием информационного пространства в преступных, террористических, иных противоправных целях, с борьбой против военно-политических угроз – это, конечно, ИКТ. А угрозы, связанные с созданием искусственного интеллекта – это, скорее, только цифровые технологии, тут использование термина ИКТ могло бы вызвать путаницу. Именно поэтому дальше в этой работе эти термины и используются – в зависимости от предполагаемого источника угроз.

Как известно, в цифровых устройствах, используемых человеком, используется двоичный код, который также называют бинарным кодом. Двоичный код лежит в основе двоичной системы счисления. Это простейший код, в его основе лишь два варианта: "да" или "нет", "0" или "1". Такое кодирование информации представляется предельно простым. Тем не менее именно оно и лежит в основе цифровых технологий.

Может ли столь простая система быть использована в злонамеренных целях? Или, тем более, сама представлять какую-то угрозу для кого бы то ни было? Грубо говоря, может ли исходить угроза для человечества от игры в "крестики-нолики"? Некоторые сложные явления нашего времени основываются на достаточно простых схемах. Нейтрон попадает в атом изотопа урана, в результате тот излучает два или больше нейтрона, при этом выделяется энергия. Этот простой процесс лежит в основе всей современной ядерной энергетики, в основе атомной бомбы и политики ядерного паритета и сдерживания. "Скорость света постоянна относительно любых наблюдателей" – эта внешне достаточно простая констатация лежит в основе теории относительности. Так что достаточно простые в своей

основе процессы и схемы вполне могут породить достаточно сложные последствия.

Собственно говоря, даже на обывательском, пользовательском уровне понятно, что цифровые технологии способны моделировать даже саму нашу жизнь. Разве более или менее сложные компьютерные игры – это не попытка воспроизвести в виртуальном пространстве именно саму жизнь, к тому же не копируя ее примитивно, а предлагая варианты, которые в реальности вообще невозможны?

1. Генокод. Душа и свобода воли

Возникает хороший вопрос: можно ли утверждать, что в основе живых существ, в том числе человека, тоже лежит простой двоичный код? Тут ситуация непростая, с одной стороны, есть очевидные открытия в области генной инженерии, согласно которым, например, человеческое тело формируется и развивается на основе информации, содержащейся в геноме. Внешне, вроде бы, гены и хромосомы выглядят как носители чего-то, очень похожего на обычные программы, которые используются в вычислительных машинах[41]. Носители ведь могут быть разными: магнитная лента, перфокарта, лазерный диск. Почему бы молекуле ДНК не быть таким же носителем? При этом пока ученым не удалось найти в устройстве человека чего-то такого дополнительного, что отличало бы его от обычной вычислительной машины. Речь идет, например, о таких понятиях, как "душа", "свобода воли"[42], "свобода выбора" (стохастический или детерминистский поход). Уместно также упомянуть, что основатель кибернетики Н. Винер исходил как раз из подобия процессов управления, связи в машинах, живых организмах и обществе[43].

С другой стороны, если на миг допустить, что у человека нет никакой такой особой "души", и он, как машина, не обладает свободой

---

[41] Конечно, это очень упрощенное изложение сути кодирования информации в молекуле ДНК. См., например: *Волобуев А.Н., Петров Е.С., Романчук Н.П. и др.* Биофизические основы организации генома и нейропластичности // Здоровье и образование в XXI веке. 2017. № 10. С. 324–325.

[42] *Стрельцова Г.Я.* Парадоксы свободы воли // Вестник Московского университета. Сер. 7. Философия. 2015. № 6. С. 83–87.

[43] *Винер Н.* Кибернетика, управление и связь в животном и машине. М.: Наука, 1983; *Винер Н.* Кибернетика и общество. М.: ИЛ, 1958.

воли[44], то тогда возникает пара очень серьезных проблем. Мы, как живые существа, субъективно убеждены, что у нас есть свобода выбора тех или иных поступков. Как быть с этим субъективным ощущением? Оно, что, ложное?

Вторая проблема еще более радикальная: все человеческое общество устроено на презумпции наличия свободы воли, что выражается, например, в свободе выбора договора и способа защиты своих прав в гражданском праве. Это и уголовная ответственность: человека сажают в тюрьму за то, что он поступил плохо, а мог бы поступить хорошо, по закону. Герою дают медаль за то, что он решил не отсиживаться в сторонке, а бросился совершать героический поступок. Но если человек – просто биологическая машина, тогда какой спрос с машины? Тогда получается, что все устройство человеческого общества – полная бессмыслица.

Такая двойственная ситуация приводит к тому, что в общепринятых интерпретациях человек рассматривается как нечто, принципиально отличное от машины. При этом как бы предполагается, что хотя пока наука не доказала, в чем именно заключается это отличие, но когда-нибудь "потом" обязательно докажет. Мало того, человек как нечто особое противопоставляется и всем остальным живым существам. У тех – "инстинкты", а у человека нечто иное: привычки, приобретенные навыки, образ поведения, когнитивные функции. То есть вроде бы как бы предполагается, что остальные живые существа ближе к биологической машине, чем человек, хотя тоже не машины.

Кстати, как пример живой машины, фигурирует, например, такое понятие, как "зомби". Внешне у него все признаки человека, но поведение какое-то особое, предполагающее как минимум отсутствие "души". "Зомби" – обычный персонаж из фильмов ужасов и соответствующей литературы. Тут же можно упомянуть и голем[45].

---

[44] Тут следует упомянуть, что, например, В.М. Глушков отдавал предпочтение детерминистскому подходу. *Глушков В.М.* Кибернетика, вычислительная техника, информатика. Избранные труды: в 3 т. Киев: Наукова думка, 1990.

[45] *Мельников Г.П.* Живое/неживое: голем, машина и концепция современной культуры Э. Фромма // Вестник культурологии. 2002. № 2. С. 89–91.

2. Тест Тьюринга и "китайская комната"

Теперь пора упомянуть о так называемом "тесте Тьюринга"[46] и "китайской комнате"[47]. С помощью этих экспериментов ученые пытались разработать методику, как провести грань между машиной и человеком. Смысл теста Тьюринга заключался в том, что человек, участвовавший в эксперименте, должен был только по ответам определить, кто именно ему отвечает, человек или машина. Семьдесят лет назад машины были довольно несовершенные, отделить ответы машины от ответов человека было более или менее просто. В наши дни ситуация иная. Например, в ходе эксперимента (конференция по искусственному интеллекту Opentalks.Al, 2019) машина (бот) пыталась выдать себя за человека, а человек пытался запутать экспериментатора и выдать себя за бота. Итоги следующие: человек легко запутывал экспериментатора, ему удалось выдать себя за машину в 75 процентах случаев. А машина смогла выдать себя за человека более чем в 50 процентах случаев. То есть более чем в половине случаев экспериментатор был убежден, что общается с живым человеком.

"Китайская комната" – это эксперимент, призванный опровергнуть тест Тьюринга и доказать, что машина неспособна обладать сознанием, как человек. Смысл эксперимента заключается в следующем: представим себе, что в комнате, заполненной китайскими иероглифами, находится экспериментатор, который не знает китайского языка. Но у него есть подробная инструкция (алгоритм), которая четко предписывает, какой набор иероглифов надо подобрать в ответ на определенное сочетание полученных иероглифов. По замыслу автора эксперимента (Джон Серл), человек, который знает китайский язык и находится снаружи "китайской комнаты", передает внутрь какой-то вопрос на китайском языке. Экспериментатор, который находится внутри и не знает ни китайского языка, ни значения отдельных иероглифов, согласно инструкции подбирает ответ. Конечно же, он не понимает вопрос и не знает содержание составленного им же ответа. Но поскольку инструкция составлена

---

[46] *Turing A.M.* The chemical basis of morphogenrsis // Philosophucal transactions of the Royal society of London. Ser. B, Biological sciences. 1952. Vol. 237, N 641 Aug. 14. P. 37–72.

[47] *Черепанов И.В.* В защиту аргумента китайской комнаты Д. Серла // Вестник ЛГУ им. А.С. Пушкина. 2014. № 2. С. 41–50.

особо точно, ответ получается вполне осмысленным. Парадокс, как считал Д.Серл, заключался в том, что автор ответа не сознавал, что именно он написал, но тем не менее ответ выглядел как плод человеческой деятельности. Получается, что и машина, "не сознавая", что именно она делает, может давать такие ответы, которые выглядят как ответы человека.

Тут нужно отметить, что в научном сообществе нет единой оценки указанного эксперимента, хотя до сих пор дискуссия идет довольно жаркая. Многие ученые не без оснований полагают, что Серл не доказал, что между человеком и машиной существуют принципиальные различия (в частности, применительно к "сознанию").

В связи с "китайской комнатой" следует упомянуть такие понятия, как "сильный интеллект" и "слабый интеллект"[48]. Внутри "китайской комнаты" сидит, по замыслу Серла, носитель "слабого интеллекта" (если это машина), который способен связно ответить, но по сути лишь имитирует человека, "не понимая", что именно делает. Однако в научном сообществе достаточно сторонников "сильного интеллекта", которые считают, что, в принципе, может существовать программа, с помощью которой машина будет не только отвечать, как человек, но и "понимать", что именно она делает.

Сильным ИИ (Strong AI) нередко называют обобщенный искусственный разум (Artificial general intelligence), который теоретически может быть воплощен некоторой машиной, проявляющей способности, сравнимые с человеческими способностями. Сильный ИИ наделяют такими чертами, как способность ощущать (sentience), способность выносить суждения (sapience), самоанализ (self-awareness) и даже самосознание (consciousness). Слабым ИИ (Weak AI) называют не имеющий разума и умственных способностей (Non-sentient computer intelligence) ИИ, ориентированный на решение прикладных задач[49]. Тут уже уместно отметить, что некоторые разработчики систем искусственного интеллекта придерживаются концепции приоритета поведенческого

[48] См., например: *Гутенев М.Ю.* Проблема искусственного интеллекта в философии xx века // Вестник ЧГАКИ. 2012. № 4 (32). С. 77–80.

[49] *Смирнов А.И.* Современные информационные технологии в международных отношениях // МГИМО(у) МИД РФ, Центр международной информационной безопасности и научно-технологической политики. М., 2017. 334[2]. С. 53.

подхода (автономные агенты, адаптивное поведение)[50], другие – сторонники логического знаниевого подхода[51].

А что, если когда-нибудь, используя достижения генной инженерии, удастся с нуля создать геном человека и записать его на соответствующий органический носитель? Что получится в результате? Именно человек? Или нечто иное? Ведь при таком методе создания человека за скобками оказываются "душа" и "свобода воли". Да и откуда им взяться? Ведь в этом случае генный инженер будет использовать в качестве исходных материалов предметы, которые не обладают никакими волшебными свойствами. Откуда же они, эти свойства, в таком случае возьмутся? Получается парадокс: ученые уже сейчас могут твердо назвать все составные элементы, из которых состоит человек. По отдельности эти молекулы и соединения, надо полагать, подчиняются правилу: у одной причины может быть только одно следствие. То есть на этом уровне причинно-следственная связь присутствует. А когда эти элементы собраны вместе, причем именно таким образом, как они собраны в человеческом организме, то должно появиться новое качество: окончательный продукт (человек) вдруг перестает подчиняться причинно-следственным связям и получает новое, по сути, волшебное (божественное) качество. Он теперь сам, своей волей может в одной и той же ситуации определять разные последствия. То есть один раз дважды два – четыре, а другой раз – уже пять. Формально современные представления о человеке именно такой результат и предполагают. Но откуда же взялись эти новые волшебные качества? Какова их природа и на каком материальном носителе они существуют? Ведь в качестве исходного материала описываемый гипотетический опыт не предполагает использование каких-то особых материалов. Похоже, что, несмотря на то что современная наука и политика решительно отрицают божественное происхождение человека, тем не менее они в этом случае приписывают ему, по сути, именно божественные (волшебные) свойства, не имеющие ясного научного обоснования.

---

[50] *Цетлин М.Л.* Исследования по теории автоматов и моделирование биологических систем. М.: Наука, 1969; *Турчин В.Ф.* Феномен науки. Кибернетический подход к эволюции. М.: Наука, 1993; *Редько В.Г.* От моделей поведения к искусственному интеллекту. 2-е изд., стереот. Науки об искусственном. М.: URSS, 2010.

[51] *Meyer J. and Wilson S.* (eds.) From Animals to Animats. Proceedings of the First International Conference on Simulation of Adaptive Behaviour. Cambridge, MA: MIT Press, 1991; *Maes P.* Modeling Adaptive Autonomous Agents // Artificial Life. An Overview / Ed. by Langton C., Boston: MIT Press 5th edition 2000 (1995).

3. Естественный интеллект и искусственный интеллект

Почему, говоря о двоичном коде как основе цифровых технологий, мы вдруг вспомнили о человеке и иных живых существах? Основания так поступить существуют достаточно весомые, часть цифровых технологий – это так называемый "искусственный интеллект". При этом предполагается, что искусственный интеллект как бы копирует естественный интеллект, но при этом все-таки от него отличается. Ведь машины – не живые существа? А человек – не машина? В любом случае, если речь идет о создании искусственного интеллекта, похожего на естественный, то предварительно желательно выяснить, что собой представляет этот самый "естественный интеллект"[52]. Что именно мы копируем?

Может быть, если бы тема данного исследования была иная, можно было не заострять внимание на том, что такое естественный интеллект, поскольку тема эта довольно скользкая: есть шанс поставить под сомнение исключительно устоявшиеся и, якобы, совершенно бесспорные константы современной науки. Но в данном случае речь идет об обеспечении именно безопасности. Понятно, что безопасность может быть эффективной только в том случае, если рассматриваются не только очевидные угрозы, но и широкий круг предположительных угроз. Если обеспечивать эффективную безопасность, то, конечно же, надо учитывать ситуации внешне самые маловероятные или даже те, которые выглядят вовсе невероятными.

Использование цифровых технологий – это не только компьютерные игры или системы связи. Это создание искусственных интеллектуальных систем. А что, если естественный интеллект имеет чисто цифровую природу? Как правило, в настоящее время такая возможность отрицается, естественному интеллекту приписываются свойства, которыми, якобы, не могут обладать машины, вычислительные машины (в основном речь идет о "свободе воли", но не только). А что, если такой подход – не точный, а то и вовсе ошибочный? Манипуляции с человеческим геномом почти повсеместно серьезно ограничиваются, и понятно, почему: в результате может быть создано живое существо, похожее на человека,

[52] *Разумов В.И., Сизиков В.П.* Естественный и искусственный интеллект и их соотношение // Вестник ОмГУ. 2019. № 1. С. 98–105.

но обладающее другими свойствами. Создание такого существа чревато существенными социальными и формальными (юридическими) осложнениями. То есть манипуляции с человеческим геномом ограничены потому, что могут возникнуть серьезные угрозы для человечества. Так, может быть, точно так же надо в какой-то мере ограничивать и манипуляции с двоичным кодом? Вдруг в результате таких манипуляций может быть создано "нечто", не являющееся машиной в обычном ее понимании, но обладающее точно таким же интеллектом, как и человек, при этом превосходящее человека по целому ряду параметров (быстродействие, безошибочность принятия решений, совершенство периферийных устройств)[53]? Вдруг такое "нечто" будет вести себя враждебно по отношению к человеку? Является ли это угрозой, пусть хоть немыслимо маловероятной, которую надо учитывать при построении систем обеспечения безопасности человечества? Конечно, надо.

Вообще, специалисты какого именно профиля должны заниматься созданием искусственного интеллекта? Пока тут безраздельно властвуют программисты. Но ведь они – не биологи. Что именно они пытаются создать, не понимая, что такое "естественный интеллект"? Программисты и математики, конечно, с такой постановкой вопроса не согласны и считают, что разгадка феномена свободы воли заключается либо в особых математических построениях, либо, например, в феноменах квантовой механики. Грубо говоря, они пытаются найти математические формулы, когда один раз дважды два – это четыре, а другой раз – уже пять или три (детерминированная информация правил или стохастическая информация неопределенности, энтропия).

В квантовой механике нередко ссылаются на квантовую неопределенность, в обыденном обиходе сформулированной Эрвином Шредингером в виде шутливой формулы: "Кот Шредингера наполовину жив, а наполовину – мертв"[54]. Но ведь неопределенность – это не эквивалент отсутствия причинно-следственной связи! Впрочем, не будем предвосхищать будущих открытий математиков и физиков, но лишь отметим, что даже если будет доказано, что в математике и

---

[53] Технокреационизм. См., например: *Галкин Д.В.* Живое из неживого: философско-методологические проблемы искусственной жизни // Вестн. Том. гос. ун-та. Философия. Социология. Политология. 2011. № 2 (14). С. 20–33.

[54] Со взглядами Шредингера можно ознакомиться, например, в следующем издании: *Шредингер Э.* Что такое жизнь? М.: АСТ, 2018.

квантовой физике возможны ситуации, когда одна и та же причина вызывает разные последствия – это все равно вряд ли будет эквивалентом "свободы воли". Скорее, возникнет так называемый "эффект бабочки", когда малейшее изменение в исходных данных влечет значительные иные последствия, но только в отдаленном будущем.

Но ведь субъективно "свобода воли" – это, скорее всего, нечто иное по своей природе. Ни о каком отдаленном последствии тут речь не идет. Человек субъективно уверен, что он может весь и сразу же, в тот же момент, поступить не так, а иначе. Какое уж тут отдаленное последствие?!

Автор тут умышленно не углубляется в технические аспекты исследования проблемы свободы воли. В кибернетике (посткибернетике) ей уделено немало внимания, есть соответствующие сложные объяснения, типа закона сохранения информации Л. Бриллюэна, соединяющего детерминированную информацию и энтропию (вероятную информацию)[55], или принципа смешанного экстремума для решения противоречий внутри системы, баланса требований и детерминистско-вероятностных соотношений[56]. Тут же уместно упомянуть и синергетику[57]. Однако для данного исследования, посвященного вопросам безопасности, достаточно констатации, что мы не можем полностью исключить того, что человек и машина устроены, в принципе, одинаково.

4. Цифровые технологии как самостоятельный источник угроз для человека. Очевидные угрозы

Итак, не исключено, что цифровые технологии и сами по себе могут создавать угрозы для человека. Точнее, можно говорить о продуктах, созданных с использованием цифровых технологий. Однако о каких именно угрозах может идти речь? Попробуем привести в подтверждение этого тезиса несколько конкретных примеров.

Как известно, в военной сфере все чаще применяются беспилотные летательные аппараты (БПЛА). Для удобства будем оперировать уже более или менее устоявшимся термином "дрон". Дроны нередко

[55] *Бриллюэн Л.* Наука и теория информации. М.: ИФМЛ, 1960.
[56] *Теслер Г.С.* Новая кибернетика. Киев: Логос, 2004.
[57] *Хакен Г.* Синергетика. М.: Мир, 1980.

используются как средство ведения воздушной разведки, но не только. Боевые дроны вооружены различными средствами и по команде оператора могут наносить достаточно разрушительные удары по соответствующим целям.

Однако разрабатываются и такие модели дронов, которые самостоятельно, без команды оператора, выбирают и поражают те или иные цели[58]. Как правило, речь идет о таких целях, как "террористы". Формальное обоснование таких разработок понятно: террористы нередко находятся в труднодоступных местах, горах, джунглях. Дрон может залететь достаточно далеко и сблизиться с такими целями для нанесения удара. Но будет ли в этот момент существовать устойчивая связь с оператором? А если террористы умышленно будут ставить помехи, чтобы помешать боевому дрону выполнить свою задачу? Для того чтобы преодолеть такие проблемы, предполагается оснастить дрон программой, позволяющей ему самостоятельно определять и уничтожать цели (т.е. террористов). Понятно, о каких конкретно признаках может идти речь: о человеке, на котором можно явно различить оружие. При этом такой человек должен находиться на территории, где по определению не должно быть мирных жителей.

Однако отметим, что тут изобретатели боевых дронов делают принципиально новый и опасный шаг в использовании цифровых технологий. Если окончательное решение на поражение цели принимает не оператор, а машина (дрон), не исключена возможность, что, несмотря на все перестраховки, будет убит невинный человек, мирный житель. Например, охотник, который в погоне за дичью забрел в местность, где обосновались террористы. Охотник несет ружье, которое будет распознано машиной как оружие. И будет убит, причем именно машиной, а не по конкретному определенному решению оператора этой машины. Это угроза для людей? Несомненно.

Мы привели пример, касающийся только беспилотных летательных аппаратов. Но, как говорится, "лиха беда начало". Может возникнуть искушение оснащать такими программами и другие виды оружия. Зачем рисковать своими солдатами, выводя их на поле боя и делая уязвимыми для противника? Лучше использовать машины, которые управляются дистанционно. А если и их оснастить программами, позволяющими машине самостоятельно принимать

[58] См., например: *Габов А.В., Хаванова И.А.* Автономия боевых роботов и право // Пермский юридический альманах. 2019. № 2. С. 361–378.

решение на определение и уничтожение цели? Например, небольшие бронированные машины, миниатюрные танки? А мины? Может, и мины должны убивать не просто любого человека, который на них наступил, а только определенные цели?

Понятно, что такая программа позволит повысить эффективность использования машин в бою. Машина намного быстрее человека способна распознать цель и принять решение на ее уничтожение. Машина не подвержена эмоциям, у нее всегда стабильное "здоровье", она неприхотлива, не требует условий, необходимых для солдата (питание, отдых, медицинская помощь, определенные погодные условия). Но если окончательное решение будет принимать именно машина, а не человек, будет существовать угроза убить вовсе не бойца противника, а невинного человека или даже группу людей. Машина в результате использования таких программ (цифровых технологий) превращается в самостоятельный источник угроз для человека. Эта проблема формулируется как сохранение человеческого контроля за искусственным интеллектом в смертоносных автономных системах вооружений (САС)[59]. Обсуждение ее с попыткой сформулировать соответствующие международно-правовые нормы ведется, в частности, в рамках Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие.

Приведем еще один пример: так называемая "серая слизь"[60]. Возможно ли создание небольшого по размеру робота, выполняющего поставленную человеком задачу? Они уже созданы и нередко фигурируют как "нанороботы". А что, если будет создан робот,

---

[59] *Петрова Д.А., Гайворонская Я.В., Мамычев А.Ю.* Смертоносные автономные системы: этические, юридические, политические проблемы и перспективы их решения // Территория новых возможностей. 2019. № 4. С. 33–43; *Шибаева К.В., Холова Л.Н.* Три закона робототехники Айзека Азимова: к вопросу гуманности применения смертоносных автономных систем вооружения на войне // Теология. Философия. Право. 2018. № 4 (8). С. 28–41.

[60] *Дрекслер Э.* Всеобщее благоденствие. Как нанотехнологическая революция изменит цивилизацию. М., Издательство Института Гайдара, 2014; *Кокорина А.В., Летунова О.В., Сергеева М.А.* Анализ концепций о будущем человечества // Символ науки. 2016. № 12-3. С. 51; *Ефременко Д. В.* Социальные науки и развитие конвергентных технологий // Инновации. 2012. № 5 (163). С. 82; *Кузнецов В.А.* Эволюция систем искусственного интеллекта (ИИ), появление цифровых и иных сверхтехнологий и их влияние на изменение социальной реальности, на создание нового качества общественной жизни // Вестник ЧелГУ. 2019. № 8 (430). С. 6.

который сможет сам себя воспроизводить? Теоретически такое вполне возможно. Мало того, не исключено, что в каких-то лабораториях задача уже решена и в практическом ключе. Одна из проблем заключается в том, что в вычислительных машинах в качестве материала для полупроводников используется кремний. Он всем хорош, более или менее сохраняет свои свойства в разных условиях, в том числе и при повышенной температуре. Однако производить его довольно сложно. Изготовление такого кремния возможно только в рамках хорошо отлаженного промышленного производства. Понятно, что такое производство невозможно так автоматизировать, чтобы полностью перепоручить машинам. Тут без участия человека и без использования промышленных зданий и машин никак не обойтись.

Однако кремний – вовсе не единственный материал, пригодный для изготовления полупроводников. Например, такую роль могут играть сверхтонкие органические пленки. Мало того, есть основания полагать, что для изготовления электронной начинки, основанной на полупроводниках из таких органических пленок, не потребуется никаких сложных и громоздких промышленных производств. То есть вполне возможно, что будет создан миниатюрный робот (нанороботт), который будет способен самостоятельно, без участия человека, воспроизводить устройства, подобные себе. Уже сам по себе этот процесс, если он не контролируется человеком, может создать для него угрозу: вдруг такие нанороботы будут использовать в качестве строительного материала органические вещества? Не получится ли так, что в конечном итоге они просто сожрут всю органику на планете? Конечно, это достаточно гипотетическая ситуация, но она довольно показательная. Сбрасывать ее со счетов, пытаясь обеспечить безопасность человека, никак нельзя. Указанная совокупность микроскопических вычислительных машин, способных себя воспроизводить, нередко формулируется в научной литературе как уже упомянутая "серая слизь".

Выше мы рассмотрели случаи, когда угрозу представляет машина, оснащенная соответствующей программой. То есть речь идет не только о "софте", но и о "железе". А возможна ли ситуация, когда угрозу для человека представляет сам софт, сами программы, созданные с использованием цифровых технологий? Формально программа должна существовать на каком-то материальном носителе ("железе"). Но далеко не всегда такой носитель – конкретно определен. Например, программы, существующие в пространстве

Интернета, могут работать без конкретного определенного носителя. Ведь хорошо известна ситуация, когда для хранения информации используются вычислительные машины конечного пользователя. И далеко не всегда конечный пользователь сознает, что его персональный компьютер обслуживает не только его, но и какого-то другого пользователя.

Это один конкретный пример, но можно привести и другие, подтверждающие, что программы в Интернете далеко не всегда нуждаются в определенном носителе, они могут кочевать по разным носителям, причем этот процесс достаточно сложно отследить, а тем более, контролировать. Наверное, в таком случае можно говорить, что программа, основанная на использовании цифровых технологий, существует, по сути, самостоятельно, как виртуальная реальность, без определенного материального носителя. А что это за программа? Может ли быть разработана и внедрена в Интернет, например, программа, самостоятельно ворующая персональные данные пользователей? Или даже программа, разрушающая другие программы, к примеру, те, на основе которых работает энергетика другой страны? Все это уже далеко не фантастические домыслы, такие работы ведутся в соответствующих лабораториях.

Тут мы сталкиваемся с ситуацией, когда программа по заранее определенному программистом и оператором алгоритму, может, по сути, сама принимать решения, которые могут иметь достаточно разрушительный характер, как для отдельных людей, так и даже для государственных институтов. Но можно ли гарантировать, что такая программа никогда не выйдет из-под контроля и не примет решений, которые не были запланированы ее изобретателями?

Хорошо известен эпизод, когда разработанная американцами программа была тайно внедрена в систему управления иранского производства обогащенного урана и разрушила часть центрифуг по обогащению урана (Stuxnet). Но тут алгоритмы, заложенные программистами, были выполнены точно, программа не вышла за пределы поставленных задач. Можно ли, однако, гарантировать, что никто не изобретет программу, которая внедрится в производственные процессы, связанные, например, с микробиологией, и не выпустит в свободный оборот смертоносный вирус? Или не выведет из строя

объекты критической инфраструктуры?[61] Видимо, по крайней мере, теоретически, такую опасность нельзя исключать. И вовсе нельзя исключать, что предположение, которое сегодня выглядит скорее как научная фантастика, завтра не превратится в самую настоящую реальность.

5. Неочевидные угрозы

А можно ли гарантировать, что человек, активно используя цифровые технологии, в результате, вольно, или невольно, не создаст другое живое существо? Существо, которое станет его конкурентом? Такое существо может быть из плоти и крови, как и сам человек, а может быть изготовлено и из металла и кремния, еще из каких-то материалов. Как представляется, гарантий, что такое никогда не случится, никто дать не может. Конечно, такая угроза пока представляется совсем маловероятной, даже, скорее, фантастической. Но так ли это на самом деле? Попробуем в этом разобраться.

Цифровыми технологиями занимаются, как правило, математики и программисты. Однако, по крайней мере, частично такие цифровые принципы организации информации лежат и в основе всех живых существ, используются в генокоде[62]. И манипуляциями с геномом занимаются совсем другие специалисты, в частности, генетики и микробиологи. Казалось бы, использование одних и тех же технологий означает, что, по крайней мере, контроль, а может быть, и организация и регулирование процесса манипуляций должны осуществляться на основе одних и тех же правил. Но пока этого не произошло, поэтому генетики и микробиологи ведут свои работы самостоятельно, опираясь на собственные специфические методы и руководствуясь собственными специфическими принципами и правилами.

Итак, генная инженерия. Особо выдающиеся достижения в этой области – это изменение генетического кода растений и животных с целью придать им особые свойства. Как правило, речь идет о

---

[61] *Тращенков С.В., Егоров В.Е., Смирнов В.Д. и др.* О динамической безопасности электроэнергетики // Вестник Псковского государственного университета. Серия: Экономика. Право. Управление. 2013. № 3. С. 131.

[62] Тут автор допускает определенное упрощение, возможно, кодирование в генокоде нельзя свести только к бинарному коду.

повышении, например, урожайности. Насколько такие операции с геномом представляют опасность для человека? Пока говорят о том, что люди, употребляющие в пищу генетически модифицированные продукты (ГМО), рискуют своим здоровьем. Но твердых рекомендаций и выводов пока эксперты не выносят[63].

Манипуляции с геномом человека во многих странах нередко серьезно ограничены, а то и запрещены законом[64]. Но гарантий, что такие манипуляции никем и никогда не будут проводиться, ясное дело, никто дать не может. А в результате может быть создано живое существо, которое будет, например, более совершенным, чем человек. И возникнет ситуация серьезной конкуренции, которая будет чревата неблагоприятными последствиями для людей с геномом, не подвергшимся изменениям.

Микробиологи совершают манипуляции над микроорганизмами. Методы их работы специфичны и, как правило, отличаются от методов, используемых в генной инженерии. Но цель манипуляций точно такая же: изменить свойства исходных вирусов и бактерий, что возможно только в случае изменения генома. Излишне говорить, что деятельность микробиологов представляет исключительную опасность для человечества. Новый вид вируса или бактерии, вырвавшийся из-под контроля, может стать причиной широкомасштабной эпидемии и привести к гибели значительного количества людей.

Кстати, геном меняют и селекционеры. Но у них тоже свои специфические методы работы, они не вторгаются непосредственно в систему кодирования информации в геноме, однако, как и микробиологи, отбирают из каждого нового поколения особей с походящими данными. И проделывают эту операцию подчас очень много раз, пока не добьются искомого результата.

А могут ли создать новое живое существо программисты, разрабатывающие программное обеспечение для ЭВМ? Пока считается, что такое в принципе невозможно. Однако, как

---

[63] *Осипова Г.С.* Невидимая опасность ГМО // Здоровье – основа человеческого потенциала: проблемы и пути их решения. 2011. № 1. С. 620–622; *Васильева А.С., Романцева Е.В.* ГМО – мифические опасности // БМИК. 2016. № 5. С. 668.

[64] *Казённов Д.К.* Биоэтические суждения о генной инженерии // Изв. Сарат. ун-та Нов. сер. Сер. Философия. Психология. Педагогика. 2011. № 2. С. 32–35; *Гнатик Е.Н.* Генная инженерия и биологическая безопасность // Вестник РУДН. Серия: Юридические науки. 2004. № 2. С. 79–88.

представляется, не все в этой области так уж очевидно. Предполагается, что вся вычислительная техника и программное обеспечение представляют собой лишь как бы продолжение руки человека[65]. Что-то вроде молотка, фонаря или вилки, только более сложное по устройству. Якобы цифровые технологии и устройства могут расширить способности и возможности человека, но не более того.

На чем основывается такое предположение? По сути, на том, что человек, как и другие живые существа на нашей планете, возник неким специфичным способом и при этом обладает какими-то своими особыми свойствами, совершенно недоступными вычислительным машинам. Что же это за такие за свойства? Применительно к человеку говорят, в частности, об уже неоднократно упомянутой выше "свободе воли", а применительно к остальным живым существам – об "активности". В отношении человека в обороте также такой недостаточно научный термин, как "душа"[66]. Кроме того, человеку приписывают ментальные состояния, якобы, недоступные для вычислительных машин, как-то: вдохновение, радость, злоба и т.д. В отношении человека применяют такие понятия, как "добро" и "зло".

Поскольку речь идет о безопасности человека и человечества в целом и о предотвращении потенциальных угроз, связанных с использованием ИКТ, в том числе цифровых технологий, представляется позволительным в определенной мере критически отнестись к общепринятым взглядам и теориям на природу человека и других живых существ. Любая теория может оказаться, в конечном итоге, ошибочной, в том числе и теория о происхождении всего живого на нашей планете. И ошибка в этом вопросе может дорого стоить человечеству, ведь речь идет о его безопасности, а может быть, и о выживании как биологического вида.

Не будем слишком уж углубляться в критику общепризнанных подходов, тут достаточно их просто обозначить, при этом привести также аргументы оппонентов и упомянуть об альтернативных взглядах. Однако вряд ли имеет смысл упоминать версии о

---

[65] *Лазарева Е.А.* Человек, умноженный машиной // Искусствознание. 2016. № 1–2. С. 90–113.

[66] *Петров В.В.* Душа, облачающаяся в тела, душа, ткущая тела // Schole, СХОЛЭ. 2017. № 1. С. 166–176; *Казаков Е.Ф.* От души к психике // Вестник КемГУ. 2015. № 2–4 (62). С. 206–209; *Погоняйло А.Г.* Душа/машина // Вестник СПбГУ. Философия и конфликтология. 2013. № 4. С. 39–51.

божественном происхождении человека и всего живого, они основаны не на знаниях, а на вере, и, по сути, предлагают объяснения, выглядящие как волшебные и не доступные познанию человеком. Зачем обсуждать то, что по определению является непознаваемым для нас?

Однако помимо волшебных и божественных объяснений существуют и вполне научные и материальные доводы и аргументы, а также альтернативные версии, которые могут представлять определенный интерес[67]. Как известно, общепринятой является теория эволюции, согласно которой все живое возникло на Земле в результате естественных процессов[68]. Каким-то образом смешались разные химические элементы, и возникла жизнь (возникновение живого из неживого, абиогенез). Поначалу она существовала в простейших формах, но затем стала эволюционировать, усложняться. В результате возникли именно те формы жизни и именно те виды живых существ, которые мы с вами и можем наблюдать на нашей планете.

Не будем спорить, может быть, теория эволюции и верна. Однако до сих пор не найдены до конца убедительные ответы на некоторые важные вопросы. Пройдемся по этому списку. Видимо, теория отличается от гипотезы тем, что гипотеза – это лишь смелое научное предположение. А теория – это гипотеза, которая нашла практическое подтверждение, например, в лаборатории. К сожалению, приходится констатировать, что пока в лаборатории не удалось создать жизнь из тех исходных материалов, которые существуют на Земле. То есть пока утверждение о том, что именно так возникла жизнь на Земле – это формально лишь предположение, не подтвержденное на практике. Возможно, ученые, в конце концов, смогут создать жизнь из набора органических и неорганических веществ, найдя необходимые условия. Но пока это не удалось, несмотря на очень значительные усилия.

Теория эволюции исходит из предположения, что соответствующие химические элементы соединились вместе и

[67] См., например: *Федотов В.П.* Дарвинизм vs креационизм: Pro et contra // Инновации в науке. 2017. № 1 (62). С. 20–22.

[68] См., например: *Рубцов А.С.* Чарльз Дарвин и теория эволюции // Наука и жизнь. 2009. № 1. С. 47–52.

превратились в форму жизни случайно[69]. Подсчитана вероятность такой случайности. Если отвлечься от цифр с большим количеством нулей, то некоторые специалисты формулируют такую вероятность следующей обывательской формулой: налетел вихрь, который разметал и закрутил различные предметы, находящиеся на огромной свалке, которые в конечном итоге сами собой объединились в "Боинг 747". Оставляем читателям самим оценить степень вероятности такого события.

В лабораториях ставятся самые разные научные эксперименты, чтобы подтвердить или опровергнуть теорию эволюции. Согласно этой теории живые существа в силу мутаций и естественного отбора постепенно превращались из одних видов в другие, причем все более сложные и совершенные[70]. Именно так, предположительно, и возникло все разнообразие видов живых существ. Для подтверждения этого предположения проводятся, в частности, опыты над небольшой мушкой дрозофилой. Живет эта муха меньше тридцати дней, поэтому за год сменяется довольно много поколений. Дрозофилу подвергают самым разным видам воздействий, используют радиацию, активные химические вещества[71]. Меняют условия жизни и питания. Цель – вызвать мутации, которые привели бы к возникновению нового биологического вида. Грубо говоря, чтобы из мухи получилась, например, пчела. Однако пока, несмотря на многолетние усилия, эти эксперименты успехом не увенчались. Генетические изменения возникают, у мухи может вырасти дополнительная пара крыльев или ног, меняется цвет тех или иных частей тела. Но другой биологический вид не возникает. А должен возникать, причем достаточно легко.

Эксперименты с дрозофилой касаются сложного вопроса о преобразовании одного биологического вида в другой. Как известно, все живые существа делятся на биологические виды, причем

---

[69] Конечно, есть теории, которые толкуют случайность как закономерность. См., например: *Добровольский С.Г.* Жизнь как пороговое блуждание // Общество. Среда. Развитие (Terra Humana). 2012. № 3. С. 41–47.

[70] *Шмальгаузен И.И.* Избранные труды. Пути и закономерности эволюционного процесса. М.: Наука, 1983; *Северцов А.С.* Направленность эволюции. М.: МГУ, 1990; *Симпсон Дж.Г.* Темпы и формы эволюции. М.: ИЛ, 1948; *Яблоков А.В.* Эволюционное учение. М.: Высш. шк., 1998.

[71] См., например: *Князева И.Р., Большаков М.А., Ельчанинов А.А. и др.* Сравнительное изучение действия импульсно-периодического микроволнового и рентгеновского излучений на развитие дрозофилы // Вестн. Том. гос. ун-та. 2007. № 302. С. 228–230.

межвидовой барьер – достаточно труднопреодолимый. Как правило, скрещивание разных видов не ведет к продолжению рода. На самом деле межвидовой барьер можно преодолеть, то есть можно создать новый вид живого существа. Например, известен эксперимент, когда из одного вида виноградной тли удавалось получить другой вид. Но на это ушло много лет, при этом экспериментальные особи были поставлены в очень жесткие условия, на самую грань выживания. Однако если теория эволюции верна, межвидовых барьеров вообще не должно быть, они представляют собой излишнее препятствие. Но они, несмотря на все теоретические выкладки, существуют и при этом преодолеваются с большим трудом и только в отдельных определенных случаях.

Следует также упомянуть о таких понятиях, как "микроэволюция" и "макроэволюция"[72]. Как известно, существует достаточно существенная внутривидовая изменчивость. Если объяснять этот феномен на обывательском уровне, то за счет селекции можно вывести из овчарки таксу. Но пока не удается преодолеть межвидовой барьер и вывести из овчарки, например, кошку. Не исключено, что и никогда не удастся, потому как в этом направлении были предприняты очень значительные усилия, которые так и не увенчались успехом.

Так вот, если мы говорим о внутривидовой изменчивости (овчарка и такса), это описывается термином "микроэволюция", а если о попытке преодолеть межвидовой барьер (овчарка и кошка), то это уже "макроэволюция". Критики теории эволюции указывают, что микроэволюция, бесспорно, существует, но ошибочно переносить ее в целом на устройство живого мира. Нельзя подменять макроэволюцию микроэволюцией и утверждать, что эволюция характерна в целом для всего живого, это антинаучная подмена понятий.

Еще одно обстоятельство: если эволюция действительно имеет место, то для этого необходимо, чтобы живое существо каким-то образом передавало своим потомкам приобретенный опыт. Однако, как выясняется, приобретенные признаки по наследству не

[72] *Попов А.В.* О кризисе синтетической теории эволюции и его причинах // Вестник СПбГУ. Науки о Земле. 2006. № 2. С. 9–19; *Юсуфов А.Г., Магомедова М.А.* Современное состояние учения Ч. Дарвина и его значение для биологии // Известия вузов. Северо-Кавказский регион. Серия: Естественные науки. 2009. № 5. С. 112.

передаются[73]. Точнее, существуют исключительные и даже парадоксальные случаи, когда что-то подобное имеет место. Но в целом такого явления нет. Тогда как получается, что потомки совершеннее своих предков? Этому вопросу посвящено немало научных исследований и выдвинуты соответствующие гипотезы[74]. Выдвигаются и контраргументы, например, со ссылкой, что предлагаемые объяснения процесса эволюции противоречат второму закону термодинамики. Впрочем, в научном мире достаточно гипотез, как именно формируется противодействие возрастанию хаоса, энтропии. Например, Н. Винер отождествлял количество информации как количество выбора с отрицательной энтропией[75].

Еще есть такое понятие: "несократимая сложность"[76]. Согласно теории эволюции, те или иные органы возникали у живых существ постепенно, шаг за шагом. Но если это так, то можно выявить цепочку последовательных трансформаций и вычислить, каким именно был тот или иной орган раньше. К сожалению, такой обратный отсчет далеко не всегда получается. Например, существует такой самостоятельный орган как глаз. Глаз состоит из целого набора элементов. Убери любой из них, и как орган глаз перестанет существовать. Однако тогда должен получаться какой-то промежуточный орган. Но какой? Сразу оговоримся, что сторонники теории эволюции уже давно пытаются ответить на этот вопрос, предлагая варианты, как, например, какая-то кость в скелете постепенно трансформируется в ухо[77] или глаз. Убедительны ли эти предположения?

Еще один пример из этой области – это растения-хищники, которые, например, охотятся на насекомых. Устройство таких растений довольно сложное. И в этом случае, по мнению автора, также не получается предложить убедительную версию, каким было предыдущее более простое устройство растения.

---

[73] *Трофимов В.Н.* Искусственный интеллект: добро и зло как запретный плод. М.: Дашков и Ко, 2011. С. 40–41.

[74] *Гринченко С.Н., Щапова Ю.Л.* О биологической предыстории археологической эпохи: числовое моделирование // Biocosmol. – neo-Aristot.. 2017. № 1. С. 117–140.

[75] *Винер Н.* Кибернетика, управление и связь в животном и машине. М.: Наука, 1983.

[76] *Щеголев С.Ю.* Современные взгляды на эволюцию: о роли горизонтального переноса генов // Известия Вузов. ПНД. 2013. № 4. С. 43–76; *Behe M.J.* Darwin's black box. The biochemical challenge to Evolution. N.Y.: Simon & Shuster, 1998.

[77] Тут нередко ссылаются на три человеческие слуховые косточки и скулы акулы.

А клетки, из которых состоят живые организмы? У некоторых таких клеток бывает до сорока тысяч функций. Но если ликвидировать хотя бы одну из них, клетка погибает. А должна переходить в какое-то более простое состояние. Опять феномен несократимой сложности.

Вымирание видов[78]. Если теория эволюции верна, то количество видов живых организмов на Земле должно возрастать. Но, как известно, в настоящее время это количество не возрастает, а, наоборот, стремительно уменьшается, каждые пятьдесят лет – примерно вдвое. При этом количество видов насекомых уменьшается еще быстрее[79]. По некоторым оценкам, насекомые почти полностью исчезнут через сотню лет. Даются прогнозы и по вымиранию человека как биологического вида[80]. Все это больше похоже на деградацию, причем довольно быструю, а не на эволюцию.

Но почему это происходит? Климат на планете достаточно щадящий, никакие астероиды на Землю не падают, а супервулканы не извергаются. Как правило, тут специалисты ссылаются на так называемый "антропогенный фактор", то есть на результаты деятельности человека. Но ведь есть районы планеты, например, Амазонка или Конго, где практически нет никакой деятельности человека, тем более ядовитых промышленных производств. Но и там взрывного роста видов живых существ пока не замечено, в лучшем случае речь идет о десятках открытых новых видов за год, а должны быть сотни тысяч и миллионы. Сторонники теории эволюции тут ссылаются на то, что работа по выявлению новых видов ведется недостаточно масштабно.

Ради справедливости необходимо отметить, что новые виды живых существ все-таки появляются. Но, во-первых, это происходит достаточно редко (или ученые просто не замечают части появившихся новых видов?). Во-вторых, если новый вид появляется, например, за счет деления генома, можно ли считать, что такой вид обладает

---

[78] *Снакин В.В.* Вымирание видов // Жизнь Земли. 2017. № 3. С. 321–337.

[79] Насекомые начали вымирать со скоростью 2,5% в год. МК, 13.02.2019. URL: https://volg.mk.ru/science/2019/02/12/nasekomye-nachali-vymirat-so-skorostyu-25-v-god.html; Ничего живого. Ученые зафиксировали начало нового массового вымирания. URL: https://news.mail.ru/society/37268331/.

[80] *Мокий В.С., Лукьянова Т.А.* Трансдисциплинарные аспекты массовых вымираний в биосфере Земли (логика и прогнозы) // Universum: химия и биология. 2015. № 5 (13).

какими-то дополнительными качествами? Вряд ли. Однако в таком случае это уже не процесс эволюции.

Если живые существа в результате эволюции становились все более совершенными и превращались из одного вида в другой, то палеонтологи должны находить остатки большого количества переходных видов. Однако пока их если и находят, то совсем не в таких количествах, которые должны быть. Как правило, в качестве переходного вида указывают на археоптерикса, что-то среднее между летающим ящером и птицей. Найдено уже около четырех десятков скелетов этих существ.

Ссылались также на так называемую кистеперую рыбу, у которой плавники похожи на ноги. Предполагалось, что именно так, постепенно, живой мир вышел из воды на сушу, при этом у отдельных особей плавники постепенно трансформировались в ноги. Однако такое предположение исходило из того, что кистеперая рыба жила на границе воды и суши. Однако, как оказалось, этот вид рыб вовсе не вымер и существует до сих пор. Но он оказался глубоководным. То есть конструкция постепенного выхода на сушу, по крайней мере на этом примере, не получилась. Отметим, однако, что сторонники теории эволюции предлагают рассматривать в качестве переходных видов довольно много вариантов тех или иных существ, как давно вымерших, так и существующих на нашей планете сейчас.

Кстати, далеко не все ученые соглашаются, что найденные переходные виды – именно переходные. Например, высказывается мнение о мозаичной структуре соответствующих живых существ[81]. Такой подход предполагает, что речь не идет ни о каком переходе от одного вида к другому. Мозаичность – значит, что в силу каких-то причин происходит использование ряда самостоятельных элементов в разных комбинациях. Какая-то высшая инстанция, Инженер с большой буквы, экспериментирует с разными элементами конструкции, соединяя их то так, то сяк? Предположение звучит вполне фантастически[82].

Еще один вопрос – почему человек и некоторые другие живые организмы спят? Что такое "сон"? Как известно, среди людей встречаются такие феноменальные личности, которые никогда не

[81] "Мозаичная эволюция" и "параллельная эволюция". См.: *Патцельт В.Д.* Исследуя историю: очерк эволюционной морфологии // Полит. наука. 2012. № 4. С. 68–69, 78–79.

[82] Такой подход перекликается с монадой пифагорийцев.

спят, у них участки мозга работают попеременно. Но ведь отсутствие сна – это колоссальное эволюционное преимущество! Особи, которые никогда не спят, должны иметь значительное преимущество, хищник никогда не застанет их врасплох спящими, у них намного больше времени для поиска пищи. Эволюционный отбор, по логике, должен был привести к тому, что виды живых существ обходились бы без сна. Но реальная ситуация – ровно обратная.

Вообще, хороший вопрос, имеет ли место именно эволюция живых организмов? Можем ли мы утверждать, что каждое новое поколение – более совершенное, чем предыдущее? Когда говорят про эволюцию, нередко ссылаются на изменения, которые очевидно присутствуют в человеке ряда последних поколений. Человек стал жить дольше, люди стали выше ростом, более здоровыми, спортивные рекорды возрастают. Однако является все это доказательством именно эволюции? Или это результат достижений в области медицины, повышения качества потребляемых продуктов, более изощренных методов подготовки спортсменов? Однозначного ответа тут, пожалуй, пока нет.

А что является основополагающим "кирпичиком", из которого состоят живые организмы? Это аминокислоты. В природе аминокислот – сотни, но в строительстве генома участвует всего двадцать определенных аминокислот. Они бывают так называемыми левозакрученными и правозакрученными. Если бы эти вещества случайно стали строительным материалом для живых организмов, то левозакрученные и правозакрученные аминокислоты встречались примерно поровну. Однако на практике это не так: все двадцать аминокислот – левозакрученные. Эволюционисты дают тут довольно незамысловатое объяснение: это произошло случайно. Впрочем, выдвигаются и иные версии этого феномена[83].

Есть и другие соображения, которые ставят для сторонников теории эволюции сложные вопросы. Как известно, много миллионов лет назад на Земле случались оледенения. Единого мнения о сроках и масштабах оледенений среди специалистов нет, но можно, видимо, говорить о таком событии, случившемся 600 миллионов лет назад, хотя есть основания предполагать значительное оледенение и ближе к нам, например, в 200 миллионов лет. Оледенение, значит, значительная часть планеты, а может быть, и вся планета имеет

[83] *Кабалдин Ю.Г.* Квантовый подход к эволюции сложных систем // Труды НГТУ им. Р.Е. Алексеева. 2011. № 3. С. 103–109.

температуру ниже нуля по Цельсию, причем достаточно продолжительное время. Понятно, что практически никакие известные нам живые организмы не могут выжить в таких условиях. Однако могли выжить цианобактерии, которые существовали у геотермальных источников. Но в таком случае из цианобактерий получилось все имеющееся разнообразие живых организмов, березы и елки, слоны и носороги, а также и человек.

Оледенение было необходимо упомянуть потому, что сторонники теории эволюции, когда полемизируют со своими оппонентами, в случае сложных вопросов нередко ссылаются на то, что в лаборатории можно ставить опыты продолжительностью в лучшем случае в сотни лет, а природа имела в запасе миллиарды лет. Однако фактор оледенения серьезно ослабляет ссылку на миллиарды. Никаких миллиардов лет никак не получается, а несколько сотен миллионов лет маловато для подтверждения теории эволюции.

В этой связи сторонники теории эволюции начали ссылаться на то, что жизнь на самом деле зародилась не на Земле. А где? Там, где есть вода. Ближайшая планета – Марс[84]. Но как жизнь была перенесена на Землю? Существует гипотеза, согласно которой о поверхность Марса ударился крупный астероид, куски поверхности улетели в Космос и, в конце концов, приземлились на нашу планету. А на этих кусках каким-то образом сохранились образцы марсианской жизни. Кстати, действительно, на нашей планете находят обломки метеоритов, которые, как предполагается, имеют именно марсианское происхождение. Но могли ли они перенести органическую жизнь? Она исключительно уязвимая и неустойчивая, а ведь надо было пережить сотни и тысячи лет в открытом Космосе, под радиацией, в полном вакууме, при значительном перепаде температур!

Как мы видим, эволюционистам предстоит еще ответить не на один сложный вопрос, чтобы защитить свою теорию (на самом деле соответствующих теорий – несколько). Интересно, что в этой связи в оборот все активнее стала внедряться следующая формула: "Вероятно, жизнь зародилась не на Земле. А где именно и как именно: мы пока не знаем". В этой связи уместно отметить, что эта формула предполагает, что жизнь могла возникнуть вовсе не в результате какой-то эволюции

[84] *Ахметзянова Л.Г., Мисик И.И., Снежко А.А. и др.* Проблема поиска жизни на планетах Солнечной системы // Актуальные проблемы авиации и космонавтики. 2010. № 6. С. 361–362.

и естественного отбора. Согласитесь, такая трансформация взглядов сторонников теории эволюции достаточно показательна.

Кстати, следует учитывать, что теория эволюции возникла не просто в силу тех или иных открытий в области биологии и других естественных наук, а, скорее, в силу определенных политических причин. Две сотни лет назад нужно было доказать, что есть альтернатива божественному объяснению происхождения человека и самой жизни. А иначе церковь имела слишком значительное влияние в обществе. Более того, божественные теории предполагали, что человек мог сказать: "Я не признаю ваш суд и вашу власть! У меня только один судья – сам Бог!" Согласитесь, такая ситуация сильно ослабляла авторитет светской власти. В результате для снижения влияния церкви можно было согласиться на научные гипотезы, которые в то время еще не в полной мере были подкреплены результатами лабораторных или иных практических исследований.

Однако если допустить на миг, что теория эволюции не совсем точна, а то и вовсе неверна, то тогда возникает один большой и очень неудобный вопрос: а откуда тогда взялась жизнь на Земле? Ведь жизнь на нашей планете существует, это несомненный факт.

На самом деле тут есть свои гипотезы, которые не опираются на божественные или иные волшебные объяснения. Конечно, такие гипотезы не признаются в научном сообществе, но упомянуть их все-таки следует. Зачем? Сам факт существования таких гипотез, пусть хоть сколько угодно внешне фантастичных, доказывает, что альтернатива теории эволюции все-таки может существовать, причем вовсе не божественной природы.

Для начала, однако, попытаемся ответить на следующие два вопроса попроще: чем отличается живое от неживого и чем отличается человек от других живых организмов?[85] Ответы нам пригодятся для оценки альтернативных гипотез происхождения жизни.

---

[85] *Волков Г.Ю.* На грани живого и неживого // Вестник Курганского государственного университета. 2016. № 1 (40). С. 44–46; *Асаул В.В.* Самоорганизация в живых и неживых системах // ЭВР. 2009. № 4; *Греченко Т.Н.* Электрографический критерий отличия живого от неживого // Вестник РГГУ. Серия "Психология. Педагогика. Образование". 2019. № 4. С. 80–99; *Вахрамеева Л.Е.* Проблема соотношения живого и неживого в современной науке // Вятский медицинский вестник. 2009. № 1. С. 121; *Трофимов В.Н.* Искусственный интеллект: добро и зло как запретный плод. М.: Дашков и Ко, 2011. С. 221–228, 339–342.

Читатель тут может попытаться дать легкий ответ: "Да это же очевидно, чем отличается живое от неживого!" Однако, как представляется, очевидность тут вовсе даже не очевидна. Материал? В природе полным-полно органических соединений, которые не являются ничем живым. Наличие белка? В таком случае придется исключить из списка живых организмов вирусы, в их составе нет белка. На самом деле гарантированно отличительным признаком живого организма является так называемая "активность". Применительно к человеку говорят уже не об "активности", а о "свободе воли".

Однако оправданно ли проводить столь жесткое разграничение между человеком и другими живыми существами?[86] И тут существуют непризнанные в научном сообществе гипотезы, которые предполагают наличие только одного отличия: способности человека строить модели окружающего мира и рассчитывать их развитие на большее число шагов вперед, чем другие живые существа.

В этой связи можно сослаться на следующий пример: стая волков загоняет оленя. В конце концов, олень пойман и съеден. У волков это получилось потому, что они строили модель, в которой фигурировал виртуальный олень и виртуальные волки из стаи. Каждый волк просчитывал эту модель на несколько шагов вперед, высчитывал предположительные будущие действия оленя и действия других волков и в результате сформировал собственную выигрышную линию поведения, позволявшую в итоге поймать оленя.

Свою линию поведения просчитывает и человек. Например, он может собрать зерно и тут же его съесть. Но он так не поступает, а строит дом для себя и для хранения зерна. Через полгода, весной, опять-таки, не съедает зерно, а сеет его. И осенью собирает урожай, который больше первоначального количества зерна. Как представляется, такая модель просчитывается человеком на большее количество ходов вперед, чем у волка при поимке оленя.

Чем определяются способности просчитывать модели на определенное число шагов вперед? Наука еще четко не ответила на этот вопрос. Впрочем, тут есть разные догадки: кора головного мозга

---

[86] *Ростова Н.Н.* Человек на границе животного мира // Вестн. Том. гос. ун-та. 2019. № 446. С. 68–75; *Кременцов Н. Л.* Человек и животное: к истории поведенческих сопоставлений // Рус. орнитол. журн.. 2009. № 514. С. 1659–1681; *Андрюшина Л.В.* Человек как культурное животное в немецкой антропологии начала XX // Ученые записки ОГУ. Серия: Гуманитарные и социальные науки. 2014. № 5. С. 103–105.

человека состоит из семи слоев. Ни у каких других живых существ такого количества слоев нет, ближайший конкурент человека – дельфин, у него четыре слоя. Может быть, количество слоев и определяет способность просчитывать модели на какое-то количество шагов вперед?

Но мы видим, что человек живет совсем иначе, чем животные, он создает и пользуется благами цивилизации. Язык, письменность, право, медицина, организация общества. Ничего подобного у животных нет. Казалось бы, разница не просто значительная, она принципиальная. Однако известны случаи, когда человек в детском возрасте попадал в дикую природу. Если он не погибал, то вовсе не становился человеком в обычном понимании этого слова (в отличие от Маугли Киплинга), а был вполне похож по поведению на других зверей. Получается, что физиологической разницы для человека недостаточно, чтобы принципиально отличаться от животных.

Видимо, цивилизационная разница между человеком и животными возникает в силу того, что человек передает своим потомкам накопленный опыт не наследственным путем (да это и невозможно), а фиксируя полученные знания специфическими средствами: сначала устный пересказ, а потом и с помощью письменности. Конечно, для этого нужен язык, намного более богатый, чем у животных. Но это всего лишь количественная разница, у животных тоже есть свой язык[87]. И использование языка для передачи опыта – это, по сути, тоже построение модели на будущее, тоже расчет на много ходов вперед.

Однако если человек отличается от всех остальных живых существ в основном способностью рассчитывать свои действия на большее число ходов вперед, то это всего лишь количественная разница, причем не слишком принципиальная. Да, нельзя отрицать, что она привела к тому, что человек создал цивилизацию, пользуется деньгами, лекарствами, машинами, играет на бирже и вообще делает все то, что отличает его от животных как человека. Но по своему устройству он ничем особо не лучше и не хуже других живых

[87] *Соколова Е.Е., Федорович Е.Ю.* "Говорить – еще не значит быть человеком": критический анализ современных исследований "языка" животных в свете идей Л.С. Выготского // Национальный психологический журнал. 2016. № 3 (23). С. 8–19; *Chernigovskaya Tatiana V.* BIOLOGY, ENVIRONMENT, AND CULTURE: FROM ANIMAL COMMUNICATION TO HUMAN LANGUAGE AND COGNITION // Вестник СПбГУ. Философия и конфликтология . 2020. № 1. С. 157–170.

существ. Так это или нет, пока твердо сказать нельзя. Наверное, будущие поколения ученых найдут четкие ответы на этот вопрос. Однако в целях данного исследования, а именно: выявления угроз, связанных с использованием ИКТ, в том числе цифровых технологий, лучше исходить из самых неприятных и маловероятных вариантов. Поэтому попробуем установить эти угрозы, исходя из презумпции, что человек ничем принципиально не отличается от других известных живых существ.

А что отличает живых существ от неживых предметов? Мы уже выше обозначили, что принципиальной разницей является свойство живых организмов проявлять "активность". Если человек устроен так же, как и другие живые существа, можно в таком случае исходить из того, что у него нет какого-то особого свойства в виде "свободы воли". Точнее, мы в целях данного исследования условно ставим знак равенства между "свободой воли" и "активностью". Исследуемый нами предмет (угрозы, связанные с цифровыми технологиями и безопасность человечества), видимо, позволяет в порядке исключения сделать такое допущение.

Итак, что же такое "активность"? Какова его природа? Единственно, мы знаем, что и человек, и другие живые организмы возникают, развиваются и в конечном итоге умирают потому, что именно такой алгоритм заложен в их геноме. Может, существуют и еще какие-то факторы, определяющие это, но о них мы не можем пока достоверно говорить, они пока наукой не выявлены. А может, их и нет. Так что будем исходить из того, что известно, то есть из генома. В таком случае, может быть, активность – это просто особая программа, записанная с помощью генокода?

А что, если попробовать описать живое существо и его поведение с помощью простейших программ для ЭВМ? Обычная вычислительная машина никак себя из окружающего мира не выделяет, человек создал ее в определенных целях: помогать ему. За пределы такой поставленной задачи ЭВМ, в общем, и не выходит. Но можно сформулировать задачу для ЭВМ и иначе. Например, разработать программу, согласно которой машина будет четко отграничивать себя от других предметов. То есть машина будет "знать", где находятся ее границы. Человек-то хорошо знает, где границы принадлежащего ему компьютера. Вот он, лежит на столе, границы корпуса очень четкие. Так пусть и машина "знает", где она начинается и кончается. Вряд ли эта задача слишком сложная для квалифицированного программиста.

Итак, машина "знает", где ее границы. Следующий шаг: поставить перед машиной задачу сохранять себя в этих границах. Сохранять и защищать. Что значит "защищать"? Противодействовать всему, что может не позволить "сохранять". Наверное, задачи "сохранять" и "защищать" тоже вполне могут быть сформулированы в виде математической задачи (программы).

У нас уже почти получилось живое существо. Оно имеет определенные границы и "хочет" сохранить себя в этих границах. "Хочет?" Тут не хватает еще одного элемента, еще одной программы. Не хватает "активности". Возможно ли написать такую программу для ЭВМ?[88] Не исключено, что задача в принципе решаемая. Она где-то близка программам самообучения, генератору случайных чисел. Причем такая программа активности вряд ли будет слишком сложной, в ней важно сформулировать основополагающую принципиальную формулу или группу формул.

А как описать такой феномен, как "сознание" (или "разум")?[89] Пока согласно общепринятому подходу, сознание – это один из элементов, который принципиально отличает человека от машины в частности и от неживой природы в целом. При этом есть определение "сознания" ("состояние психической жизни"), его изучают ученые, на эту тему пишутся подробные научные работы. А можно ли его воспроизвести как функцию вычислительной машины?[90] Пока считается, что это невозможно, ведь человек – это, предположительно, нечто особое, отличающееся от машины[91].

Однако позволим себе упомянуть одну из гипотез, что представляет из себя "сознание" с точки зрения цифровых технологий.

---

[88] *Нотченко А.В., Градов О.В., Бережная Л.А.* Бифуркационные эффекты, электрофизиологическая активность нейронов и волны аксонального тока в морфогенезе модели на базе уравнения Шредингера: эвм-моделирование и эксперимент // Физика живого. 2012. № 2. С. 9–29; *Брындин Е.Г.* Квантодетерминированная информационная технология // Известия ТПУ. 2003. № 3. С. 28–32; *Охлопков Н.М.* Вычислительный метод познания диалектический синтез экспериментального и теоретического методов познания // Вестник СВФУ. 2010. № 1. С. 138–142.

[89] *Чернухин Ю.В.* Компьютеры и Нейрокомпьютеры // Известия ЮФУ. Технические науки. 1997. № 2. С. 84–87.

[90] Есть, например, гипотеза о квантовой природе сознания. *Иванов Е.М.* Сознание в квантовом мире. О происхождении сознания. Издательский центр "Наука", Саратов, 2008.

[91] *Акулов О.А., Медведев Н.В.* Информатика: базовый курс: учебник для вузов. 4-е изд. М.: Омега-Л, 2007. С. 9.

Как известно, машина не просто передает информацию, она постоянно перепроверяет, что именно передала, а иначе при передаче могут возникнуть потери. Так, может, и человек делает то же самое? Можно ли допустить, что функция перепроверки деятельности человеческого мозга существует в основном в виде зрительных образов? Может, на самом деле это и есть наше "сознание"?

Итак, мы имеем машину, которая пытается защитить и сохранить себя, при этом проявляет какую-то активность. Можно ли считать такую машину именно "живым существом"? Как хотите! Но подобная машина точно может создать человечеству проблемы. Ведь это почти готовый составной элемент "серой слизи". Добавить функцию самовоспроизведения, довести машину до предельно миниатюрных размеров, вот и все. Машина будет "вести" себя активно, размножаться, занимать жизненное пространство, при этом еще и защищаться. Проблемы для человека возникнут совершенно точно.

А если такую машину снабдить программой самообучения? Такие программы в том или ином виде уже широко распространены. Если машина будет совершенствоваться, то тогда это уже не "серая слизь", это уже что-то значительно более проблемное для человека[92]. Машина по определению считает быстрее, чем человек, она не отягощена ничем вроде "совести", чувства справедливости, сострадания, жалости (не исключено, однако, что эти чувства вполне возможны в виде соответствующих программ, заложенных изначально или приобретенных в процессе самообучения). Но таких программ может и не быть. К тому же машина редко ошибается, мгновенно реагирует на ситуацию, легко рассчитывает оптимальные варианты "поведения". Да, несомненно, это будет серьезный конкурент для человека. Конкурент, который может либо подчинить себе человека, превратив его в раба или слугу, либо вообще уничтожить как претендента на общее жизненное пространство.

Если ли что-то недостижимо фантастическое в описанных свойствах машины? Она себя осознает в определенных границах, сохраняет себя, защищает, проявляет активность и может воспроизводить. Как представляется, тут нет ничего невозможного, все в пределах разумных возможностей программистов и создателей компьютерного "железа". Видимо, определяя круг угроз, не следует

[92] *Волгин Л.И., Мишин В.А.* Онтологические аспекты искусственного интеллекта // Вестник УлГТУ. 1999. № 4 (8). С. 13–19.

пренебрегать в том числе и вышеописанными достаточно гипотетическими ситуациями.

Ведь теоретически никак нельзя исключить, что когда-нибудь какой-то микробиолог, озлобленный на все человечество, выведет в домашней лаборатории смертоносный вирус и выпустит его, чтобы уничтожить других людей. И этот вирус – тоже машина, только на основе органических носителей. Точно так же злонамеренно настроенный разработчик и изготовитель вычислительных машин может создать монстра, микроскопического размера или побольше, снабдить его вышеописанными программами и тоже выпустить на волю.

Еще один хороший вопрос, который, хотя и косвенно, но тем не менее касается безопасности при использовании цифровых технологий: откуда взялись все живые существа на нашей планете? Как уже упоминалось выше, согласно общепризнанной точке зрения живые существа возникли случайно, в результате удачного совпадения ряда благоприятных факторов и со временем превратились во все многообразие видов живых существ. Собственно говоря, речь идет о теории эволюции, предложенной еще Ч. Дарвиным. К ней, как мы уже указывали, есть сложные вопросы, на которые пока нет бесспорно убедительных ответов.

Конечно, существует мнение, что человека и весь окружающий нас мир создал какой-то бог, Иисус Христос, Аллах. Поскольку такая версия опирается не на знания, а на веру, не будем ее рассматривать. А другие варианты (кроме волшебно-божественных)? Тут можно строить только гипотезы, подчас выглядящие совсем фантастически. Вот одна из них: например, на Земле достаточно материалов, которые имеют структуру, схожую с нейронной сетью, или которые могут послужить основой для возникновения чего-то похожего на нейронную сеть. Это в том числе разнообразные кристаллические вещества, вода[93], лед. Бесспорно, что происходящие рядом события могут отражаться и фиксироваться в таких материалах. Хорошо, например, известен эффект снежинок, которые приобретают разную

[93] *Масару Эмото.* Послание воды. М., Попурри, 2006; *Зенин С.В.* Биологические и информационные свойства воды // Традиционная медицина. 2000: Сб. материалов конгр. (Г. Элиста) М., 2000. С. 503–510; *Зенин С.В.* Структурированное состояние воды как основа управления поведением и безопасностью живых систем: дис. … д-ра биол. наук. М., 1999.

форму в зависимости от характера музыки. Кто-то даже утверждает, что носителем информации может быть время[94].

Накопление информации – это первый шаг. Следующий – обработка информации. Тут нужен какой-то алгоритм, например, нечто вроде программы, используемой человеком в современных ЭВМ. Могла ли такая программа возникнуть случайно? В любом случае вероятность такого события повыше, чем Боинг, который сам собой собрался сильным ветром из помойных отбросов (выше уже упоминалось это сравнение, наглядно показывающее, чему равна вероятность случайного возникновения жизни).

Преимущество цифровой информации в том, что она может передаваться на большие расстояния без потерь (и мгновенно). Такая передача более реальна, чем обломок с поверхности Марса, который прилетел на Землю в результате падения астероида на марсианскую поверхность, при этом перенес на нашу планету живых существ, которые не погибли даже в Космосе. Так что соответствующий алгоритм в виде определенной программы мог возникнуть где угодно, случайно или нет, а потом быть перенесен на Землю.

Если так, то жизнь могла возникнуть на Земле первоначально в виде, например, вычислительной машины, существующей на природном "железе" (минералы, вода, лед?) и оперирующей программами активности и самозащиты. А уж эта гипотетическая ЭВМ стала строить на Земле жизнь, используя органические носители и шифруя информацию, используя генокод. Зачем? Какой-то эксперимент, способ накопления определенного опыта, просто игра. Кто знает?! На самом деле гипотезы об эволюции интеллекта вовсе не новы[95].

Однако если дело обстоит именно так (понятно, что это только чисто теоретическое предположение), человек должен обращаться с ИКТ, в том числе цифровыми технологиями, особо осторожно. Он, создавая все более совершенные машины и используя все более совершенные технологии, рискует вторгнуться в чужую область деятельности, что может повлечь определенную реакцию, может быть, даже неблагоприятную. Или рискует создать машину, более совершенную, чем он сам.

---

[94] *Козырев Н.А.* Избранные труды. Л.: Изд-во Ленинградского университета, 1991.

[95] *Редько В.Г.* Эволюционная кибернетика. На пути к теории происхождения мышления. М.: УРСС, 2005.

Еще одно фантастическое предположение: теоретически не исключено, что все изначально было задумано так, чтобы человек сам своими руками создал себе альтернативу, более совершенную, чем он. Чем вам не эволюция, только цифровая? Конечно, все эти рассуждения – не более чем догадки. Тем не менее в рамках данного исследования они могут быть полезны для того, чтобы предвидеть все мыслимые и немыслимые угрозы, связанные с использованием ИКТ, в том числе цифровых технологий, и находить соответствующие средства по противодействию им, если это еще возможно.

Гипотеза о первичности "цифрового разума" предполагает, что и все живые существа, населяющие Землю, в своей основе тоже всего лишь машины, хотя и построенные на органических носителях. Но такой вывод противоречит всему нашему субъективному, чувственному опыту. Человек явно ощущает, что у него есть свобода выбора, какой поступок совершать, а какой – нет. У человека, по его мнению, явно есть свобода воли. Похоже, что точно так же остальные живые организмы, по крайней мере, высшие, исходят из того, что имеют выбор, какие действия совершать, а какие – нет.

Мало того, предположение о том, что свободы воли нет, входит в решительное противоречие с основами устройства человеческого общества. Свобода договора, система поощрений и наказаний – все это неотъемлемые элементы человеческой цивилизации. Получается, что вся наша цивилизация построена неправильно, базируется на заведомо ложном субъективном ощущении? Казалось бы, невозможно сделать такое научное открытие, которое в принципе отвергалось человеком, которое он не мог бы "переварить". Но предположение, что все живое на Земле – лишь биологические машины без свободы выбора – именно такое.

Не будем дальше покушаться на фундаментальные основы устройства нашего общества, однако, затронув феномен свободы воли, все-таки выскажем следующее крамольное предположение. Допустим, в человеческую голову каким-то особым способом была введена программа активности. Такая программа должна побуждать человека не вести себя пассивно, а активно искать варианты, как обеспечить свою безопасность и дальнейшее комфортное существование. И как человек должен субъективно ощущать наличие такой программы? Как нечто постороннее, непонятно почему толкающее его на те или иные проступки? Вряд ли. Если не будет обеспечено, что такая программа ощущается как нечто неразрывно

целое с человеком, органично присущее ему, он будет ей сопротивляться, ставить под сомнение. Нет, конечно же, такая программа активности должна ощущаться человеком как его собственное, имманентно присущее ему качество. Какое именно? Может быть, именно ощущение свободы выбора, свободы воли и есть субъективное восприятие действия программы активности? Человеку кажется, что он имеет возможность сделать выбор. И он делает этот выбор, выходя из пассивного состояния и проявляя активность. Может быть, именно так он на самом деле и выполняет требование программы активности?

Понятно, что все эти довольно фантастичные предположения ставят под сомнение сам смысл существования человека и человеческого общества. Зачем что-то предпринимать, если все заранее предопределено? Зачем наказывать преступников? Ведь они не вольны в своем преступном поведении. Зачем работать, все равно это по большому счету бесполезно и бессмысленно? Что написано на роду, то и случится.

Но научные открытия бывают разные, приятные и неприятные, подходящие и неподходящие. Нельзя исключать, что некоторые из них могут входить в противоречие даже с самыми устоявшимися и общепризнанными основами. Нельзя же заранее ставить условие, что некоторые научные открытия заранее будут неприемлемы. Мало того, пока наука так и не доказала, что свобода воли на самом деле существует объективно. В этом вопросе человек опирается исключительно на свои субъективные ощущения. Нам именно кажется, что мы свободы в выборе своих поступков. При этом субъективное ощущение может совпадать с объективной реальностью, а может и не совпадать.

Кстати, тут вполне уместно упомянуть, какую позицию по вопросу о происхождении всего живого на Земле занимали или занимают те или иные известные ученые. Например, Владимир Вернадский считал, что жизнь вовсе не зародилась на Земле, а была занесена на нашу планету извне (теория панспермии). Таких же взглядов придерживались немецкий ученый Герман Гельмгольц, английский физик Кельвин, шведский физик и химик Сванте Аррениус. Академик РАН А.Ю. Розанов, известнейший специалист в области палеонтологии, придерживается примерно такой же точки зрения. Об управляемой панспермии говорит известный американский астрофизик Томас Голд, автор теории стационарного состояния.

А Френсис Крик является сторонником теории так называемой "управляемой панспермии" (жизнь занесена на Землю инопланетными цивилизациями). Вот что он, мировой авторитет по молекулярной биологии, получивший Нобелевскую премию за открытие структуры ДНК, утверждает: "Зарождение жизни представляется почти чудом, столь велико количество условий, соблюдение которых необходимо для того, чтобы это произошло"[96].

Наталья Бехтерева, известнейший советский и российский нейрофизиолог, научный руководитель Института мозга человека РАН, хотя формально и не отрицала теорию эволюции, но говорила, что ей ближе иные взгляды на происхождение жизни на Земле, считала, что существует жизнь после смерти, полагала, что "в начале всего лежит мысль".

Уместно также отметить, что среди сторонников теории эволюции в принципе нет согласия, как именно зародилась на Земле жизнь. Некоторые придерживаются версии "первичного бульона", другие говорят про "химическую эволюцию". Еще есть версия, что жизнь зародилась около "черных курильщиков" (глубоко под водой, у геотермальных источников). Александр Опарин отстаивал вариант "протоклеток". Следует также упомянуть теорию "эндосимбиоза". Понятно, что до сих пор никто из сторонников всех этих вариаций в рамках теории эволюции не смог в лаборатории создать жизнь, опираясь на свои научные предположения.

[96] *Horgan J.* Scientific Americanю Т. 264. February 1991. P. 101.

Глава 3. Перспективы заключения конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, а также иных соглашений

1. Будапештская конвенция 2001 года, другие значимые международные документы

Будапештская конвенция

В 2001 году в рамках Совета Европы в Будапеште была выработана и в 2004 году вступила в силу Конвенция о преступности в сфере компьютерной информации (о киберпреступности). Россия не участвует в указанной конвенции, ссылаясь на то, что в соответствии с ее статьей 32 в целях противодействия киберпреступности государства-участники получают возможность "трансграничного доступа к компьютерным данным", что, по мнению РФ, противоречит принципу государственного суверенитета. К тому же российские специалисты отмечают, что в Конвенции не содержатся, например, такие понятия, как спам, бот-атаки, фишинг.

Участники Будапештской конвенции преследуют пять основных целей:

1) гармонизация материального уголовного законодательства по борьбе с киберпреступностью;

2) гармонизация уголовно-процессуального законодательства;

3) содействие взаимной правовой помощи;

4) кодификация международного права, с акцентом на юрисдикционные нормы на основе территориальности;

5) обеспечение правовой базы для содействия развитию и пониманию вопросов, связанных с киберпреступностью.

В Конвенции предусмотрены меры по противодействию следующим преступлениям:

преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы, противозаконное использование устройств); правонарушения, связанные с использованием компьютерных средств (подлог с использованием компьютерных

технологий, мошенничество с использованием компьютерных технологий); правонарушения, связанные с детской порнографией; правонарушения, связанные с нарушением авторского права и смежных прав[97].

В целом цель Будапештской конвенции – дополнить соответствующие многосторонние или двусторонние соглашения или договоренности между разными государствами, включая положения Европейской конвенции о выдаче, Европейской конвенции о взаимной правовой помощи по уголовным делам, Дополнительного протокола к Европейской конвенции о взаимной правовой помощи по уголовным делам, открытого для подписания в Страсбурге 17 марта 1978 г. (СЕД № 99).

К Будапештской конвенции был принят и в 2006 году вступил в силу Дополнительный протокол, касающийся криминализации актов расистского и ксенофобского характера, совершенных при помощи информационных систем (Договор Совета Европы (European Treaty Series) № 189) . Он подписан 36 из 47 государств – членов Совета Европы, а также еще двумя государствами: Канадой и ЮАР.

В статье 6 Протокола "Отрицание, грубое преуменьшение значения или оправдание геноцида или преступлений против человечности" предусмотрены следующие положения:

"1. Каждая Сторона принимает такие законодательные меры, какие могут потребоваться для того, чтобы криминализировать в соответствии с ее внутренним законодательством следующие деяния, совершенные умышленно и противоправно:

распространение или предоставление общественности каким-либо иным образом при помощи информационных систем материалов, которые отрицают или грубо преуменьшают, одобряют или оправдывают деяния, являющиеся геноцидом или преступлениями против человечности согласно определению, принятому в международном праве, и признанные таковыми вступившими в законную силу и обязательными к исполнению решениями Международного военного трибунала, созданного в соответствии с Лондонским соглашением от 8 августа 1945 г., или любого другого

---

[97] *Данельян А.А.* Международно-правовое регулирование киберпространства. Образование и право. № 1. 2020. С. 265; *Долженко Н.И., Хмелевская И.Г.* К вопросу о содержательных аспектах киберпреступности // Научные ведомости БелГУ. Серия: Философия. Социология. Право. 2020. № 2. С. 318–319.

международного суда, созданного согласно соответствующим международно-правовым актам, юрисдикция которого признана этой Стороной.

2. Сторона может:

a) потребовать, чтобы отрицание или грубое преуменьшение значения деяний, о которых говорится в пункте 1 настоящей статьи, совершались с умыслом на подстрекательство к ненависти, дискриминации или насилию в отношении любого лица или группы лиц по признаку расы, цвета кожи, родства по восходящей линии, национального или этнического происхождения, а также религии, если она используется в качестве предлога для любого из этих признаков, или

b) оставить за собой право не применять пункт 1 настоящей статьи полностью или частично".

Общие перспективы заключения международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях

28 декабря 2019 года была принята Резолюция ГА ООН A/RES/74/247 "Противодействие использованию информационно-коммуникационных технологий в преступных целях", согласно которой учреждается специальный межправительственный комитет экспертов открытого состава, представляющий все регионы, для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Собственно говоря, возникла ситуация, когда международное сообщество разделилось на две большие группы: первая поддерживает Будапештскую конвенцию как основной международный многосторонний инструмент для борьбы с киберпреступностью и считает избыточной разработку нового документа, как это предусмотрено указанной выше Резолюцией ГА ООН, принятой в декабре 2019 года. Вторая группа государств считает, что необходимо новое международное соглашение, и выступила в поддержку Резолюции ГА ООН.

За принятие указанной Резолюции ГА ООН проголосовали 79 государств. "Против" голосовали 60 стран, в их числе — США, Франция, Германия, Великобритания, Канада, Украина. 33 страны

воздержались от голосования. Авторами документа стали 47 стран, среди которых — Россия, Китай, Индия, Белоруссия, Казахстан, Сирия, Египет, КНДР.

В США высказывается мнение, что декабрьская Резолюция ГА ООН позволит таким странам, как Россия и Китай, создать одобренный ООН инструмент как блокировки критических по отношению к властям сайтов, так и слежки за диссидентами, а не договор по борьбе с киберпреступностью. Российские специалисты не согласны с этим мнением и говорят о желании осовременить Будапештскую конвенцию, в которой, например, упомянуты лишь девять видов киберпреступлений[98], а их в настоящее время насчитывается уже несколько десятков. К тому же Будапештская конвенция никак прямо не регулирует проблемы кибертерроризма.

Итак, возникает перспектива, что в будущем международном соглашении, разработанном на основе указанной Резолюции ГА ООН, не будут участвовать США и другие страны НАТО. Возможно, этого не произойдет, и группе экспертов удастся выработать конвенцию, приемлемую для широкого круга стран и не вступающую в конфликт с Будапештской конвенцией 2001 года. Но следует учитывать и иной вариант: существование двух международных договоров, не объединяющих страны международного сообщества, а фиксирующих во многом два разных подхода к обеспечению безопасности в связи с использованием ИКТ. В таком случае, надо полагать, два международных договора станут основой для дальнейших переговоров по выработке единой позиции мирового сообщества к указанной проблеме. Нужно отметить, что по вопросам безопасности информационных технологий уже заключены многосторонние договоренности в рамках ШОС, ОДКБ, СНГ, а также на двустороннем уровне с участием России.

Другие значимые договоренности

Помимо Будапештской конвенции существуют также другие международные договоры, затрагивающие вопросы обеспечения безопасности в связи с использованием киберпространства. Однако они либо региональные, либо двусторонние. Существуют также договоренности, не являющиеся международными договорами,

[98] *Федорович В.Ю.* Что такое "Киберпреступление"? // Вестник Московского университета МВД России. 2020. № 3. С. 17.

существующие в качестве итоговых документов тех или иных международных форумов и носящие рекомендательный характер. Но они содержат соответствующие формулировки, которые могут оказаться полезными при разработке будущих международных договоров, в том числе универсального характера.

В 1998 году заключено Соглашение о свободном доступе и порядке обмена открытой научно-технической информацией государств – участников СНГ. Соглашение включает в себя положения об информационных ресурсах общего пользования.

В 1999 г. в ходе Тамперского совещания Европейского совета ЕС было принято решение о целесообразности включения преступлений в области высоких технологий (high-tech crime) в число преступлений, по которым необходима выработка общего европейского подхода в части криминализации и санкций. В 2001 г. Европейская комиссия представила специальное сообщение "Создание безопасного информационного общества посредством повышения защищенности информационной инфраструктуры и борьбы с преступлениями с использованием компьютерных средств", в котором содержались предложения правового и организационного характера по борьбе с киберпреступностью в Европейском союзе. (Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computerrelated Crime". Brussels, 26.1.2001.)

В 2000 году восемь ведущих государств мира, в том числе Россия, приняли Окинавскую хартию глобального информационного общества, согласно которой в целях развития глобального информационного общества предлагается предпринять "согласованные действия по созданию безопасного и свободного от преступности киберпространства". В документе декларируется принцип – "все люди повсеместно, без исключения должны иметь возможность пользоваться преимуществами глобального информационного общества". Устойчивость глобального информационного общества основывается на стимулирующих развитие человека демократических ценностях, таких как свободный обмен информацией и знаниями, взаимная терпимость и уважение к особенностям других людей. Вхождение человечества в XXI в. омрачено ростом террористической опасности в самых различных ее

проявлениях. Методы террористов становятся все более разнообразными и изощренными. Увеличение числа и роста экстремистских группировок сопровождается их возрастающей технической оснащенностью. Чтобы активно и плодотворно противостоять международному кибертерроризму, следует базироваться на следующих важнейших основополагающих признаках:

− следовать нормам и принципам международного права;

− всеобщее осуждение и признание противоправности терроризма во всех его проявлениях (кибертерроризм);

− международное сотрудничество и обмен информацией между государствами;

− неотвратимость ответственности кибертеррористов, совершивших преступление;

− действенность антикибертеррористических мер.

В 2001 году принято Соглашение о сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации. Документ направлен на определение единообразных составов компьютерных преступлений, которые государства должны включить в свое национальное законодательство, а также разработку мер борьбы с ними.

В 2001 году заключена Конвенция Совета Европы "Об информационном и правовом сотрудничестве".

В 2003 году на Всемирной встрече на высшем уровне в Женеве принята Декларация принципов построения информационного общества (Declaration of Principles WSIS-03/Geneva).

В 2009 году на саммите ШОС в Екатеринбурге было подписано и в 2011 году вступило в силу Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности. Соглашение определило основные принципы и направления сотрудничества в этой сфере, а также впервые в международно-правовом плане обозначило существование конкретных угроз в области информационной безопасности. Соглашение открыто для присоединения других государств, что подтверждает саму идею создания всеобъемлющей системы обеспечения международной информационной безопасности.

В 2011 году Россия представила в ООН проект Конвенции об обеспечении международной информационной безопасности. В ст. 4 проекта Конвенции закреплены основные угрозы международному

миру и безопасности в информационном пространстве, из которых выделено 11 базовых и 4 дополнительных. Среди базовых названы, например, использование информационных технологий и средств для осуществления враждебных действий и актов агрессии; целенаправленное деструктивное воздействие в информационном пространстве на критически важные структуры другого государства; трансграничное распространение информации, противоречащей принципам и нормам международного права, а также национальным законодательствам государств. Проект Конвенции содержит ст. 5, посвященную основным принципам обеспечения международной информационной безопасности, которые условно можно разделить на четыре группы: принципы участия государства в системе международной информационной безопасности как члена международного сообщества; принципы, позволяющие государству сохранить свой суверенитет в процессе международного сотрудничества в борьбе с киберпреступностью; принципы обеспечения свободного информационного обмена между странами. Четвертая группа принципов устанавливает характер взаимодействия государства и частных субъектов в рассматриваемых отношениях. В гл. 5 "Международное сотрудничество в сфере международной информационной безопасности" предусмотрены меры международного сотрудничества, в том числе "обмен национальными концепциями обеспечения безопасности в информационном пространстве, оперативный обмен информацией о кризисных событиях и угрозах в информационном пространстве и принимаемых мерах в отношении их урегулирования и нейтрализации", "консультации по вопросам деятельности в информационном пространстве, которая может вызывать озабоченность государств-участников, и сотрудничество в отношении урегулирования конфликтных ситуаций военного характера".

В 2011 году Россия инициировала в рамках ООН рассмотрение документов, связанных с международно-правовым регулированием вопросов информационной безопасности: на имя Генсека ООН было направлено письмо Постоянных представителей при ООН: Китая, Российской Федерации, Таджикистана и Узбекистана. Четыре государства – члена ООН предложили к рассмотрению Правила поведения в области обеспечения международной информационной безопасности (далее – *Кодекс информационной безопасности*). Необходимость принятия Кодекса информационной безопасности эти

государства связывали с тем, что вопросы интернет-безопасности имеют большое значение, и их следует рассматривать в рамках международного сотрудничества и в духе взаимного уважения. Кодекс призван защищать Интернет и другие информационно-коммуникационные сетевые технологии от угроз и "уязвимости" (A66/356).

В 2013 году Постоянный совет ОБСЕ одобрил документ "Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью снижения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий".

В 2013 году Центр передового опыта НАТО в области компьютерной безопасности выпустил сборник рекомендаций "Таллинское руководство по применению международного права в кибервойне". Основными задачами предполагаются адаптация существующих правовых норм в отношении вооруженных конфликтов под специфику враждебной деятельности в виртуальном пространстве и попытка разработать дефиниции основных понятий в сфере компьютерной безопасности.

В 2013 году между Россией и США заключены "Договоренности о мерах укрепления доверия в сфере использования ИКТ".

В 2015 г. на основании Договора о добрососедстве, дружбе и сотрудничестве между Российской Федерацией и Китайской Народной Республикой 2001 г. было заключено Соглашение между Правительством РФ и Правительством КНР о сотрудничестве в области обеспечения международной информационной безопасности. В Соглашении подчеркивается значение совместной работы в рамках ШОС и важность дальнейшего развития взаимодействия в области использования информационно-телекоммуникационных технологий.

В 2016 году НАТО и ЕС подписали Техническое соглашение по киберзащите. (Technical Arrangement on Cyber Defence between NATO (NCIRC) and the EU (CERT-EU).)

В 2017 году Россия представила в ООН Концепцию конвенции ООН (или Концепцию безопасного функционирования и развития сети Интернет). В документе предлагается система управления сетью Интернет. Цель документа: "Установление режима равноправного международного сотрудничества в управлении сетью Интернет". Там же сказано: "Государства имеют равные права и обязанности в отношении связанных с управлением сетью Интернет вопросов государственной политики международного уровня. Доступ к сети

Интернет не может использоваться государствами в качестве инструмента влияния на другие государства".

В 2017 году Россия представила в ООН проект Конвенции о сотрудничестве в сфере противодействия информационной преступности (A/C.3/72/12). В документе предлагаются определения следующих терминов: "арест имущества", "бот-сеть", "вредоносная программа", "имущество", "конфискация", "объекты критической инфраструктуры", "организованная преступная группа" и др. В проекте даны определения, какие именно деяния должны считаться преступлением, а именно: неправомерный перехват, нарушение функционирования ИКТ, создание, использование и распространение вредоносных программ, распространение спама, незаконный оборот устройств, хищение с использованием ИКТ, преступления, связанные с детской порнографией, нарушение авторских и смежных прав с использованием ИКТ и др. При этом, согласно проекту, участники конвенции должны предусмотреть, что указанные деяния должны квалифицироваться во внутреннем законодательстве как преступления.

Итак, на современном этапе ключевая проблема заключается в отсутствии на международном уровне функционирующих механизмов предупреждения и сдерживания конфликтов в киберпространстве. Действующая система международного права не адаптирована к реальности использования ИКТ в политических и военных целях. При этом существующие нормы международного права, регулирующие конфликты и военные столкновения, не могут применяться к сфере ИКТ в формате "как есть" в силу ее технологических особенностей. Речь идет о нормах международного гуманитарного права (jus in bello) и права вооруженного конфликта (jus ad bellum), которые кодифицированы в таких актах, как Гаагская конвенция 1899 г., Гаагская конвенция 1907 г., Женевская конвенция 1928 г., Женевские конвенции I–IV 1949 г., и Дополнительные протоколы I–III 1977, 1997 и 2005 гг. к Женевским конвенциям I–IV[99].

[99] См., например: *Нежельский А.А.* Информационная безопасность государств и граждан в нем: ключевые компоненты и группы интересов. Азимут научных исследований: экономика и управление. 2017. Т. 6. № 3(20). С. 406.

2. Позиция России, КНР и США по ключевым проблемам обеспечения МИБ

Конечно, и позиция России, и США по вопросам обеспечения безопасного использования ИКТ могут со временем измениться и даже наверняка будут меняться. Трудно сказать, будет ли при этом происходить именно сближение позиций. Не исключено, что в конечном итоге общепризнанной станет та позиция, которая сформируется по итогам силового противоборства как в киберпространстве, так и в целом на международной арене, с учетом всех экономических, политических и военных факторов[100]. Однако пока можно констатировать, что у России и США более или менее четко обозначились собственные ключевые подходы, которые подчас расходятся между собой.

Россия

Что касается России, то тут можно констатировать следующие публично декларируемые подходы:

- информационно-коммуникационные технологии должны использоваться исключительно в мирных целях. Международное сотрудничество должно быть нацелено на предотвращение конфликтов в сфере использования ИКТ, а не на их регулирование;
- могут вырабатываться дополнительные правовые нормы для регулирования международных отношений в сфере использования ИКТ, однако в определенной мере продолжают оставаться применимыми и уже существующие нормы международного права, имеющие важное значение для поддержания международного мира, безопасности и стабильности и создания открытого, безопасного, стабильного, доступного и мирного информационного пространства;
- государства должны обладать суверенитетом над информационно-телекоммуникационной инфраструктурой на своей территории;

[100] *Коровкин В.В.* Международное регулирование киберпространства: возможно ли эффективное взаимопонимание? // Социальные новации и социальные науки. 2020. № 1 (1). С. 60–76.

- любые обвинения в адрес государств о причастности к компьютерным атакам должны быть обоснованными и доказанными;

- государства не должны допускать возможности использования своей территории для осуществления компьютерных атак и не должны содействовать использованию в этих целях посредников;

- государства должны бороться с внедрением и использованием скрытых вредоносных функций и программных уязвимостей в IT-продукции, а также добиваться ее безопасности для пользователей[101].

Позиция России в отношении обеспечения международной информационной безопасности состоит в необходимости признания триады угроз. Это угрозы военно-политические, криминальные (преступные) и террористические. Сразу нужно отметить, что США не согласны включать в какие-либо международные документы положений, касающихся регулирования военно-политических угроз, среди которых одна из ключевых – это вмешательство во внутренние дела других стран с использованием ИКТ.

В России сформировались следующие основные направления государственной политики по проблемам обеспечения информационной безопасности страны:

- совершенствование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы страны;

- повышение защищенности информационных систем и сетей связи государственных органов;

- снижение рисков, связанных с объективной необходимостью использовать иностранные программы и оборудование;

- повышение безопасности и устойчивость работы инфраструктуры российского сегмента Интернета, особенно с учетом террористических угроз;

- участие страны в создании системы международной информационной безопасности.

[101] *Смирнов А.И.* Современные информационные технологии в международных отношениях. М.: МГИМО-Университет, 2017. С. 295–296.

США

США в целом придерживаются стратегии, ориентированной на три приоритета:

- повышение уровня кибербезопасности и защиты от киберугроз в государственном и частном секторах;
- сдерживание и прекращение злонамеренной киберактивности, направленной на Соединенные Штаты или их союзников;
- эффективное реагирование на инциденты в области кибербезопасности и восстановление систем после кибератак.

При этом США декларируют, что на международной арене:

– отстаивают применение международного права в киберпространстве;

– добиваются принятия добровольных норм поведения государств в мирное время;

– осуществляют разработку мер укрепления доверия и пытаются заставить другие государства принять на себя обязательства по противодействию краже интеллектуальной собственности и коммерческой тайны;

– стараются модернизировать процесс взаимной правовой помощи для более широкого трансграничного обмена данными между правоохранительными органами;

– разрабатывают дополнительные инструменты, чтобы сдерживать и пресекать злонамеренную киберактивность, направленную против США.

США в своей военной стратегии выступают за повышение эффективности своих вооруженных сил в киберсреде, официально признают, что совершают кибератаки, допускают наступательные кибероперации якобы для создания структур сдерживания, которые продемонстрируют противникам, что стоимость их участия в операциях против США выше, чем они рассчитывают.

США (и НАТО в целом) рассматривают киберпространство как новую сферу военной деятельности.

На экспертном уровне американские специалисты соглашаются, что необходима ответственность государств за использование их территории для совершения международно-противоправных действий с применением ИКТ. США против договоренностей об установлении границ зон ответственности государств в ИКТ-среде и против

интернационализации управления сетью Интернет, придерживаются позиции о саморегурировании при использовании Интернета[102].

Расхождения в позициях России и США

Если подвести некоторый промежуточный итог, то можно, видимо, утверждать, что позиции США и России не так уж сильно и расходятся. У каждой страны в силу определенных причин сложилось свое понимание содержания информационной безопасности, использование своей собственной терминологии, постановка своих собственных конкретных задач. Но, по сути, тут нет совсем взаимоисключающих положений, а имеющиеся расхождения в трактовках либо незначительные, либо чисто теоретические и практически непринципиальные.

Более или менее значимые расхождения следующие. США не считают нужной разработку новой всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, полагая, что достаточно уже имеющейся Будапештской конвенции 2001 года. США более открыто говорят о противоборстве в информационной среде, о применении тут силы. Россия формально провозглашает необходимость мирного использования ИКТ, но ясно, что это, скорее, декларативная, чем реальная задача.

Между США и Россией довольно много мелких терминологических расхождений, в частности, применительно к словосочетаниям с использованием "кибер-" и "информационный". Однако эти расхождения не слишком принципиальные, обе страны подчас прибегают к использованию и той, и другой терминологии.

Россия и США расходятся в определении того, что нужно понимать под информационной безопасностью, а именно: как содержание информации влияет на политические, социальные, общественные процессы, и входит ли оно в сферу проблематики ИКТ-

[102] *Медовкина Л.Ю.* Политика администрации Б. Обамы в области информационной безопасности // Вестник Омского университета. Серия "Исторические науки". 2019. № 2. С. 149–157; *Зайцев А.А.* Ключевые направления военной политики Вашингтона в современных условиях // Труды БГТУ. Серия 6: История, философия. 2016. № 5 (187). С. 76–80; *Манойло А.В.* Современные стратегии кибербезопасности и кибероборонь НАТО // АПЕ. 2020. № 3. С. 160–184.

безопасности (то есть, потенциально, в сферу международного регулирования). Иными словами, речь идет о триаде угроз, о которых говорит Россия. США, по сути, признают существование военно-политического аспекта угрозы, однако ссылаются на то, что с ней вряд ли можно эффективно бороться с использованием международно-правовых норм, поскольку возникнут сложности с определениями терминов и понятий, с расхождениями, что именно следует считать угрозой.

Россия полагает, что обладает суверенными правами для регулирования информационно-телекоммуникационной инфраструктуры на своей территории. США не согласны с этим, ссылаются на саморегулирование. Американский подход, основанный на понятиях киберпространства и кибербезопасности, в целом отрицает регулирование информации в контексте ИКТ-безопасности, но на практике тоже не ограничивается только лишь техническими аспектами. Если говорить более подробно, то речь идет о полномочиях правительственных структур в регулировании контента. В США придерживаются модели управления Интернетом при участии всех заинтересованных сторон (multistakeholder internet governance), что предполагает равноправное участие в управлении всех групп/сторон или их выбранных представителей, а также общее понимание заинтересованности всех участников в развитии Глобальной Сети.

КНР

Что касается Китая, то его позиция по международным аспектам обеспечения безопасного использования ИКТ пока практически полностью совпадает с российской. Две страны согласованно выступают на международной арене за обеспечение безопасного использования ИКТ. Однако на внутригосударственном уровне позиция Китая имеет свою специфику, и не исключено, что в конечном итоге это может повлиять и на его международные подходы.

В 2017 г. в Китае была утверждена Стратегия международного сотрудничества в киберпространстве. В этом документе определяются основные принципы участия Китая в международном обмене и сотрудничестве в киберпространстве. В частности, в указанной Стратегии упоминаются принципы Устава ООН, положения

Соглашения ШОС о сотрудничестве в области обеспечения международной информационной безопасности, Соглашения между Правительством РФ и Правительством КНР о сотрудничестве в области обеспечения международной информационной безопасности, проекта Правил поведения в области обеспечения международной информационной безопасности, Уфимской Декларации VII Саммита БРИКС (9 июля 2015 г.) и др. Стратегия предполагает суверенное равенство (интернет-суверенитет), невмешательство во внутренние дела других государств, отказ от гегемонии в Интернете. Стратегия исходит также из того, что для развития, оптимизации и повышения информационной безопасности Сети поощряется развитие сетевой инфраструктуры, технических инноваций.

Следует отметить, что в доктрине и в нормативных правовых актах КНР в качестве основных проблем и угроз киберпространства названы несбалансированность развития, несправедливый порядок, расширение "цифровой пропасти" между странами и регионами, уязвимость критической информационной инфраструктуры. Особое внимание обращается на угрозу кибертерроризма, рост информационной преступности, а также вмешательство государств во внутренние дела других стран путем злоупотребления ИКТ, массового кибершпионажа.

В качестве стратегических целей КНР при участии в международном сотрудничестве в киберпространстве определены:

- защита интернет-суверенитета, национальной безопасности и интересов Китая;
- формирование системы международных правил в киберпространстве;
- содействие справедливости в управлении Интернетом;
- защита законных прав и интересов граждан;
- содействие глобальному сотрудничеству в цифровой экономике;
- создание платформ для обмена киберкультурой[103].

В китайском законе "О кибербезопасности" закреплены такие ключевые понятия, как сеть, сетевая безопасность, сетевые данные, личная информация, операторы сети, критически важная информационная инфраструктура. Так, сетевая безопасность

[103] *Зверянская Л.П.* Организационно-правовое обеспечение международной и национальной информационной безопасности: опыт Китайской Народной Республики. Труды Института государства и права РАН. 2017. Т. 12. № 5. С. 207.

определяется как способность предотвращать сетевые атаки, вторжения, повреждения, несанкционированные доступ и использование, непредвидимые происшествия посредством осуществления необходимых мер для поддержания устойчивой и надежной работы сети, обеспечения целостности, конфиденциальности и удобства использования сетевых данных. Под критически важной информационной инфраструктурой понимается область государственных коммуникационных и информационных услуг, энергетики, дорожного и иного транспорта, ирригации, финансов, государственных услуг, электронного правительства и других ключевых отраслей и секторов, а также другая иная информационная инфраструктура, нанесение ущерба, незаконное использование и утечка данных которой могут нести серьезную угрозу национальной безопасности, национальному благополучию, жизни людей и общественным интересам[104].

Нужно отметить, что политика Китая в области информационной безопасности перекликается в целом с таким аспектом внешней политики Китая, как использование "мягкой силы". В основе китайской стратегии "мягкой силы" лежит концепция "гармоничного мира". Новые политические инициативы, такие как "улыбчивая дипломатия", "публичная дипломатия" и "добрососедская дипломатия", играют важную роль в стремлении Пекина влиться в интеграционные процессы и стать неформальным лидером. Китай широко использует такой инструмент "мягкой силы", как распространение китайского языка, с широкой опорой на культуру и образование. При этом решаются две проблемы — укрепление глобальной притягательности Китая и нейтрализация негативного влияния западной культуры на граждан КНР. Особенностью китайского подхода к "мягкой силе" является ее принципиальная ненавязчивость, невмешательство в чужие дела, уважение к чужому суверенитету и самобытности, желание создать гармоничный справедливый миропорядок, который бы не ущемлял ничьих интересов и способствовал развитию каждого через равномерное развитие.

[104] Ibid. С. 208.

В КНР особое внимание уделяется совершенствованию средств контроля за информационным пространством. В настоящее время в стране действует двухступенчатая система фильтрации и мониторинга всего интернет-трафика, для поддержания порядка в сети Интернет созданы специальные подразделения киберполиции и киберцензоров, установлены строгие обязательства и юридическая ответственность провайдеров и операторов сети, физических и юридических лиц.

3. Основные этапы международного сотрудничества по вопросам информационной безопасности

За последние двадцать с небольшим лет наблюдается активизация международного сотрудничества по вопросам информационной безопасности, причем как на двусторонней, так и на многосторонней основе, в рамках ООН, Совета Европы, ШОС, ОДКБ, ОБСЕ, НАТО и др., при этом речь, как правило, идет об адаптации международного права к особенностям киберпространства. Россия неизменно выступает за формирование глобального правового режима, не допускающего использование информационных технологий в целях, несовместимых с международной стабильностью. Вот некоторые наиболее значимые вехи многостороннего международного сотрудничества.

С 1998 года ГА ООН ежегодно принимает резолюцию: "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности".

1998 год – Резолюция ГА ООН 53/70 от 4 декабря 1998 года "Целесообразность разработки международных принципов, направленных на укрепление безопасности глобальных информационных и телекоммуникационных сетей и способствующих борьбе с информационным терроризмом и преступностью".

2000 год – восемь ведущих государств мира, включая Россию, приняли Окинавскую хартию глобального информационного общества от 22 июля 2000 года. Согласно Хартии предлагается в целях развития глобального информационного общества предпринять "согласованные действия по созданию безопасного и свободного от преступности киберпространства".

2001 год – принята и в 2004 году вступила в силу Будапештская конвенция Совета Европы о преступности в сфере компьютерной информации (о киберпреступности). Конвенция продвигалась

странами Запада как ключевой инструмент противодействия преступности с использованием информационных технологий. Россия не присоединилась к указанной конвенции.

2006 год – в рамках ООН с этого времени развивается сотрудничество по управлению Интернетом (во многом в противоположность управления Интернетом со стороны США, в частности, ICANN). В результате под эгидой Генерального секретаря ООН был создан Форум по вопросам управления Интернетом, функционирующий как многоуровневая переговорная площадка, в рамках которой на равных принимают участие государства, бизнес, НПО и представители академического сообщества. Хотя многие исследователи склонны видеть в создании подобного рода переговорных площадок инструмент доминирования в международных процессах развитых стран, широкое распространение многоуровневых моделей глобального управления представляет собой одну из современных тенденций мировой политики.

2008 год – в Таллине создан Объединенный центр в сфере кибероборонь НАТО.

2009 год – заключено и в 2011 году вступило в силу Соглашение между Правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности.

2009 год – с этого момента в рамках ОДКБ проводятся ежегодные учения "ПРОКСИ" (противодействие криминалу в сфере информации).

2010 год – принята новая стратегическая концепция кибербезопасности НАТО ("Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organization").

2011 год – проведен неофициальный саммит ОДКБ. Были обсуждены вопросы информационной безопасности и контроля над Интернетом, предложения по укреплению "информационного суверенитета". При этом в рамках ОДКБ реализуется утвержденная президентами Программа совместных действий по формированию системы информационной безопасности. Программа охватывает, в частности, следующие направления:

- совместные научные и исследовательские разработки и обмен информацией о достижениях в этой области;
- подготовка кадров;
- унификация законодательной и нормативно-правовой базы;

- совместное обеспечение безопасности жизненно важных объектов;

- проведение совместных мероприятий, направленных на борьбу с преступлениями в сфере информационных технологий.

2011 год – постоянные представители Китая, России, Таджикистана и Узбекистана в ООН направили Генсекретарю ООН совместное письмо с просьбой распространить Международный кодекс по обеспечению безопасности в сфере информации в качестве официального документа ООН на 66 сессии ГА ООН. В кодексе определены права и обязанности государств в информационном пространстве.

2011 год – Россия разработала проект Конвенции об обеспечении международной информационной безопасности (концепция).

2013 год – между Россией и США заключены "Договоренности о мерах укрепления доверия в сфере использования ИКТ".

2014 год – опубликована новая оперативная концепция армии США "Победа в сложном мире. 2020–2040".

2014 год – начал работу Центр НАТО в области стратегических коммуникаций (Стратком).

2014 год – в рамках ОДКБ создан Консультационный координационный центр по вопросам реагирования на компьютерные инциденты (ККЦ ОДКБ).

2015 год – завершение работы группы правительственных экспертов ООН (Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности). Главный итог: признание необходимости выработки правил поведения государств в киберпространстве.

2015 год – в Таллине создан Кибернетический тренировочный центр НАТО.

2017 год – Россия внесла на рассмотрение ООН проект "Конвенции о сотрудничестве в сфере противодействия информационной преступности".

2017 год – в Финляндии создан Европейский центр противодействия гибридным угрозам.

2018 год – рассмотрение российских инициатив в области информационной безопасности в профильных комитетах ООН и проведение форума по вопросам управления Интернетом.

2018 год – форум по вопросам управления Интернетом. Президент Франции озвучил инициативу "Парижский призыв к доверию и безопасности в киберпространстве" (Paris Call for Trust and Security in Cyberspace)[105].

2018 год – ГА ООН приняла российскую резолюцию по международной информационной безопасности: "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности". Ее поддержало подавляющее большинство государств. Более 30 стран из всех регионов мира стали ее соавторами. Данный документ открыл новый этап в глобальной дискуссии по международной информационной безопасности (эта проблема была впервые включена в повестку дня ООН в 1998 г. по инициативе России). Генеральной Ассамблее удалось принять прорывные решения, нацеленные на реальное укрепление этой дискуссии. Главная задача – защитить интересы всех стран в цифровой сфере, вне зависимости от того, на каком уровне технологического развития они находятся. Речь идёт о ряде исторических новаций в документе. Это свод из тринадцати правил, норм и принципов ответственного поведения государств в информационном пространстве. По сути, это первые в истории "правила дорожного движения" в цифровой сфере. Их смысл – заложить основу мирного взаимодействия государств в ней, обеспечить предотвращение войн, конфронтации и любых агрессивных действий. В ООН создаётся рабочая группа по МИБ открытого состава (РГОС) по международной информационной безопасности. В резолюции предусмотрен механизм консультаций РГОС с бизнесом, неправительственными организациями и научным сообществом.

2019 год – принята Резолюция ГА ООН A/RES/74/247 "Противодействие использованию информационно-коммуникационных технологий в преступных целях". Резолюция предусматривает учреждение специального межправительственного комитета экспертов открытого состава, представляющего все регионы, для разработки всеобъемлющей международной конвенции о

[105] *Молчанов Н.А., Матевосова Е.К.* Концептуально-политический и формально-юридический анализ Парижского призыва к доверию и безопасности в киберпространстве и российские инициативы в области международного права // Актуальные проблемы российского права. 2020. № 1 (110). С. 133–141.

противодействии использованию информационно-коммуникационных технологий в преступных целях.

4. Интернет и ИКТ

Интернет – это глобальная информационная система, составными частями которой являются различные информационные сети. С технической точки зрения Интернет состоит из самых разнообразных устройств, серверов, маршрутизаторов, кабелей, компьютеров конечных пользователей. С помощью всех этих устройств в рамках Интернета передается определенная информация. Всемирная коммуникационная паутина WorldWideWeb – WWW – это один из сервисов Интернета, связанные гиперссылками текстовые страницы, а также видео с программами для их воспроизведения и распространения. Другие сервисы Интернета: электронная почта, файлообменные сети, IP-телефония, электронные платежные системы и др.

Например, в рамках "Проекта управления Интернетом" при Сиракузском университете (Internet governance project) выделяются следующие особенности Интернета:

1. Открытость стандартов. Интернет основывается на открытых технических стандартах, которые может использовать бесплатно каждый пользователь. Иногда стандарты платные, но цена разумная.

2. Рыночные механизмы. Сети в Интернете нередко частные. Большая часть инвестиций идет из частного сектора. Услуги координируются, как правило, на рыночной основе. Активно идет коммерциализация киберпространства.

3. Интеллектуальные средства и контрольные функции, как правило, рассредоточены на периферии сетей. Сети передают информацию и протоколы, технологически нейтральные.

4. Интернет – глобален. Он не локализован ни в одном отдельном государстве, соединения устанавливаются вне зависимости от границ.

Согласно сведениям, которыми располагает Интерпол, в Интернете преступность растет самыми быстрыми темпами. Нарастает количество попыток несанкционированного вмешательства в государственные, военные, банковские, корпоративные

компьютерные системы, компьютеры отдельных пользователей[106]. При этом объектами информационных атак (кибератак) становятся уже не только информационные ресурсы в Интернете, но и критически важные объекты инфраструктуры отдельных государств, что представляет особую опасность.

Исследователи отмечают следующие специфические черты современного Интернета: главным образом в Интернете используется английский язык. Второй по распространению – китайский. Создан домен на кириллице .рф. Наибольшее число пользователей Интернета находится в Азии и на Ближнем Востоке. Как правило, соединения в Интернете осуществляются не с помощью стационарных ЭВМ, а через мобильные устройства, которые при этом имеют не статические IP-адреса (присваиваются навсегда), а динамические, присваиваемые на время подключения.

Особо популярными стали блоги и социальные сети. Пользователи становятся активными участниками обмена информацией. Число пользователей Фейсбук превысило один миллиард, по объему трафика это первая сеть в мире. Происходит слияние различных сетей с участием Интернета. Все более популярной становится облачная обработка данных.

Активно идет коммерциализация киберпространства, причем не столько по государственной линии, сколько за счет частных, подчас транснациональных компаний, а также научных сообществ, ВУЗов, научно-исследовательских центров, организаций гражданского общества. До настоящего времени безопасность киберпространства обеспечивалась, как правило, государствами, однако в этой области стали действовать и частные компании.

На нынешнем этапе научно-технического развития человечества важную роль стали играть ИКТ (информационно-коммуникационные технологии) (Information and Communication Technologies).

Существует согласие[107] и в том, что ИКТ-среда является новым пространством международных отношений. Основными признаками,

---

[106] *Сафронова И.Л.* Информационная безопасность: основные проблемы и перспективы // Вестник Самарского государственного технического университета. Серия: Психолого-педагогические науки. 2006. С. 182.

[107] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности. 22 июля 2015 г., A/70/174.

отличающими ИКТ-среду от традиционных пространств реализации отношений суверенных государств (суши, моря, воздушного пространства), являются:

искусственный характер ИКТ-среды, образуемой совокупностью средств телекоммуникаций, вычислительной техники, программного обеспечения, функционирующих в системе глобальных цифровых идентификаторов, работоспособность которой поддерживается усилиями, прежде всего, негосударственных организаций, находящихся в различных юрисдикциях;

виртуальность процессов применения ИКТ, следствием которой является невозможность непосредственного наблюдения условий возникновения инцидентов в ИКТ-среде;

трудность определения источников инцидента в ИКТ-среде;

дестабилизирующие последствия злонамеренного или враждебного использования ИКТ против критически важной инфраструктуры общества, совершения террористических нападений на объекты ИКТ-среды и связанную с ИКТ инфраструктуру;

использование ИКТ террористическими организациями для вербовки сторонников, финансирования, обучения, подстрекательства и проведения терактов.

Современный научно-технический уклад в целом (а не только киберпространства) нередко описывается аббревиатурой NBIC, при этом имеется в виду конвергенция четырёх типов технологий: нано-, био-, инфо- и когно-технологий[108] (иногда вместо NBIC используется NBICS (нано-, био-, инфо-, когно- и социальные технологии), поскольку возрастает роль социальных технологий. Популярность приобретает концептуализация современного этапа технологического развития в терминах "промышленной революции 4.0" (Industry 4.0). Эта концепция предполагает повсеместное распространение устройств, подключенных к Интернету, что влечёт за собой трансформацию промышленного производства, основанную на интеграции виртуальных и реальных производительных сил, что в свою очередь коренным образом изменяет все сферы жизни общества и государства (как это произошло, в своё время, в ходе других

[108] *Wolbring G.* Why NBIC? Why human performance enhancement? // Innovation: The European journal of social science research. 2008. No. 1. Pp. 25–40.

промышленных революций после появления парового двигателя, конвейера и массового производства, компьютеров и ЭВМ)[109].

Итак, Интернет способствует глобализации, свободному обмену информацией без учета государственных границ, географии и языка. При этом, однако, человеческое общество не становится гомогенизированным, наоборот, происходит его сегментация и маргинализация. Число конфликтных ситуаций не снижается, растет киберпреступность и терроризм, сталкиваются интересы разных государств, идет информационная война. Возрастает роль информационной безопасности. Сложилась триада угроз, связанных с использованием Интернета: использование его в преступных, террористических и военно-политических целях.

5. "Международная информационная безопасность" и "кибербезопасность". Управление Интернетом

К настоящему времени сложилась двойственность в использовании терминов при описании проблем безопасности в информационном пространстве. США, другие страны НАТО, государства-члены ЕС чаще используют термин "кибербезопасность". Россия, страны, входящие в ШОС, ОДКБ, СНГ, как правило, оперируют термином "международная информационная безопасность" или его более коротким аналогом "информационная безопасность". За использованием различных терминов скрывается несколько различное понимание такой безопасности.

Видимо, различие в подходах более или менее ясно обозначилось в 1998 году. Тогда Россия, используя термин "международная информационная безопасность" (МИБ), попыталась вложить в него собственное понимание безопасности. Однако страны Запада, а также представители бизнес-сообщества и некоторые международные организации выразили свое несогласие с предложенным подходом, предлагая придерживаться уже сложившейся к тому моменту практики и продолжать использовать термин "кибербезопасность". Поначалу казалось, что различие больше техническое,

[109] *Шваб К.* Четвертая промышленная революция. М.: Эксмо, 2016. С. 11.

терминологическое. Но в дальнейшем стало ясно, что речь идет о принципиальных различиях в подходах[110].

В основе подхода России к обеспечению безопасности в информационном пространстве стоит идея о том, что государство имеет право распространять свои законы и в целом суверенные права на информационную инфраструктуру, расположенную на его территории[111]. Если так, то в таком случае государство рассматривает свои действия по ограничению доступа к тому или иному контенту как в принципе правомерные. Иными словами, в таком случае государство рассматривает себя не столько как источник распространения контента, сколько как объект, подвергающийся воздействию враждебного контента. В частности, государство полагает, что не столько оно вмешивается в дела других государств, сколько само подвергается такому вмешательству.

Понятно, что страны Запада, особенно США, которые обоснованно считают себя родоначальниками Интернета, и которые в силу своих доктринальных установок рассматривают весь остальной мир как зону своих интересов и, соответственно, полагают, что обладают правом на вмешательство во внутренние дела других стран, не согласны с российским подходом. Более того, в странах Запада, как правило, популярны идеи либерализма, саморегулирования. Применительно к Глобальной сети это означает отрицание права государства на его регулирование.

В США изначально сложилась модель, основанная на саморегулировании всех участников системы, которая позже оформилась в "модель управления Интернетом при участии всех заинтересованных сторон" (multistakeholder internet governance). Данная модель предполагает равноправное участие в управлении всех сторон или их выбранных представителей, а также общее понимание заинтересованности всех участников в развитии Глобальной сети. Первоначально в список "заинтересованных сторон" (stakeholders) входили государственные структуры, частный сектор и гражданское

---

[110] *Нежельский А.А.* Информационная безопасность государств и граждан в нем: ключевые компоненты и группы интересов // Азимут научных исследований: экономика и управление. 2017. Т. 6. № 3(20). С. 405.

[111] *Терентьева Л.В.* Понятие киберпространства и очерчивание его территориальных контуров // Правовая информатика. 2018. № 4. С. 69–70.

общество. Позже список пополнили представители экспертного сообщества и организованные сообщества интернет-пользователей.

С технической точки зрения Интернет, в первую очередь, управляется через систему доменных имен и интернет-адресов, выработку параметров интернет-протоколов. В настоящее время это осуществляется через частную некоммерческую организацию ICANN (Internet Corporation for Assigned Names and Numbers), зарегистрированную в Калифорнии. Изначально Интернет был создан в рамках Агентства перспективных разработок (Advanced Research Project Agency, ARPA) Минобороны США. В дальнейшем функции управления системой доменных имен (Domain Name System, DNS) были переданы ICANN. В ноябре 1998 г. был подписан Меморандум о взаимопонимании между ICANN и Министерством торговли США. В функции ICANN входит решение следующих задач: координация работ по выработке технических параметров интернет-протоколов; выполнение административных функций по управлению базами данных корневого сервера системы доменных имен (в том числе создание новых доменов верхнего уровня); распределение блоков IP-адресов. В 2016 г. функции управления адресным пространством сети были переданы дочерней организации ICANN Public Technical Identifiers (PTI).

Конечно, управление Интернетом – это не только техническая координация. В широком смысле координация – это борьба с преступностью в Интернете, защита интеллектуальной собственности, прав человека, цензура и др. Надо отметить, что, например, защита прав интеллектуальной собственности в Интернете решается в рамках международных организаций, в частности, ВТО и ВОИС. Россия придерживается позиции о необходимости интернационализации функций ICANN и передачи их Международному союзу электросвязи. Определенные попытки в этом направлении предпринимаются, например, в рамках ООН: в 2006 году был создан Форум по вопросам управления Интернетом. Форум функционирует как многоуровневая переговорная площадка, в рамках которой на равных принимают участие государства, бизнес, НПО и представители академического сообщества.

Согласно определению Рабочей группы ООН по вопросам управления Интернетом, такое управление "представляет собой разработку и применение правительствами, частным сектором и гражданским обществом, при выполнении ими своей

соответствующей роли, общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение Интернета".

Различие в подходах к содержанию терминов, описывающих безопасность в информационном пространстве, связано также с пониманием содержания терминов "киберпространство" и "информационное пространство". Можно попробовать определить содержание понятия "киберпространство" как совокупность компьютерных и иных электронных сетей и находящейся в них информации. Информационное пространство – вся информация и данные, существующие как в виртуальном, так и в реальном измерении. Предположительно понятие "информационное пространство" шире, чем "киберпространство". Хотя тут надо отметить, что пока не сложилось точное в юридическом смысле понимание того, что именно надо понимать под "киберпространством". Различия в подходах не носят принципиального характера, но они все-таки имеются[112].

В Доктрине информационной безопасности РФ под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети Интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Согласно документам, принятым в рамках ООН, под МИБ в целом понимается защищенность от триады угроз: террористических, преступных и военно-политических (информационные войны и информационное противоборство). Видимо, к указанной триаде должно также относиться вмешательство во внутренние дела других государств, нарушение общественной стабильности, разжигание межэтнической, межнациональной розни.

Этот подход перекликается с предложениями России о необходимости демилитаризации информационного пространства,

---

[112] *Данельян А.А.* Международно-правовое регулирование киберпространства // Образование и право. 2020. № 1. С. 262.

выработки определенных правил поведения государств. Соответственно, должен быть заключен международный договор, содержащий отказ от создания средств информационного воздействия и осуществления любых возможных агрессивных действий в информационном пространстве.

Нужно отметить, что угрозы международной информационной безопасности не всегда являются результатом умышленных действий, поскольку не исключены риски системных сбоев, а также возможность возникновения угроз в результате случайных событий.

Выделяют два аспекта международной информационной безопасности: информационно-технический и информационно-психологический. Информационно-технический – это защита, контроль и соблюдение законности и правопорядка в информационной сфере (защита от несанкционированного доступа, хакерских взломов компьютерных сетей и сайтов, логических бомб, компьютерных вирусов и вредоносных программ, несанкционированного использования частот, радиоэлектронных атак и др.). Информационно-психологический: защита психологического состояния общества и государства от негативного информационного воздействия.

Важный вопрос при обеспечении ИКТ – это защита так называемых "критических информационных инфраструктур". Согласно ст. 2 ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации":

"6) критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

7) объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры".

Вероятно, атаку США на ядерное оборудование Ирана в 2010 году с помощью вируса, воздействовавшего на программное обеспечение, управлявшего центрифугами по обогащению урана (Stuxnet), можно рассматривать именно как атаку на критические информационные инфраструктуры. Таким образом, угрозы с использованием ИКТ – вполне объективная реальность, которая может рассматриваться как casus belli.

Следует отметить, что США и их союзники возражают против подхода России к определению международной информационной безопасности, ссылаясь на то, что в таком случае в МИБ будет включен слишком широкий круг вопросов, по которому вряд ли удастся найти общие подходы.

В целом, Россия, как и Китай, предлагают полную демилитаризацию информационного пространства, ссылаясь на то, что гонка вооружений в информационной сфере способна расшатать сложившиеся договоренности о разоружении и международной безопасности.

США, как и ЕС, придерживаются позиции, согласно которой ключевыми угрозами кибербезопасности являются кибертерроризм и киберпреступность, а межгосударственные конфликтные вопросы надо регулировать в рамках международного гуманитарного права.

Нужно отметить, что в России предпринимались попытки, но пока безуспешные, найти общее понимание содержания терминов "МИБ" и "кибербезопасность". Например, в 2012–2013 гг. в Совете Федерации России была предпринята попытка привлечь экспертов к составлению единого доктринального документа – концепции стратегии кибербезопасности Российской Федерации.

В России содержание термина "международная информационная безопасность", видимо, наиболее полно отражено в проекте Конвенции об обеспечении международной информационной безопасности от 22 сентября 2011 года ("Конвенция об обеспечении международной информационной безопасности (Концепция)"). Там содержится следующий текст: "информационная безопасность — состояние защищенности интересов личности, общества и государства от угроз деструктивных и иных негативных воздействий в информационном пространстве".

В целом в указанном проекте, особенно в статье 4, раскрывается, что именно подразумевается под информационной безопасностью.

В соответствии с утвержденной Президентом Российской Федерации Доктриной информационной безопасности Российской Федерации, под информационной безопасностью России понимается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-

экономическое развитие Российской Федерации, оборона и безопасность государства.

В Доктрине сформулированы основные положения государственной политики обеспечения информационной безопасности Российской Федерации, а в качестве приоритетного направления такой политики называется правовое обеспечение информационной безопасности, которое должно базироваться, прежде всего, на соблюдении принципов законности и баланса интересов граждан, общества и государства в информационной сфере.

В Будапештской конвенции о компьютерных преступлениях 2001 года термин "кибербезопасность" не используется. Тем не менее в тексте в том или ином контексте упоминается безопасность в целом, например: "запрашиваемая Сторона полагает, что исполнение этой просьбы может нанести ущерб ее суверенитету, безопасности, общественному порядку или другим важным интересам". И в целом из контекста конвенции следует, что она направлена на обеспечение безопасности, возникающей в силу угрозы компьютерных преступлений.

6. Акты агрессии с использованием ИКТ

Важный вопрос, связанный с обеспечением безопасности в связи с использованием киберпространства: следует ли рассматривать какие-либо действия в киберпространстве как акт агрессии. Как известно, ключевую роль в вопросе о квалификации тех или иных действий как акт агрессии играет такой документ, как Резолюция ГА ООН 3314 (XXIX) от 14 декабря 1974 года "Определение агрессии". Конечно же, в указанной резолюции не упоминается ни Интернет, ни безопасность информационных технологий – потому, что такие понятия в то время просто не существовали. Однако в какой-то мере этот документ может быть применим и к вопросам безопасности информационных технологий. В резолюции используется следующее определение:

"Агрессией является применение вооруженной силы государством против суверенитета, территориальной неприкосновенности или политической независимости другого государства, или каким-либо другим образом, несовместимым с Уставом Организации Объединенных Наций, как это установлено в настоящем определении".

Можно ли считать использование, например, Интернета, как акт применения вооруженной силы? В период принятия "Определения агрессии", конечно же, не имелись в виду какие-либо действия в информационном пространстве. Однако в указанном определении ясно сказано также: "или каким-либо другим образом", что оставляет возможность для разных толкований. В любом случае, явно назрела необходимость уточнить эти положения[113].

Казалось бы, использование киберпространства – это всего лишь передача какой-то информации. Разве можно приравнивать передачу информации к применению силы, а тем более вооруженной силы? Такая постановка вопроса вовсе не праздная: если действия в киберпространстве можно квалифицировать как акт агрессии, это дает право государству, подвергшемуся такой агрессии, применять ответные меры, в том числе прямо применять вооруженную силу. И в определенных ситуациях можно приравнивать действия в информационном пространстве к применению вооруженной силы. Самый показательный пример – это уже упоминавшаяся выше атака со стороны США с помощью вируса Stuxnet в 2010 году на центрифуги, использовавшиеся Ираном для обогащения урана. Результат атаки не совсем ясен. По сведениям из некоторых источников атака была лишь относительно успешной. Вирус заставлял центрифуги вращаться слишком быстро, и, по замыслу американцев, те должны были разрушаться. Якобы иранцы довольно быстро разобрались с проблемой, и ущерб, а также задержки в производстве были незначительны. Однако госсекретарь США Х. Клинтон в 2011 г. заявила, что проект по разработке вируса Stuxnet оказался успешным, и иранская ядерная программа якобы была отброшена на несколько лет назад.

Возможно, операция Stuxnet может быть квалифицирована как применение силы. Но "Определение агрессии" ясно говорит именно о "вооруженной силе". Международное право не содержит какого-либо общего запрета на применение силы, тем более в киберпространстве, хотя существует такой общепризнанный принцип, как неприменение

---

[113] *Костин С.А.* Международно-правовое обеспечение коллективной кибербезопасности – направление для сотрудничества и интеграции в Европе и на Евразийском пространстве // Международные отношения и общество. 2019. Т. 1. № 3. С. 45.

силы или угрозы силой. Тут явно возникает определенная теоретическая и практическая проблема[114].

С формальной стороны использование киберпространства для действий, наносящих существенный ущерб интересам какого-либо государства или его лиц, предполагает уточнение вопроса об ответственности государства, с территории которого были совершены указанные действия, или ответственности государства за действия своих граждан. Понятна настороженность многих стран к такой постановке вопроса, поскольку можно предполагать, что пострадавшее государство предпримет какие-то ответные меры в отношении страны, с территории которой было совершено действие, нанесшее существенный ущерб, тем более действие граждан этой страны. О каких ответных мерах может идти речь? Например, подача иска в суд и в случае выигрыша дела обращение взыскания на активы страны-ответчика. Теоретически возможен и иной вариант: применение в отношении такой страны вооруженной силы.

Конечно, можно понять такую настороженность. А что, если таким правом воспользуются государства, нередко прибегающие к применению вооруженной силы и по меньшим поводам? Не даст ли норма, закрепляющая ответственность государств за акты злоупотребления ИКТ, право все тем же США наносить ракетно-бомбовые удары по территории государства, откуда предположительно была совершена хакерская атака?

Мало того, понятно, что возможности государства по контролю использования, например, Интернета, злонамеренными лицами вовсе не безграничны. Для хакерской атаки не нужно владеть каким-то особым оборудованием или обладать какими-то сверхъестественными знаниями, такую атаку может совершить довольно широкий круг лиц. Как может государство гарантированно предотвратить такие действия?

С другой стороны, точно так же понятно, что государство не должно полностью устраняться от контроля за действиями своих

---

[114] *Капустин А.Я.* К вопросу о международно-правовой концепции угроз международной информационной безопасности // Журнал зарубежного законодательства и сравнительного правоведения. 2017. № 6. С. 49–50; *Данельян А.А.* Международно-правовое регулирование киберпространства // Образование и право. 2020. № 1. С. 263.

граждан или за действиями со своей территории, тут явно требуются какие-то нормы хотя бы самого общего плана[115].

Как бы то ни было, операция Stuxnet показала, что использование информационного пространства в определенных целях может вести к вполне осязаемым материальным потерям, сопоставимым с потерями, например, от прямой бомбардировки. В результате страны НАТО сделали для себя вполне определенные выводы. Так, Таллинский центр НАТО разработал в 2013 году "Руководство по международному праву, применимому к ведению военных действий в киберпространстве" ("Tallinn Manual") – в феврале 2017 года вышло его второе издание. Согласно указанному документу возможно применение достаточно широкого круга кинетического оружия против государств или отдельных лиц, стоящих за атаками в киберпространстве. По логике данного Руководства, Иран в ответ на атаку Stuxnet был вправе применить в ответ кинетическое оружие.

Легализует ли в правовом смысле Таллинское руководство применение силы в киберпространстве, вплоть до действий, которые можно квалифицировать как военные? Некоторые российские специалисты именно так и полагают и в этой связи критически относятся к Таллинскому руководству как к документу, разрешающему использовать информационно-коммуникационные технологии в военных целях.

А если объектом атаки, подобной Stuxnet, окажутся, например, критические информационные инфраструктуры Российской Федерации? Таллинское руководство создает в таком случае для России правовую основу для применения против тех, кто стоит за атакой (то есть против государств или лиц, действующих в интересах этих государств – proxy actors), вооруженной силы, в том числе квалифицируя подобные действия как акт агрессии. Тем более что Россия и ее структуры, в том числе государственные, уже не раз становились объектами кибератак. Наверное, учет такой возможности создаст основу для того, чтобы пересмотреть, хотя бы частично,

[115] *Молчанов Н.А., Матевосова Е.К.* Информационный терроризм в международно-правовом контексте // Вестник Университета имени О.Е. Кутафина (МГЮА). 2018. № 5. С. 96.

критическое отношение российских специалистов к Таллинскому руководству.

Может ли критическое отношение к Таллинскому руководству препятствовать использованию ИКТ в военных целях? Может ли воспрепятствовать проведению информационных войн? Вряд ли. Дело в том, что сила стоит выше международного права, так объективно сложилось в современных международных отношениях. Применение силы, а также угроза применения силы являются крайними средствами защиты своих интересов тем или иным государством. Даже если такое применение силы запрещено международным правом, это не является стопроцентной гарантией того, что та или иная страна не прибегнет к применению вооруженной силы вопреки запрету. Крайнее (последнее) средство по определению является тем, к чему можно прибегнуть в самой крайней ситуации, нарушая любые запреты.

Конечно, тут могут возразить, что если определенный способ применения вооруженной силы запрещен международным правом, то остальные государства могут жестко наказать за подобные действия. Но этот аргумент применим только к государству-нарушителю, которое не является ядерным, не является постоянным членом СБ ООН. Наверное, он не всегда применим и к государству, обладающему мощной армией и способному дать отпор попыткам его наказать. Этот аргумент, скорее всего, не в полной мере применим и к военным союзникам ядерных государств и также постоянных членов СБ ООН. В конце концов, далеко не всегда государства-члены СБ ООН могут прийти к согласию по вопросу о применении силы к государству-нарушителю.

Мало того, в настоящее время использование киберпространства (Интернета) вообще никак не ограничено международно-правовыми запретами, признаваемыми всеми государствами или хотя бы всеми крупнейшими странами. В Интернете практически повсеместно используются те или иные вирусы. Часто это делается для сбора той или иной информации. Но нередко имеет место использование в том числе разрушительных вирусов, направленных против критических информационных структур. Информационное пространство используется для подрывной пропаганды, для вмешательства в дела других государств. И такие действия пока никак эффективно не ограничены и не регулируются на международной основе. В лучшем случае речь идет о мерах, принимаемых на национальном уровне.

Иными словами, киберпространство и так используется государствами без особых ограничений для ведения, по сути, наступательной кибервойны. Для этого не требуется никакая дополнительная легализация со стороны, например, упомянутого Таллинского руководства.

В Будапештской конвенции 2001 года нет никакого упоминания об агрессии. Оно и понятно, этот документ направлен не против действий государств, а против действий отдельных лиц, противоправно злоупотребляющих ИКТ. Такие действия квалифицируются как уголовные преступления.

В "Стратегии национальной безопасности Российской Федерации до 2020 года" (утв. Указом Президента РФ от 12 мая 2009 г. № 537) термин "агрессия" упоминается в п. 26:

"Стратегическое сдерживание предполагает разработку и системную реализацию комплекса взаимосвязанных политических, дипломатических, военных, экономических, информационных и иных мер, направленных на упреждение или снижение угрозы деструктивных действий со стороны государства-агрессора (коалиции государств)".

Как видно из этого текста, Россия рассматривает информационное пространство как место для проведения операций по противостоянию агрессии.

В "Основах государственной политики Российской Федерации в области международной информационной безопасности" (утв. Президентом РФ от 24 июля 2013 г. № Пр-1753) содержится следующее положение:

"8. Основной угрозой в области международной информационной безопасности является использование информационных и коммуникационных технологий:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности".

В пункте 10 указанного документа сказано:

"Достижению цели государственной политики Российской Федерации будет способствовать участие Российской Федерации в решении следующих задач:

а) формирование системы международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях;

б) создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности".

Там же содержатся следующие положения:

"12. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по созданию условий, способствующих снижению риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности, являются:

а) развитие диалога с заинтересованными государствами о национальных подходах к противодействию вызовам и угрозам, возникающим в связи с масштабным использованием информационных и коммуникационных технологий в военно-политических целях;

б) участие в выработке на двустороннем и многостороннем уровнях мер по укреплению доверия в области противодействия угрозам использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии;

в) содействие развитию региональных систем и формированию глобальной системы международной информационной безопасности на основе общепризнанных принципов и норм международного права (уважение государственного суверенитета, невмешательство во внутренние дела других государств, неприменение силы и угрозы силой в международных отношениях, право на индивидуальную и коллективную самооборону, уважение прав и основных свобод человека)".

В "Доктрине информационной безопасности Российской Федерации" (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) говорится:

"8. Национальными интересами в информационной сфере являются:

……

б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее — *критическая информационная инфраструктура*) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время".

Там же содержатся следующие положения:

"20. Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности".

Россия в 2011 году разработала проект Конвенции об обеспечении международной информационной безопасности (концепция). В статье 4 указанного проекта содержится следующая формулировка:

"В качестве основных угроз в информационном пространстве, приводящих к нарушению международного мира и безопасности, рассматриваются следующие:

1) использование информационных технологий и средств для осуществления враждебных действий и актов агрессии".

В статье 5 сказано:

"9) государства-участники признают, что агрессивная "информационная война" составляет преступление против международного мира и безопасности;

……

11) каждое государство-участник имеет неотъемлемое право на самооборону перед лицом агрессивных действий в информационном пространстве в отношении его при условии достоверного установления источника агрессии и адекватности ответных мер".

В Письме постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации

Объединенных Наций на имя Генерального секретаря от 12 сентября 2011 г. A/66/359 от 14 сентября 2011 г. предусмотрены следующие формулировки:

"Каждое государство, добровольно соблюдающее настоящие Правила, обязуется:

……

b) не использовать информационно-коммуникационные технологии, включая сети, для осуществления враждебных действий, актов агрессии, создания угроз международному миру и безопасности или распространения информационного оружия или соответствующих технологий;

…….

e) подтверждать права и обязанности каждого государства, в соответствии с надлежащими нормами и правилами, в отношении законной защиты своего информационного пространства и критической информационной инфраструктуры от ущерба в результате угроз, вмешательства, атак и актов агрессии".

В приложении "Правила поведения в области обеспечения международной информационной безопасности" к Письму постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций на имя Генерального секретаря от 9 января 2015 г. A/69/723 сказано:

"Каждое государство, добровольно соблюдающее настоящие Правила поведения, обязуется:

……..

6. Подтверждать права и обязанности каждого государства, в соответствии с надлежащими нормами и правилами, в отношении законной защиты своего информационного пространства и критической информационной инфраструктуры от ущерба в результате угроз, вмешательства, атак и актов агрессии".

В документе, озаглавленном "Вклад Российской Федерации, посвященный общей оценке проблем международной информационной безопасности и угроз международной информационной безопасности (Доклад Генерального секретаря ООН A/56/164/Add.1 от 21 июня 2001 г.)" содержится следующая формулировка:

"Враждебное информационное воздействие на системы связи и управления противоздушных, противоракетных и других систем

обороны обезоруживает государство перед лицом потенциального агрессора, лишает его возможностей использования законного права на самооборону".

В документе ООН "Вклад Российской Федерации, посвященный общей оценке проблем международной информационной безопасности и угроз международной информационной безопасности" (Доклад Генерального секретаря ООН A/56/164/Add.1 от 21 июня 2001 г.) сказано:

"Враждебное информационное воздействие на системы связи и управления противоздушных, противоракетных и других систем обороны обезоруживает государство перед лицом потенциального агрессора, лишает его возможностей использования законного права на самооборону".

В документе ООН "Вклад Российской Федерации, посвященный вопросам, связанным с работой Группы правительственных экспертов ООН по проблеме информационной безопасности" (Доклад Генерального секретаря ООН A/58/373 от 17 сентября 2003 г.) содержится следующий текст:

"17. Следовало бы подумать о возможных путях международного взаимодействия правоохранительных органов по предотвращению и пресечению правонарушений в информационном пространстве, в частности, по выявлению источников информационной агрессии; взглянуть на проблему сопряжения национальных законодательств отдельных стран в части, регулирующей вопросы информационной безопасности, с тем чтобы обеспечить унифицированную классификацию правонарушений в сфере информационной безопасности и ответственность, возникающую в связи с совершением действий, классифицируемых как преступные".

Существуют международные многосторонние договоры, в которых в какой-то мере затрагивается вопрос об актах агрессии в ИКТ. Например, в приложении 2 к Соглашению между Правительствами государств–членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г) сказано следующее:

"Перечень основных видов угроз в области международной информационной безопасности, их источников и признаков

1. Разработка и применение информационного оружия, подготовка и ведение информационной войны.

Источником этой угрозы являются создание и развитие информационного оружия, представляющего непосредственную угрозу для критически важных структур государств, что может привести к новой гонке вооружений и представляет главную угрозу в области международной информационной безопасности.

Ее признаками являются применение информационного оружия в целях подготовки и ведения информационной войны, а также воздействия на системы транспортировки, коммуникаций и управления воздушными, противоракетными и другими видами объектов обороны, в результате чего государство утрачивает способность обороняться перед лицом агрессора и не может воспользоваться законным правом самозащиты; нарушение функционирования объектов информационной инфраструктуры, в результате чего парализуются системы управления и принятия решений в государствах; деструктивное воздействие на критически важные структуры".

В Приложении № 2 к Соглашению между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности от 25 декабря 2013 г. содержится следующий текст:

"Признаки угрозы — применение информационного оружия в целях подготовки и ведения информационной войны, воздействия на системы транспортировки, коммуникаций и управления воздушными, противоракетными и другими видами объектов обороны, в результате чего государство утрачивает способность обороняться перед лицом агрессора и не может воспользоваться законным правом самозащиты; нарушение функционирования объектов информационной инфраструктуры, в результате чего парализуются системы управления и принятия решений в государствах; деструктивное воздействие на критически важные объекты".

В Преамбуле к Соглашению между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности от 11 июля 2014 г. содержится текст:

"будучи убежденными в том, что сотрудничество Сторон является действенным механизмом предотвращения рисков, угроз и агрессии, противостояния им, а также недопущения превращения информационного пространства в театр военных действий".

В том же соглашении предусмотрены также следующие положения:

"Статья 2. Основные угрозы в области обеспечения международной информационной безопасности

При осуществлении сотрудничества в соответствии с настоящим Соглашением Стороны исходят из того, что основными угрозами международной информационной безопасности является неправомерное использование информационных и коммуникационных технологий:

1) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на нарушение суверенитета, территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности".

Примерно такие же положения содержатся в Соглашении между Правительством Российской Федерации и Правительством Южно-Африканской Республики о сотрудничестве в области обеспечения международной информационной безопасности от 4 сентября 2017 г.

Итак, несомненно, существует проблема международно-правового урегулирования вопроса о квалификации действий государств в ИКТ как актов агрессии. Позиция России тут достаточно четко сформулирована как в ее национальных документах, так и в документах, представленных в ООН от ее имени. Более того, в определенной мере вопрос об агрессии с использованием ИКТ затронут и в некоторых международных соглашениях с участием России.

Можно пытаться применить к ситуациям с совершением актов агрессии в информационной среде "Определение агрессии" от 1974 года, особенно если будет приниматься соответствующее решение в СБ ООН. Однако еще предстоит предпринять значительные усилия, чтобы выработать общепринятые международно-правовые нормы, которые прямо бы регулировали эту проблему.

7. Информационная среда: право на войну и правила ведения войны

В отдельной главе мы рассмотрели, какие действия можно рассматривать как агрессию в информационной среде, а также какие

действия с использованием ИКТ могут рассматриваться как повод к войне (casus belli). При разработке норм международного права, регулирующих поведение в информационной среде, следует различать jus ad bellum и jus in bello. Первое – это "право войны", а второе – "правила ведения войны". Право войны (право на войну) включает право на самооборону (в том числе в случае агрессии), а также право начать военные действия по справедливому поводу. Второе – это правила ведения войны (правила цивилизованного ведения вооруженных действий).

Итак, правила ведения войны с использованием ИКТ. По этому вопросу в научной среде сложилось более или менее однородное понимание, что к информационной среде применимы уже существующие международные соглашения, представляющие основу современного гуманитарного права. Речь идет, в частности, о следующих договорах:

Женевская конвенция 1964 г. об улучшении состояния раненых на поле боя;

Гаагские конвенции 1899 г. и 1907 г. о законах и обычаях сухопутной войны;

Женевский протокол 1928 г. о запрещении использования на войне удушающих газов и бактериологического оружия;

Женевская конвенция 1949 г. об улучшении состояния раненых и больных и членов экипажа судов на море;

Женевская конвенция 1949 г. об обращении с военнопленными;

Женевская конвенция 1949 г. об улучшении положения гражданского населения во время войны;

Женевская конвенция 1975 г. о запрещении разработки создания и хранения бактериологических и токсических вооружений и их уничтожении;

Дополнительные протоколы к Женевским конвенциям 1977 г. о защите жертв международных вооруженных конфликтов, о защите жертв немеждународных вооруженных конфликтов, о принятии дополнительных отличительных знаков.

Конечно, в указанных международных договорах не упомянуты ни информационно-коммуникационные технологии, ни сеть Интернет. Тем не менее, по мнению многих специалистов, изложенные в указанных договорах нормы могут в той или иной мере применяться в случае, если в информационной среде возникнут ситуации, которые можно будет рассматривать как войну, как применение вооруженных

сил. Однако точно так же понятно, что при разработке будущих международных норм, регулирующих поведение в информационной среде, было бы желательно отдельно уточнить или подробно заново сформулировать и соответствующие нормы гуманитарного права. При этом наверняка поначалу позиции тех или иных государств будут радикальным образом отличаться. Например, США в настоящее время вряд ли согласятся на какую-либо правовую регламентацию в этой сфере, рассматривая сеть Интернет как нечто свободное от государственного регулирования. Такая позиция, надо полагать, сформировалась в связи с тем, что Соединенные Штаты исходят из своего тотального доминирования в информационной среде. Соответственно, любые нормы, ограничивающие тут деятельность, будут препятствовать вмешиваться во внутренние дела других государств, вести информационную войну, заниматься сбором чувствительной информации, совершать те или иные кибератаки на объекты других стран.

Вряд ли, однако, такое доминирование сохранится надолго. Возможно, что уже сейчас США утрачивают такие доминирующие позиции или даже уже их утратили. При этом, как только утрата доминирующего положения станет очевидной, то есть как только они сами будут становиться объектом разрушительных кибератак, информационных войн или вмешательства во внутренние дела, с этого момента, скорее всего, США изменят свою позицию и будут активно выступать за заключение соответствующих международных договоров. Во всяком случае, именно это ранее и происходило применительно к ядерному оружию или использованию Космоса.

Россия пока в целом выступает за демилитаризацию информационного пространства, ссылаясь при этом на сложившееся международно-правовое регулирование поведения в Космосе или, например, в Антарктике. Конечно, в связи с изменением баланса сил в информационной среде и эта позиция может претерпеть кардинальные изменения.

Вопрос о применимости международного гуманитарного права к информационной среде нередко связывается с так называемыми "критическими информационными инфраструктурами". В международном праве не прописан четкий список, какие именно объекты следует относить к таким инфраструктурам. При этом предполагается, что это такие объекты, которые, в случае сбоя в их работе в результате кибератак, могут вызвать серьезные последствия

для соответствующего государства и его населения. Например, это ядерные объекты, система энергоснабжения, банковская сфера. Возможно, успешные кибератаки на такие объекты могут рассматриваться как акты агрессии, как повод на самооборону с использованием вооруженных сил. Одновременно, если в результате таких кибератак пострадает, например, гражданское население, можно будет говорить о применимости международных договоров, составляющих основу современного гуманитарного права. При этом предполагается, что такие кибератаки будут квалифицированы как акт применения оружия, а само противоборство в связи с такими атаками будет квалифицировано как война.

В Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы (утв. Указом Президента РФ от 9 мая 2017 г. № 203) сказано:

"объекты критической информационной инфраструктуры – информационные системы и информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, в сфере здравоохранения, транспорта, связи, в кредитно-финансовой сфере, энергетике, топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленности".

Уже сейчас предпринимаются попытки сформулировать нормы международного права, касающиеся кибератак на объекты критической информационной инфраструктуры. Например, в проекте Конвенции об обеспечении международной информационной безопасности от 22 сентября 2011 г., разработанном Россией, сказано:

"критически важный объект информационной инфраструктуры – часть (элемент) информационной инфраструктуры, воздействие на которую может иметь последствия, непосредственно затрагивающие национальную безопасность, включая безопасность личности, общества и государства".

В том же проекте содержится следующий текст:

"Статья 4. Основные угрозы международному миру и безопасности в информационном пространстве

В качестве основных угроз в информационном пространстве, приводящих к нарушению международного мира и безопасности, рассматриваются следующие:

…….

2) целенаправленное деструктивное воздействие в информационном пространстве на критически важные структуры другого государства".

Нужно также отметить, что в России принят Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации".

8. Терроризм и ИКТ

Терроризм

Термин "терроризм" в наше время очень широко используется как в специальной научной литературе, так и в СМИ. Казалось бы, мы хорошо понимаем, что имеется в виду под этим словом[116]. Более того, "терроризм" используется и в нормативных документах. Например, в Уголовном кодексе России это слово в той или иной форме используется несколько десятков раз. При этом УК РФ дает в ст. 205 "Террористический акт" и определение терроризма:

"Совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями".

В том же нормативном документе используется и термин "террористическое сообщество". Это устойчивая группа лиц, заранее объединившихся в целях осуществления террористической деятельности либо для подготовки или совершения одного либо

[116] *Литвинова Т.Н.* Европейская и российская политики противодействия кибертерроризму (на примере борьбы с "Кибер-джихадом") // Национальная безопасность / nota bene. 2020. № 3. С. 32–47.

нескольких преступлений, предусмотренных статьями 205.1, 205.2, 206, 208, 211, 220, 221, 277, 278, 279, 360 и 361 УК РФ, либо иных преступлений в целях пропаганды, оправдания и поддержки терроризма, а равно руководство таким террористическим сообществом, его частью или входящими в такое сообщество структурными подразделениями.

Уголовный кодекс России оперирует также термином "террористическая организация". Более того, там же, в последней статье УК РФ (ст. 361) дается определение и "акта международного терроризма". Это:

"Совершение вне пределов территории Российской Федерации взрыва, поджога или иных действий, подвергающих опасности жизнь, здоровье, свободу или неприкосновенность граждан Российской Федерации в целях нарушения мирного сосуществования государств и народов либо направленных против интересов Российской Федерации, а также угроза совершения указанных действий".

Казалось бы, определения предельно точны, их использование для пресечения соответствующих неправомерных действий не могут вызывать особых затруднений. Возникает вопрос: если во внутригосударственных нормативных документах можно сформулировать соответствующие понятия, то могут ли возникнуть трудности при заключении международных соглашений, направленных на борьбу с терроризмом, в том числе и в ИКТ? Трудности могут возникнуть[117].

Попробуем разобрать этот вопрос на конкретном примере. Допустим, небольшая группа людей убивает высшее государственное лицо, причем делает это демонстративно, явно выставляя эти действия как акт устрашения и преследуя цель, чтобы в результате убийство вызвало широкий резонанс в СМИ. Это акт терроризма? Вроде бы, именно так. Более того, если для убийства применялось оружие, действие которого предполагает использование искусственного интеллекта, то мы имеем не просто террористический акт, а акт кибертерроризма.

Давайте, однако, немного усложним описанную ситуацию. Допустим, что указанная группа лиц действовала не сама по себе, а получила указание от других лиц. Каких? К примеру, от руководства другого государства. Это уже не терроризм? Но государства бывают

[117] *Хованская Е.В.* Международный терроризм: новые вызовы, старые ответы // Вестник РУДН, сер. Юридические науки. 2001. № 2. С. 89.

разные. А что, если указание было получено от ИГ, то есть государства, признанного террористической организацией? Получается, что тогда все равно описанное убийство – это акт терроризма.

А если это не ИГ, а признанное всеми государство, но государство, приверженное принципам Ислама? Например, Иран? Большой шанс, что и в таком случае описанное убийство будет рассматриваться значительной частью мирового сообщества как акт терроризма. Хотя, скорее всего, возникнет и иная трактовка: такое убийство это не террористический акт, а просто военные действия одного государства против другого, casus belli, причем с использованием кибертехнологий.

А если приказ на убийство отдало руководство вполне светского государства? Тогда, надо полагать, международное сообщество сочтет, что речь идет исключительно о военных действиях, о фактическом объявлении войны.

Итак, как мы видим, непосредственные исполнители во всех этих случаях – одни и те же: небольшая группа лиц использует оружие, основанное на искусственном интеллекте, и убивает высшее должностное лицо какого-то государства. При этом далеко не всегда такие действия можно трактовать как акт терроризма (кибертерроризма). Все зависит от того, кто именно принял решение о совершении убийства. Если это просто самостоятельная группа лиц, то это похоже на терроризм. Если это государство, но его не признают в качестве законного государственного образования, а рассматривают как террористическое, то это тоже акт терроризма. Если государство общепризнано, но придерживается какой-то религиозной идеологии, которую некоторые другие страны рассматривают в качестве экстремистской, то тоже большой шанс, что убийство будет квалифицировано как терроризм.

А если светское государство отдает команду группе лиц убить должностное лицо другого государства, которое придерживается религиозных принципов, признаваемых некоторыми экстремистскими? Тут трактовка будет радикально иной. Скорее всего, такое убийство будет представлено вообще не как акт терроризма, а как акт борьбы с терроризмом.

Наконец, пора описать конкретную историческую ситуацию, которая и послужила основой всех вышеописанных теоретических построений. В начале 2020 года группа американских военных

применила беспилотный летательный аппарат (дрон), действовавший на основе технологий искусственного интеллекта, и убила в аэропорту Ирака Касема Сулеймани – главу крупного иранского военного подразделения, фактически второе лицо в иерархии высших должностных лиц Ирана. Указанная группа лиц действовала по прямому указанию президента США. Эти действия были представлены как акт борьбы с терроризмом, при этом высшие должностные лица США ссылались на то, что хотя Сулеймани и не совершал никаких террористических актов, но мог в будущем сделать нечто подобное.

Как нетрудно заметить, те или иные действия, в том числе демонстративное убийство высшего должностного лица небольшой по численности группой лиц, можно, в зависимости от трактовок, рассматривать как преступный акт терроризма, а также ровно наоборот: как вполне правомерный акт борьбы с терроризмом. Все зависит больше от субъективных толкований, чем от объективных обстоятельств. При этом очевидно, что стороны подобных действий достаточно вольно обращаются с понятием "терроризм", толкуя его в свою пользу в зависимости от политических соображений, нередко сиюминутных.

Так, в начале октября 2014 г. в США была обнародована новая оперативная концепция сухопутных войск США – "Победа в сложном мире. 2020–2040". Впервые в концепции официально признаны сферы войны:

1) традиционные боестолкновения с использованием летального оружия;

2) внутриполитические гражданские конфликты;

3) противоборства в сфере дипломатии;

4) информационные воины;

5) финансово-экономические войны;

6) жесткое технологическое противоборство;

7) поведенческие войны (целенаправленное воздействие на поведение больших групп населения и элитных структур стран – потенциальных источников вероятных угроз).

При этом в концепции выделяют пять полей противоборства: суша, море, воздух, космос и киберпространство[118].

[118] *Григорьев Н.Ю., Родюков Э.Б.* Современный кибернетический терроризм и его социальные последствия // Вестник Университета. 2016. С. 234.

Рассмотрим еще одну ситуацию. Небольшая группа использовала оружие, в том числе тяжелое, пытаясь убить даже не одного, а несколько высших должностных лиц государства. Это покушение на террористический акт? Внешне, вроде бы, именно так. Попробуем, однако, как и в предыдущем примере, постепенно усложнить ситуацию дополнительными обстоятельствами. Известно, что указанная группа лиц действовала по указанию человека, который хотя и был избран президентом, но совершил государственный военный переворот, то есть поставил себя вне закона. При этом он формально был отстранен от должности как решением полномочного суда, так и решением высшего органа государственной власти – парламента.

Итак, с чем мы имеем дело? С террористическим актом или нет? Есть узкая группа лиц, которая применяет оружие, чтобы убить высших должностных лиц государства. Этой группой лиц руководит человек, который объявлен преступником как по решению высшего органа власти страны, так и в судебном порядке. Это теракт или нет? В Российской Федерации описанные действия не трактуются как террористический акт. Речь идет об обстреле из танков парламента страны в 1993 году. Мало того, ни одно из государств мира даже в устном заявлении не осудило указанные действия, не говоря уж о том, чтобы рассматривать их как террористический акт. Хотя речь шла именно о физическом уничтожении узкой группой заговорщиков законно избранных депутатов страны. При этом имелись официальные решения как Конституционного суда страны, так и Съезда народных депутатов. Мало того, рядом с телецентром страны группа снайперов по указанию заговорщиков стреляла в толпу заведомо мирных, невооруженных граждан, убив несколько десятков человек. И эти действия тоже так и не были осуждены ни в каком виде, не говоря уж о том, чтобы трактовать их как акт терроризма.

В вопросе о том, что можно считать актом международного терроризма, а что нет – достаточно много неясностей. Первая неясность – это субъекты террористического акта. Казалось бы, акт терроризма совершает небольшая группа лиц, а то и одиночка, которые преследуют цель запугать остальную часть населения, тем самым навязать им свою волю. Вроде бы, очевидно, что тут нужно ориентироваться на волю абсолютного большинства против воли абсолютного меньшинства. Обратимся к истории России. В марте 1881 года представители достаточно небольшой организации

"Народная воля" убили царя Александра II. То есть убийцы были малочисленны. А какова была воля большинства? Даже в этом примере, который считается классическим для подтверждения, что именно надо понимать под "терроризмом", не все ясно. Какая тут воля большинства? Ведь царя никто не выбирал. Народовольцы, покушаясь на царя, полагали, что они действуют в пользу молчаливого большинства, которое как раз хотело ликвидировать монархию и переустроить государство на основе демократических принципов. Кстати, не исключено, что, действительно, такие настроения были широко распространены в обществе. Но в то время никто никаких опросов населения не проводил и голосование не устраивал, так что мы можем опираться только на свои догадки или предположения.

Обратим внимание, что, например, в уже упомянутом выше нормативном акте (УК РФ) нет ясной трактовки по поводу субъектного состава лиц, совершающих террористический акт. Там нет никаких указаний на малочисленность. С какого момента, с какой численности "организации" или "сообщества" оно перестает быть субъектом терроризма? Это неясно. Более того, в России судебным актом было признано террористическим сообщество (организация), которое было явно достаточно многочисленным и даже претендовало на статус государства, имея его некоторые атрибуты, как то: органы власти, в том числе судебные, верховенство над определенной значительной территорией. Речь идет об ИГ. Возникает вопрос: можно ли считать террористическим даже целое государство? Тогда в чем смысл использования понятия "терроризм"?

Видимо, можно констатировать, что в современных международных отношениях не без оснований имеет место достаточно вольное обращение с понятием "терроризм" или "террористический акт". Наверное, этому есть достаточно убедительное объяснение. По определению как бы следует, что акт терроризма – это нечто особо опасное. Настолько опасное, что с ним можно бороться любыми методами. То есть не исключено существование злоупотреблений, когда со ссылками на угрозу терроризма физически уничтожают каких-то лиц, не прибегая при этом ни к какому публичному разбирательству, включая судебное. Вина убитых террористов не доказывается в соответствии с демократическими процедурами, а как бы презюмируется. В качестве доказательств могут фигурировать, например, сообщения в СМИ, которые в хлесткой форме тенденциозно излагают те или

предположения, выдавая их за установленные факты. В качестве примера можно привести сообщения в СМИ о "фактах" применении властями Сирии химического оружия против мирных граждан. Сообщения базировались на информации, якобы полученной от некоей организации "белых касок". В итоге получалось, что законные власти государства являлись "террористами". Из чего, видимо, следовало, что их можно было уничтожить без суда и следствия, без каких-либо иных доказательств, помимо сообщений в СМИ.

Итак, ссылаясь на "терроризм", можно убить высшее должностное лицо другого государства, при этом выдавая свои действия не за акт агрессии или войны, а как метод борьбы с терроризмом. К сожалению, надо констатировать, что именно такая ситуация и сложилась сейчас в международных отношениях. То есть ссылки на терроризм подчас не имеют ничего общего с настоящей борьбой с терроризмом и служат лишь оправданием неограниченного применения силы в отношении тех или иных лиц или даже государств.

Мало того, современная борьба с терроризмом, в том числе и на международном уровне, нередко имеет оттенок конфликта атеистов или приверженцев одной религии со сторонниками другой религии. Формально это, конечно, всячески отрицается. Но, к сожалению, есть основания и для таких трактовок. Ссылки на терроризм иногда являются прикрытием именно межконфессионального конфликта.

Обратимся к фактам. Нередко террористы – это некто "исламисты". Даже из этого слова следует, что тут существует какая-то связь с Исламом. Термин "исламист" используется достаточно широко в вопросах, касающихся терроризма. Речь идет о лицах, которые придерживаются экстремистских взглядов, совершают акты насилия, в том числе убийства, при этом ссылаются на какие-то принципы и понятия из Ислама. При этом многие лидеры Ислама осуждают их и утверждают, что те не имеют никакого отношения к этой религии. Таких же позиций придерживаются и власти ряда светских государств, а также лидеры других конфессий, в том числе Христианства.

Так идет ли на самом деле в таких случаях речь о конфликте религий между собой или конфликте верующих с атеистами? К сожалению, тут вряд ли можно ответить однозначно. Кто вообще имеет право решать, являются ли "исламисты" представителями Ислама, или они только прикрывают свои преступные действия ссылками на эту религию? Могут ли принять на себя функцию судьи в

этом вопросе представители других религий или тем более светские власти? Это крайне сомнительно. В лучшем случае можно говорить, что какое-то право высказывать суждения тут имеют представители (лидеры) той же религии, то есть Ислама. Но и тут все вовсе не однозначно. Внутри той или иной религии, как правило, всегда есть несколько течений. Более того, вся история человечества полна конфликтами именно внутрирелигиозного порядка. Крупные вооруженные конфликты, целые войны с большим числом жертв возникали именно в результате противоречивых толкований той или иной религии. Как правило, кто побеждал в этой борьбе, тот и объявлял себя единственным правильным толкователем соответствующего религиозного учения.

Иными словами, оценка действий террористов со стороны лидеров соответствующей конфессии – это весомый факт. Но он, к сожалению, не носит абсолютного характера. В лучшем случае он может служить оправданием не ограниченного никакими рамками применения силы против лиц, которые рассматриваются как террористы, но не более того. При этом нужно учитывать, что применение силы без каких либо ограничений, в том числе демократического или гуманитарного характера, – это тоже достаточно сомнительное действие, которое чревато значительными побочными осложнениями. Разрушение правил применения силы в международных отношениях может привести к очень серьезным отрицательным последствиям для всего человечества. Отказываясь придерживаться правил в одном вопросе, рискуешь получить такой же отказ со стороны других участников в иных вопросах.

Терроризм и ИКТ

Вопрос о субъектах террористических атак, в том числе в Интернете, – далеко не праздный и совсем не простой. Выше мы показали, что от субъекта полностью зависит квалификация тех или иных действий именно как теракта (теракта в киберпространстве). Перечислим для примера, как в научной литературе описываются приемы кибертерроризма:

- нанесение ущерба физическим элементам киберпространства;
- кража или уничтожение информационных ресурсов;
- искажение программного обеспечения;
- раскрытие для общего доступа чувствительной информации;

- захват каналов связи и распространение дезинформации;
- уничтожение или подавление линий связи;
- проведение информационно-психологических операций;
- ложная угроза кибератаки;
- воздействие на операторов в киберпространстве[119].

Казалось бы, приемы кибертеррористов описаны содержательно и полно. Не хватает только одного: определения, кого именно надо считать информационным террористом. Это не праздное замечание. Дело в том, что все описанные приемы кибертеррористов вполне широко используются и другими субъектами. Например, все теми же государствами, причем с целью нанести точно такой же ущерб, который обычно пытаются нанести именно террористы в киберпространстве. Однако если подобные действия совершает государство, они, несмотря на полное совпадение с действиями террористов, не будут считаться террористическим актом. Это будут либо элементы информационной войны, либо различные формы вмешательства в дела других государств, либо и вовсе подрывные действия в отношении других стран. Можно даже встретить утверждения, что речь идет не о теракте, а о действиях, направленных на борьбу с терроризмом (например, в случае убийства Сулеймани).

Изложенное означает, что до тех пор, пока не будет выработано общепризнанное определение, кого именно надо считать террористом, международные договоренности будут либо невозможны, либо неэффективны. Если четко не определить понятие "террорист" или "кибертеррорист", то каждая сторона соответствующего международного договора будет толковать норму, направленную на борьбу с кибертерроризмом, по-своему. Понятно, что в таком случае эта норма формально будет существовать, но на практике вряд ли будет эффективно работать.

Можно предположить, что, например, США будут считать террористами как некоторых высших должностных лиц Ирана или Сирии, так и сами эти страны. Не исключено, что в конечном итоге такое же отношение возникнет и к России. Страны, которые придерживаются принципов Ислама, наоборот, будут вряд ли склонны связывать в любом виде акты насилия с этой религией. А Ислам – это

---

[119] *Гаврилин Ю.В., Смирнов Л.В.* Современный терроризм: сущность, типология, проблемы противодействия. М.: ЮИ МВД России, Книжный мир, 2003. С. 37.

примерно четыреста миллионов человек (по некоторым оценкам – даже намного больше). Еще один пример: вооруженные группировки, действующие на территории Сирии. Россия считает значительную их часть террористическими. США, наоборот, склонны относить некоторые из них к так называемой "умеренной оппозиции". Наверное, свои толкования понятия "террорист" и "кибертеррорист" возникнут и у других крупных международных субъектов. Можно ожидать, что Индия сочтет террористами всех приверженцев левой коммунистической идеологии, вне зависимости от их численности. А таких в этой стране очень много, наверное, десятки и сотни тысяч. Китайцы могут записать в террористов всех сторонников независимости Тибета, и подобное отношение наверняка встретит серьезное сопротивление со стороны США.

Возникает также проблема с использованием терминов "информационный терроризм" и "кибертерроризм". Возможно, выход будет найден либо в случае, если эти определения будут признаны тождественными, либо в случае, если понятие "информационный терроризм" будет включать в себя "кибертерроризм", но им не исчерпываться. Вообще, спор вокруг этих понятий во многом связан со спором вокруг понятий "информационная безопасность" и "кибербезопасность"[120].

Определенная теоретическая проблема заключается также в том, как определить понятие "компьютерный терроризм" ("кибертерроризм"), поскольку нелегко установить четкую границу для отличия его от информационной войны и информационного криминала. Еще одна трудность состоит в том, что необходимо выделить специфику именно этой формы терроризма[121].

Что же следует понимать под "кибертерроризмом"? Видимо, это может быть политически мотивированная атака на информацию. Например, речь может идти о непосредственном управлении социумом с помощью устрашения. Речь также может идти об информационной атаке на компьютерную информацию,

---

[120] *Молчанов Н.А., Матевосова Е.К.* Информационный терроризм в международно-правовом контексте // Вестник Университета имени О.Е. Кутафина (МГЮА). 2018. № 5. С. 95–96.

[121] *Григорьев Н.Ю., Родюков Э.Б.* Современный кибернетический терроризм и его социальные последствия // Вестник Университета, 2016. С. 227.

вычислительные системы, аппаратуру передачи данных, иные составляющие информационной инфраструктуры, совершаемой группировками или отдельными лицами. В результате может иметь место проникновение в атакуемую систему, перехват управления или подавление средств сетевого информационного обмена.

Некоторые нормативные документы

Вопросы терроризма применительно к ИКТ неоднократно упоминаются в российских официальных программных документах. Отметим лишь некоторые, наиболее принципиальные формулировки.

В Доктрине информационной безопасности Российской Федерации (утв. Президентом РФ, № Пр-1895 от 9 сентября 2000 г.) содержится следующее положение:

"Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности являются:

……..

— предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми".

В Концепции внешней политики Российской Федерации (утв. Президентом РФ от 12 февраля 2013 г. № Пр-251) сказано:

"Укрепление международной безопасности

32. Россия последовательно выступает за снижение роли фактора силы в международных отношениях при одновременном укреплении стратегической и региональной стабильности. В этих целях Российская Федерация:

<...>

з) будет принимать необходимые меры в интересах обеспечения национальной и международной информационной безопасности, предотвращения угроз политической, экономической и общественной безопасности государства, возникающих в информационном

пространстве, для борьбы с терроризмом и иными криминальными угрозами в сфере применения информационно-коммуникационных технологий, противодействовать их использованию в военно-политических целях, противоречащих международному праву, включая действия, направленные на вмешательство во внутренние дела, а также представляющие угрозу международному миру, безопасности и стабильности".

В Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ от 24 июля 2013 г. № Пр-1753) содержатся следующие формулировки:

"8. Основной угрозой в области международной информационной безопасности является использование информационных и коммуникационных технологий:

…….

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников".

В том же документе сказано:

"13. Основными направлениями государственной политики Российской Федерации, связанной с решением задачи по формированию механизмов международного сотрудничества в области противодействия угрозам использования информационных и коммуникационных технологий в террористических целях, являются:

а) развитие сотрудничества с государствами – членами Шанхайской организации сотрудничества, государствами – участниками Содружества Независимых Государств, государствами – членами Организации Договора о коллективной безопасности, государствами – участниками БРИКС, способствующего предупреждению, выявлению, пресечению, раскрытию и расследованию актов деструктивного воздействия на элементы национальной критической информационной инфраструктуры, минимизации последствий реализации таких актов, а также противодействию использования информационно-телекоммуникационной сети Интернет и других информационно-телекоммуникационных сетей в целях пропаганды терроризма и привлечения к террористической деятельности новых сторонников".

Нужно упомянуть, как регулируются вопросы борьбы с терроризмом во внутренних документах КНР. В 2011 году в Китае был принят Закон "О противодействии терроризму", заменивший Постановление ВСНП "О соответствующих вопросах усиления работы по борьбе с терроризмом" 2011 г. Закон определяет терроризм как убеждения и действия, создающие панические настроения в обществе, направленные против общественной безопасности, посягающие на личное имущество или угрожающие государственным органам и международным организациям, направленные на реализацию собственных политических и идеологических целей через применение методов насилия, разрушения и запугивания.

В ч. 2 ст. 3 указанного Закона террористическая деятельность определяется как деяния, направленные на организацию, планирование, подготовку к осуществлению, осуществление или намерение осуществления деятельности, влекущей за собой серьезное посягательство на общество в виде гибели людей, нанесения значительного вреда имуществу, разрушения социальной инфраструктуры, приведения в хаос социального порядка; пропаганда терроризма, провоцирование к осуществлению террористической деятельности либо незаконное обладание продукцией, пропагандирующей терроризм, принуждение к ношению в общественных местах одежды, символики, пропагандирующих терроризм; организация, руководство, участие в террористической организации; предоставление информации, финансирования, материальных ресурсов, услуг, технической поддержки, мест и другой поддержки, помощи, преференций для террористических организаций, террористов, осуществляемой террористической деятельности или обучения террористической деятельности; иная террористическая деятельность[122].

Во многих ныне действующих двусторонних или многосторонних международных соглашениях, касающихся вопросов информационной безопасности (безопасности киберпространства), в той или иной мере затрагивается вопрос о борьбе с кибертерроризмом.

---

[122] *Зверянская Л.П.* Организационно-правовое обеспечение международной и национальной информационной безопасности: опыт Китайской Народной Республики // Труды Института государства и права РАН. 2017. Т. 12. № 5. С. 204.

Однако до сих пор не выработано международное соглашение, участниками которого являлись бы основные государства (в первую очередь Россия, Китай, Индия, США, ЕС), в котором содержались бы общеприемлемые нормы международного права, которые регулируют проблемы борьбы с терроризмом в киберпространстве. Такие универсальные нормы еще предстоит разработать. Возможно, это будет самостоятельное соглашение, а скорее всего, часть более общего международного договора, в целом посвященного информационной безопасности. Отметим при этом, что в Конвенции о компьютерных преступлениях (Будапешт, 23 ноября 2001 г.) терроризм никак не упоминается.

Пока нормы, касающиеся кибертерроризма, содержатся лишь в региональных или двусторонних соглашениях. Среди них следует обратить особое внимание на Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности 2009 года. Участниками его являются, в том числе, Россия и Китай – две страны, играющие значительную роль в определении общемировых направлений регулирования вопросов безопасности в киберпространстве.

Указанное Соглашение ШОС 2009 года среди основных угроз в области обеспечения международной информационной безопасности упоминает и информационный терроризм:

"Статья 2. Основные угрозы в области обеспечения международной информационной безопасности

Реализуя сотрудничество в соответствии с настоящим Соглашением, Стороны исходят из наличия следующих основных угроз в области обеспечения международной информационной безопасности:

---

2) информационный терроризм".

В Приложении 1 к указанному Соглашению в "Перечне основных понятий в области обеспечения международной информационной безопасности" упомянут и информационный терроризм:

"информационный терроризм" — использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях".

В Приложении 2 среди "Перечня основных видов угроз в области международной информационной безопасности, их источников и

признаков" дается и развернутое определение, что именно понимается под информационным терроризмом:

"2. Информационный терроризм.

Источником этой угрозы являются террористические организации и лица, причастные к террористической деятельности, осуществляющие противоправные действия посредством или в отношении информационных ресурсов.

Ее признаками являются использование информационных сетей террористическими организациями для осуществления террористической деятельности и привлечения в свои ряды новых сторонников; деструктивное воздействие на информационные ресурсы, приводящее к нарушению общественного порядка; контролирование или блокирование каналов передачи массовой информации; использование сети Интернет или других информационных сетей для пропаганды терроризма, создания атмосферы страха и паники в обществе, а также иные негативные воздействия на информационные ресурсы".

В этом же Соглашении, в том же Приложении 2 в п. 5 "Распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств" также упомянут терроризм. Речь идет о таком признаке указанной информации, как пропаганда идей терроризма.

Нужно также упомянуть, в преамбуле указанного Соглашения ШОС 2009 года указано, что "Государства-члены будут… пресекать пропаганду идей терроризма… с использованием глобальной сети Интернет".

В Конвенции об обеспечении международной информационной безопасности (Концепция) от 22 сентября 2011 г. содержится следующее определение:

"терроризм в информационном пространстве" — использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях.

В Соглашении о сотрудничестве государств–участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г. содержатся следующие положения:

"информационный терроризм — использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях".

"Статья 2. Основные угрозы в области обеспечения международной информационной безопасности

Реализуя сотрудничество в соответствии с настоящим Соглашением, Стороны исходят из наличия следующих основных угроз в области обеспечения международной информационной безопасности:

…….

2) информационный терроризм".

В Соглашении между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности от 11 июля 2014 г. содержатся следующие положения:

"2. Информационный терроризм.

Источник угрозы — террористические организации и лица, причастные к террористической деятельности, осуществляющие противоправные действия посредством или в отношении информационных ресурсов.

Признаки угрозы — использование информационных сетей террористическими организациями для осуществления террористической деятельности и привлечения в свои ряды новых сторонников; деструктивное воздействие на информационные ресурсы, приводящее к нарушению общественного порядка; контролирование или блокирование каналов передачи массовой информации; использование сети Интернет или других информационных сетей для пропаганды терроризма, создания атмосферы страха и паники в обществе; иное негативное воздействие на информационные ресурсы".

"5. Распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

Источники угрозы — государства, организации, группа лиц или частные лица, использующие информационную инфраструктуру для распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

Признаки угрозы — появление и тиражирование в электронных (радио и телевидение) и прочих средствах массовой информации, в сети Интернет и других сетях информационного обмена информации:

— искажающей представление о политической системе, общественном строе, внешней и внутренней политике, важных политических и общественных процессах в государстве, духовных, нравственных и культурных ценностях его населения;

— пропагандирующей идеи терроризма, сепаратизма и экстремизма".

В Соглашении между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г. сказано, в частности, следующее:

"Статья 2. Основные угрозы в области обеспечения международной информационной безопасности

При осуществлении сотрудничества в соответствии с настоящим Соглашением Стороны исходят из того, что основными угрозами международной информационной безопасности является использование информационно-коммуникационных технологий:

…….

3) в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников".

9. Незаконный оборот наркотиков и ИКТ

Конечно, с формальной точки зрения незаконные действия в отношении наркотиков – это всего лишь один из видов уголовных преступлений. Однако понятно, что изготовление, распространение, иные манипуляции с наркотиками – особо опасное преступление. Надо полагать, что в будущей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях это преступление будет отдельно подробно упомянуто. При этом не исключено, что согласование соответствующих формулировок не будет легким, поскольку у государств – разработчиков указанной конвенции, скорее всего, будут относительно различные позиции, как именно следует сформулировать состав этого преступления, а также соответствующие процессуальные действия. В этом связи следует, например, учитывать,

что даже в рамках ОДКБ позиция государств-членов в отношении наркоугроз не совсем идентичная[123].

Например, в постановлении № 2 совместного заседания членов Совета Межпарламентской Ассамблеи государств СНГ – членов ОДКБ и Комитета секретарей советов безопасности государств – членов ОДКБ от 16 апреля 2004 года прямо указывается, что ключевой проблемой в области законодательного контроля над наркотиками в государствах – членах ОДКБ оказывается путаница в терминах и основных моментах нормативно-правового регулирования оборота и противодействия незаконному обороту наркотических средств, психотропных веществ и прекурсоров.

Нужно отметить, что различия в позиции в отношении преступлений, связанных с наркотиками, существуют и в целом в международном сообществе, причем подчас эти различия носят принципиальный характер. Например, Россия и США по-разному относятся к вопросу о борьбе с наркоторговлей, в частности, применительно к Афганистану. США считают основным приоритетом борьбу с терроризмом, поэтому если будет вестись активная работа по уничтожению посевов опиумного мака, то это, по мнению американцев, вызовет приток новых членов в ряды террористов[124].

Что же касается России, то, например, в Стратегии государственной антинаркотической политики РФ до 2020 г., вступившей в силу 9 июня 2010 г., прямо говорится о том, что "ключевым фактором негативного развития наркоситуации в Российской Федерации является масштабное производство опиатов на территории Афганистана и их последующий транснациональный трафик на территорию России".

Отметим, что в проекте Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности от 11 октября 2017 г. (A/C.3/72/12), предложенном Россией, в статье 58 "Общие принципы технической помощи" содержится следующее положение:

"5. Государства-участники поручают Управлению Организации Объединенных Наций по наркотикам и преступности оказывать

---

[123] *Струговец В.* Перспективные направления информационной политики ОДКБ // Власть. 2011. № 8. С. 96.

[124] *Зия Сайед Ахмад.* Взаимодействие России с США и НАТО в борьбе с наркоугрозой в Афганистане // Постсоветские исследования. Т. 1. № 1. (2018). С. 50.

Государствам-участникам профильную техническую помощь в целях содействия реализации программ и проектов по борьбе с преступлениями в сфере ИКТ".

В том же проекте в статье 59 "Подготовка кадров" сказано:

"2. Государства-участники поручают Управлению Организации Объединенных Наций по наркотикам и преступности оказывать Государствам-участникам профильную помощь в подготовке кадров в целях содействия реализации национальных программ и проектов по борьбе с преступлениями ИКТ".

В Приложении 2 к Соглашению между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, озаглавленном "Перечень основных видов угроз в области международной информационной безопасности, их источников и признаков", содержится следующий текст:

"3. Информационная преступность.

Источником этой угрозы являются лица или организации, осуществляющие неправомерное использование информационных ресурсов или несанкционированное вмешательство в такие ресурсы в преступных целях.

Ее признаками являются проникновение в информационные системы для нарушения целостности, доступности и конфиденциальности информации; умышленное изготовление и распространение компьютерных вирусов и других вредоносных программ; осуществление DOS-атак (отказ в обслуживании) и иных негативных воздействий; причинение ущерба информационным ресурсам; нарушение законных прав и свобод граждан в информационной сфере, в том числе права интеллектуальной собственности и неприкосновенности частной жизни; использование информационных ресурсов и методов для совершения таких преступлений, как мошенничество, хищение, вымогательство, контрабанда, незаконная торговля наркотиками, распространение детской порнографии и т.д.".

Необходимость борьбы с наркопреступлениями, совершенными с использованием ИКТ, отдельно оговорена и в других международных документах.

10. Будущий международный суд по информационной безопасности и некоторые формулировки для использования в будущей конвенции о противодействии использованию ИКТ в преступных целях

Количество уголовных преступлений в сфере высоких технологий, в том числе и информационных, год от года, к сожалению, неуклонно возрастает. Это, в частности, касается краж финансовой и коммерческой информации, похищений персональных данных, мошенничества с использованием сети Интернет и других видов преступлений. Нападениям подвергаются автоматизированные системы управления, информационные базы данных, электронные платежные системы, а также информационно-коммуникационные системы.

При этом пока нет окончательного ответа даже на вопрос, как правильно квалифицировать природу самого Интернета, является ли он субъектом права, вступающим в правовые отношения со своими пользователями, или объектом взаимоотношений, осуществляющихся в киберпространстве[125].

Обеспечение международной информационной безопасности, несомненно, приведет к конфликтам различных интересов. Существуют различные способы разрешения таких конфликтов: переговоры, как прямые, так и через посредников; преследование преступников с использованием национального законодательства и национальных средств защиты интересов; разрешение конфликта интересов путем применения силовых методов; международные судебные процедуры и др.

Рассмотрим тут только вариант разрешения спорной (конфликтной) ситуации с использованием судебного разбирательства на международном уровне. Уже создано и работает немало международных судебных органов. Можно упомянуть Международный суд в Гааге, Европейский суд по правам человека, Международный трибунал по морскому праву в Гамбурге, Международный уголовный суд. Их практика, к сожалению,

[125] *Бецков А.В., Северцев Н.А.* О некоторых аспектах правового понятия "информационная безопасность" // Труды международного симпозиума "Надежность и качество". 2018. Т. 2. С. 261.

неоднозначна: нередко можно услышать жалобы, что какой-то международный судебный орган вышел на пределы своей компетенции. Подчас отдельные государства решительно отказываются участвовать в том или ином судебном органе, ссылаясь на то, что, по их мнению, он может необоснованно привлекать к ответственности как граждан и организации такого государства, так и само это государство. Еще чаще участники судебного разбирательства на международном уровне недовольны вынесенным решением.

Как сложится конкретная ситуация с созданием международного суда по информационной безопасности, пока трудно сказать. Велика вероятность, что те государства, в частности, США и их союзники, которые не поддержали резолюцию ГА ООН A/RES/74/247 от 27 декабря 2019 года о разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, не будут участвовать в создании соответствующего международного судебного органа, а если он все-таки будет создан, не признают его компетенцию. Тем не менее, рассмотрим, какие в принципе существуют варианты такого суда и возможности для его учреждения.

Суд может иметь как сложную форму, так и простейшую. Например, Международный трибунал по морскому праву – это судебный орган с весьма подробно разработанной процедурой, он имеет свою штаб-квартиру со значительным количеством судей и сотрудников. Государства-участники вносят значительные средства в его бюджет. Этот суд был создан в связи с разработкой и принятием Конвенции ООН по морскому праву 1982 года, в которой участвуют многие страны мира. Ясно, что в таком судебном органе существует значительная практическая потребность. Нередки споры между государствами о размежевании морских пространств. Довольно широко распространена практика ареста судов, которые, по мнению прибрежного государства, нарушили его интересы в прибрежной экономической зоне. Международный трибунал по морскому праву рассматривает такие спорные ситуации, в том числе и с применением упрощенных процедур.

На данном этапе вряд ли существует практическая возможность в разработке и создании такого же полноценного и всеобъемлющего суда по рассмотрению споров о нарушении интересов того или иного государства или физических или юридических лиц в связи с использованием информационных технологий в преступных целях.

Для его создания потребуются значительные усилия экспертов, согласование нередко конфликтных интересов различных государств, наконец, затраты значительных финансовых ресурсов. Вряд ли можно ожидать, что государства-разработчики указанной выше конвенции пойдут на такие усилия, не будучи уверены, что созданный судебный орган будет пользоваться более или менее всеобщим признанием.

Но это не означает, что вопрос о создании судебного органа, рассматривающего споры, связанные с использованием информационного пространства, вообще не стоит в повестке дня. Возможны такие варианты создания подобного суда, которые не повлекут ни значительных усилий в рамках переговорного процесса, ни существенных финансовых затрат. При этом если суд будет создан и сможет работать, практика рассмотрения споров может сыграть значительную положительную роль для учреждения в дальнейшем полноценного судебного органа.

Международно-правовой порядок решения многих вопросов, связанных с борьбой с киберпреступностью, был сформулирован Россией в ее проекте Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности от 11 октября 2017 г. (A/C.3/72/12). Некоторые положения и процедуры могут быть использованы и при создании соответствующего международного судебного органа. Далее в данном разделе в соответствующих случаях будут приведены такие формулировки.

Варианты места совершения киберпреступлений и соответствующие процессуальные действия

Если кратко, то процедура привлечения к ответственности физических лиц за преступления в области информационно-коммуникационных технологий будет различной в зависимости от того, где именно находится киберпреступник и в отношении какого государства или каких физических или юридических лиц он совершает преступление. Рассмотрим разные варианты.

Вариант 1. Киберпреступник находится в государстве А и совершает преступление в отношении именно этого государства, его граждан или организаций. В таком случае государство А в соответствии со своим уголовным и уголовно-процессуальным законодательством выявляет преступника, совершает в отношении него в полном объеме все предусмотренные законом следственные

действия, передает дело в суд. Суд выносит соответствующее решение (приговор), преступник отбывает наказание в государстве А. В общем случае никакое международное сотрудничество при этом варианте не нужно. Но тут тоже могут быть исключения, связанные с наличием имущества у преступника за пределами территории государства А. Рассмотрим такие исключения чуть ниже.

Вариант 2. Киберпреступник находится в государстве А, но совершает преступление в отношении государства Б, его граждан или организаций. Тут возможны различные действия государства А. Если в соответствии с внутренним законодательством невозможна выдача такого преступника (ст. 13 УК РФ "Выдача лиц, совершивших преступление": "Граждане Российской Федерации, совершившие преступление на территории иностранного государства, не подлежат выдаче этому государству"), то государство А в соответствии с международными процедурами должно обеспечить задержание преступника, провести следственные действия и привлечь преступника к ответственности в соответствии с собственным национальным законодательством, которое должно содержать специальную норму. Согласно этой норме граждане государства А будут привлекаться к уголовной ответственности на территории государства А за преступления, совершенные в отношении государства Б, его организаций и граждан. Как правило, в национальном уголовном законодательстве предполагается, что преступник должен был совершить преступление либо против собственного государства, его организаций или граждан, либо должен был совершить преступление на территории этого государства. Но такой нормы не всегда будет достаточно, чтобы привлекать к ответственности лицо, находящееся на территории данного государства, но нанесшее ущерб интересам другой страны или ее граждан, причем если ущерб нанесен именно на территории другой страны. Не исключено, что тут понадобится новая норма со ссылкой на международные обязательства (например, на норму будущей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях).

В российском проекте Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности от 11 октября 2017 г. (A/C.3/72/12) содержится следующее положение:

"Статья 5. Установление ответственности

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния, согласно его внутреннему законодательству, деяний, предусмотренных статьями 6–12, 15, 18 и 19 настоящей Конвенции, применяя при этом такие уголовные и иные санкции, включая лишение свободы, которые учитывают степень общественной опасности конкретного деяния и размер причиненного ущерба.

2. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, деяний, предусмотренных статьями 13, 14, 16 и 17 настоящей Конвенции.

3. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления, согласно его внутреннему законодательству, деяний, предусмотренных статьями 6, 8, 9, 10 и 15 настоящей Конвенции, если они совершены в отношении устройств ИКТ объектов критической инфраструктуры.

4. Каждое Государство-участник обеспечивает применение в отношении юридических лиц, привлекаемых к ответственности в соответствии со статьей 20 настоящей Конвенции, эффективных, соразмерных и оказывающих сдерживающее воздействие санкций, включая финансовые.

5. Без ущерба для норм общего международного права настоящая Конвенция не исключает возможность осуществления любой уголовной юрисдикции, установленной Государством-участником в соответствии с его внутренним законодательством".

В том же проекте есть статья 48 "Выдача", подробно регламентирующая вопросы, связанные с выдачей преступника.

Итак, важный вопрос – это место совершения киберпреступления (локализация). Обычно при совершении уголовного преступления преступник находится именно там, где совершает преступное деяние. При этом в другом месте может находиться организатор, заказчик преступления, некоторые другие лица. Что же касается киберпреступности, то тут ситуация нередко как раз иная: преступник находится в одном месте, при этом, используя кибертехнологии, наносит ущерб государству, его организациям и гражданам, находящимся в другом месте, подчас за многие тысячи километров от него. Более того, ясно, что будущая международная конвенция о

противодействии использованию информационно-коммуникационных технологий в преступных целях будет касаться именно случаев, когда киберпреступление носит международный характер, то есть преступник находится на территории одного государства и при этом наносит ущерб интересам другого государства, его организаций или граждан. Таким образом, местом совершения преступных действий является одновременно территория двух или более государств, что будет создавать определенные сложности с определением подсудности.

В некоторых случаях действия преступника будут предварительно расследоваться и рассматриваться судом по месту физического нахождения указанного лица (например, в отношении российских граждан, которые не могут быть выданы в соответствии с требованиями Конституции РФ). В других случаях, когда выдача возможна, место судебного разбирательства будет, скорее всего, определяться по договоренности соответствующих государств. Почему по договоренности? Не логичней ли было бы всегда выдавать предполагаемого преступника государству, которому он нанес ущерб? Если национальное законодательство предусматривает возможность выдачи другому государству преступника, совершившего преступление в отношении этого другого государства, то в таком случае применяется обычная, как правило, подробно отработанная процедура выдачи преступника. Тем не менее применительно к киберпреступлениям в некоторых случаях это будет нецелесообразно. Приведем следующий пример: иностранный гражданин с территории РФ совершает киберпреступление в отношении другого государства, его организаций или граждан. При этом может возникнуть вопрос не только об уголовном наказании, но и о компенсации ущерба в рамках гражданских правоотношений. Если у такого преступника имущество находится именно на территории РФ, целесообразно проводить судебное разбирательство именно тут, поскольку в таком случае намного проще будет обратить взыскание на такое имущество. Все будет зависеть от пострадавшей стороны: будет ли она заинтересована в первую очередь в уголовном наказании преступника или в компенсации нанесенного ущерба и возвращении украденного имущества (в том числе денежных средств).

В случае совершения киберпреступления с территории государства А в отношении государства Б, его организаций или граждан, возникает еще один вопрос: будет ли наказан преступник по законам

такого государства Б или по нормам, содержащимся в международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях? Дело в том, что в рамках указанной конвенции возможно создание международного судебного органа. Если так, то не исключено, что предполагаемый преступник будет выдаваться не государству, в отношении которого было совершено преступление, а такому международному суду. Конечно, применение такой процедуры потребует предварительной выработки соответствующих международно-правовых процессуальных норм.

Существенно, что в российском проекте Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности от 11 октября 2017 г. (A/C.3/72/12) содержится статья 43 "Юрисдикция", в которой содержатся формулировки, которые могут оказаться полезными при решении вопросов, связанных с определением юрисдикции и применимых процедур.

Отметим также, что в российском УК РФ есть ст. 11 "Действие уголовного закона в отношении лиц, совершивших преступление на территории Российской Федерации". В УК РФ также содержится ст. 12 "Действие уголовного закона в отношении лиц, совершивших преступление вне пределов Российской Федерации". В указанной статье следует упомянуть часть 3:

"Иностранные граждане и лица без гражданства, не проживающие постоянно в Российской Федерации, совершившие преступление вне пределов Российской Федерации, подлежат уголовной ответственности по настоящему Кодексу в случаях, если преступление направлено против интересов Российской Федерации либо гражданина Российской Федерации или постоянно проживающего в Российской Федерации лица без гражданства, а также в случаях, предусмотренных международным договором Российской Федерации или иным документом международного характера, содержащим обязательства, признаваемые Российской Федерацией, в сфере отношений, регулируемых настоящим Кодексом, если иностранные граждане и лица без гражданства, не проживающие постоянно в Российской Федерации, не были осуждены в иностранном государстве и привлекаются к уголовной ответственности на территории Российской Федерации".

Нужно также обратить внимание на ст. 13 УК РФ "Выдача лиц, совершивших преступление".

"1. Граждане Российской Федерации, совершившие преступление на территории иностранного государства, не подлежат выдаче этому государству.

2. Иностранные граждане и лица без гражданства, совершившие преступление вне пределов Российской Федерации и находящиеся на территории Российской Федерации, могут быть выданы иностранному государству для привлечения к уголовной ответственности или отбывания наказания в соответствии с международным договором Российской Федерации".

Что касается УПК РФ, то там предусмотрена ст. 32 "Территориальная подсудность уголовного дела", в которой содержится общая норма, согласно которой уголовное дело подлежит рассмотрению в суде по месту совершения преступления, за исключением некоторых случаев.

Вариант 3. Киберпреступник находится в государстве Б, но совершает преступление в отношении государства А, его граждан или организаций. То есть речь, по сути, идет о ситуации, предусмотренной вариантом 2, однако рассмотренной со стороны не государства, где находится киберпреступник, а государства, которому был нанесен ущерб. Применительно к Российской Федерации эта ситуация будет выглядеть следующим образом: преступник совершает киберпреступление, факт преступления устанавливается по заявлению потерпевших или иным образом, предусмотренным УПК РФ. Заводится уголовное дело. Далее, в отличие от обычного порядка расследования уголовных дел, надо будет решать, каковы интересы потерпевшей стороны и российского государства в целом. Можно требовать выдачи преступника, расследования его преступных действий в соответствии с УПК РФ, привлечения его к ответственности и применения наказания. При этом в рамках уголовного дела могут быть предъявлены и гражданско-правовые требования. Тогда для их удовлетворения придется применять процедуры исполнения решения суда на территории другого государства, предусмотренные российским гражданским и гражданско-правовым законодательством. Но всегда ли это будет оправдано? Например, ясно, что в отношении имущества преступника чрезвычайно важно принятие мер обеспечения иска, то есть наложение ареста на имущество предполагаемого преступника, чтобы он не имел возможности воспрепятствовать наложению взыскания на такое имущество. Если идти обычным путем, предусмотренным

российским законодательством, то потребуется сначала передать уголовное дело в суд, потом предъявить гражданский иск в рамках уголовного дела. Потом суд вынесет определение о применении мер обеспечения иска. Это определение будет передано в государство, где находится имущество преступника, и в случае, если все процедуры соблюдены должным образом, на имущество будет наложен арест. Возможен и более простой вариант: наложение ареста на имущество в рамках предварительного следствия. Но в любом случае ясно, что все эти действия потребуют определенного, возможно, значительного времени. Преступник будет иметь хорошую возможность вывести имущество из-под мер взыскания.

Намного рациональнее было бы использование процедур, когда государство, где расположено имущество предполагаемого преступника, само применяет меры обеспечения иска. Видимо, для этого в рамках международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях целесообразно предусмотреть процессуальную норму, когда меры по обеспечению иска могут быть применены просто по заявлению государства, где был нанесен ущерб. Иными словами, речь идет о выработке международной нормы упрощенного порядка применения мер обеспечения иска по гражданско-правовым требованиям.

В российском проекте Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности от 11 октября 2017 г. (A/C.3/72/12) содержится следующий текст:

"Статья 4. Термины и определения

Для целей настоящей Конвенции:

а) "арест имущества" означает временное запрещение передачи, преобразования, отчуждения или передвижения имущества, или временное вступление во владение таким имуществом, или временное осуществление контроля над ним по постановлению суда или другого компетентного органа".

В том же проекте записано следующее:

"Статья 32. Механизмы изъятия имущества посредством международного сотрудничества в деле конфискации.

1. Каждое Государство-участник в целях предоставления взаимной правовой помощи в отношении имущества, приобретенного в результате совершения какого-либо из преступлений, признанных таковыми в соответствии с настоящей Конвенцией, или средств

совершения таких преступлений, в соответствии со своим внутренним законодательством:

a) принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам приводить в исполнение постановления о конфискации, вынесенные судами другого Государства-участника;

b) в пределах своей юрисдикции принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам конфисковывать имущество иностранного происхождения по судебному решению в связи с легализацией доходов, полученных в результате совершения преступлений, признаваемых таковыми в соответствии с положениями настоящей Конвенции;

c) рассматривает вопрос о принятии таких мер, какие могут потребоваться, с тем чтобы создать возможность для конфискации такого имущества без вынесения приговора в рамках уголовного производства по делам, когда преступник не может быть подвергнут преследованию по причине смерти, укрывательства или отсутствия или в других соответствующих случаях.

2. Каждое Государство-участник в целях предоставления взаимной правовой помощи по просьбе другого Государства-участника, в соответствии со своим внутренним законодательством:

a) принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам налагать арест на имущество согласно постановлению об аресте, которое вынесено судом или компетентным органом запрашивающего Государства-участника и в котором излагаются разумные основания, позволяющие запрашиваемому Государству-участнику полагать, что существуют достаточные мотивы для принятия таких мер и что в отношении этого имущества будет в конечном итоге вынесено постановление о конфискации для целей пункта 1(a) настоящей статьи;

b) принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам налагать арест на имущество по просьбе, в которой излагаются разумные основания, позволяющие запрашиваемому Государству-участнику полагать, что существуют достаточные мотивы для принятия таких мер и что в отношении этого имущества будет в конечном итоге вынесено постановление о конфискации для целей пункта 1(a) настоящей статьи;

c) рассматривает вопрос о принятии дополнительных мер, с тем чтобы позволить своим компетентным органам сохранять имущество

для целей конфискации, например, на основании иностранного постановления об аресте или предъявления уголовного обвинения в связи с приобретением подобного имущества".

Ясно, что имущественные вопросы не будут сводиться только к имущественной ответственности преступника. Важный вопрос – это возврат имущества, изъятого преступником. Нужно отметить, что этот вопрос достаточно подробно урегулирован в российском проекте Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности от 11 октября 2017 г. (A/C.3/72/12), в частности, в Разделе 3 "Меры по возращению имущества".

Совсем не очевидно, что для Российской Федерации всегда выгоднее рассматривать уголовное дело в отношении киберпреступника, находящегося на территории другого государства, только в своих собственных следственных и судебных органах. Ведь это потребует дополнительных финансовых затрат, загрузит следственные органы и суды дополнительной работой. А также потребует дополнительных финансовых и организационных затрат на содержание преступника в местах лишения свободы. Если нет сомнений в объективности иностранных следственных или судебных органов, если законодательство другого государства достаточно строгое по отношению к киберпреступнику, наверное, имеет смысл не настаивать на его выдаче.

Однако какова будет конкретная процедура рассмотрения заявления о мерах обеспечения иска и применение самих этих мер? Попробуем определить последовательность и содержание тех или иных действий. Рассмотрим эту процедуру на примере РФ. Итак, Российская Федерация устанавливает факт совершения предполагаемого преступления и предполагаемый размер нанесенного гражданско-правого ущерба. Возбуждается уголовное дело по указанному факту. Проводятся следственные действия по установлению личности предполагаемого преступника и установлению места его нахождения. Предпринимаются действия по установлению наличия у указанного лица какого-то имущества. Далее следователь в рамках уголовного дела по заявлению заинтересованных лиц выносит определение о необходимости установления имущества предполагаемого преступника и применения мер обеспечения (ст. 115 УПК РФ "Наложение ареста на имущество").

Иной вариант – это обращение заинтересованного российского лица непосредственно в суд общей юрисдикции или арбитражный суд

с требованием о возмещении ущерба и принятием этим судом мер по обеспечению иска. В таком случае суд вынесет соответствующее определение о мерах по обеспечению иска. Однако надо иметь в виду, что суд общей юрисдикции или арбитражный суд приостановит рассмотрение иска до окончания рассмотрения судебными органами уголовного дела.

Возможно одновременное существование двух возможностей для лица, потерпевшего ущерб: действовать в рамках уголовного дела или через суд посредством предъявления гражданско-правого иска.

Далее определение следователя или определение суда в упрощенном порядке направляется непосредственно либо в международную организацию, созданную в рамках конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, либо в международный суд, если он будет учрежден, либо в государство, где предположительно находится имущество киберпреступника.

Международная организация, получив такой документ, может обратиться ко всем государствам-членам с требованием (просьбой) установить наличие имущества предполагаемого киберпреступника и применить в его отношении меры обеспечения гражданско-правового иска.

Не исключено, что эта процедура будет несколько иной: в международную организацию будет направлена просьба об оказании помощи в установлении личности преступника, в установлении имеющегося у него имущества и о применении мер обеспечения иска. Тогда международная организация, в зависимости от обстоятельств дела, обратится либо ко всем государствам-членам, либо только к государству, где находится предполагаемый киберпреступник, с требованием помочь окончательно установить его личность, установить его имущество и применить к имуществу меры по обеспечению иска.

В российском проекте Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности от 11 октября 2017 г. (A/C.3/72/12) содержится статья 42 "Общие принципы взаимной правой помощи". Там же имеется статья 45 "Процедуры направления запросов о взаимной помощи в отсутствие применимых международных соглашений".

Если в рамках международной конвенции о противодействии использованию информационно-коммуникационных технологий в

преступных целях будет создана не только международная организация, но и международный суд, все вышеперечисленные обращения будут, скорее всего, направляться для исполнения именно непосредственно в такой суд и только для сведения – в международную организацию.

Еще один вариант: направление указанных определений следователя или российского суда непосредственно в страну, где предположительно находится киберпреступник. Если будущая конвенция о противодействии использованию информационно-коммуникационных технологий в преступных целях будет предусматривать упрощенную процедуру рассмотрения таких определений государством-участником, это существенно повысит эффективность борьбы с киберпреступностью.

Отметим, что в российском законодательстве предусмотрена следующая норма: ст. 12 УК РФ "Действие уголовного закона в отношении лиц, совершивших преступление вне пределов Российской Федерации". Но, скорее всего, ее будет целесообразно уточнить в связи с принятием всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Итак, можно подвести определенный итог: государство устанавливает факт совершения киберпреступления. При этом речь идет либо о преступлении, совершенном за пределами территории этого государства, но наносящего ущерб интересам государства или его организаций или граждан, либо о преступлении, совершенном в пределах территории этого государства, но против интересов другой страны. Если преступление совершено, например, на территории РФ и направлено на нанесение ущерба его интересам, то не обязательно (но иногда все-таки целесообразно) привлекать международные организации. Для наказания преступника вполне хватит норм УК РФ и УПК РФ.

Итак, факт преступления выявлен. Заведено уголовное дело. Но вряд ли будет возможно проводить обычное досудебное расследование этого преступления. Если предполагаемый преступник находится за пределами государственной территории, его вряд ли можно будет допросить, провести какие-то процессуальные действия, предполагающие личное присутствие такого лица. Если преступник находится в пределах территории государства, которое выявило преступление, но это преступление направлено против другого

государства или его граждан, также вряд ли можно будет проводить процессуальные действия с участием такого подозреваемого. Ведь для проведения процессуальных действий необходим факт нарушения нормы национального УК. Но это предполагает нанесение ущерба интересам именно этого государства или его граждан, а не другой страны. Вряд ли возможна норма в уголовном кодексе, которая предусматривает уголовную ответственность лица за нанесение ущерба какому-то другому государству. Именно потерпевшая сторона должна проявить интерес в расследовании преступления или наказании преступника, а не какие-то иные субъекты права, чьи интересы никак не затронуты и не ущемлены.

Видимо, в рамках такого ограниченного предварительного расследования можно будет провести какие-то экспертизы, способные уточнить детали выявленного преступления, собрать документы, имеющие отношение к преступлению и способные помочь доказыванию факта преступления.

Дальше государство должно передать заявление с изложением выявленных фактов. Куда именно? Либо в международную организацию, либо в государство, где предположительно находится преступник, либо в государство, где предположительно находится имущество преступника. Или, наконец, в международный суд, если он будет создан. Именно суд в таком случае будет проводить полноценное расследование с участием подозреваемого (обвиняемого). Не исключено, что в таком заявлении будет описан только факт совершения преступления, но не назван конкретный преступник. Однако если личность преступника будет устанавливать суд, в заявлении государства должна содержаться какая-то более или менее определенная информация о предполагаемом преступнике, на основе которой суд будет рассылать запросы и пытаться установить личность преступника.

Отметим, что, например, в России уже существуют органы, занимающиеся оперативной разработкой фактов предполагаемых преступлений в сети Интернет. Отметим, что работа Интерпола в плане оперативности обработки информации менее эффективна, чем специализированных организаций меньшего масштаба. Так, российские правоохранительные органы чаще используют возможности Национального контактного пункта при БСТМ МВД России, который действует в формате 24/7 и предназначен обеспечивать взаимодействие с коллегами из ближнего и дальнего

зарубежья. Офицер спецподразделения одной из стран в любое время суток может оперативно связаться с таким же пунктом в другом государстве и получить или передать нужные сведения, необходимые для проведения оперативно-розыскных мероприятий. Сегодня национальные контактные пункты действуют почти в 50 странах[126].

Нужно также отметить, что в Проекте Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности от 11 октября 2017 г. (A/C.3/72/12), подготовленном Россией, содержится соответствующее положение, согласно которому в целях обеспечения оперативного содействия в проведении расследований, преследований или судебных разбирательств в связи с преступлениями, имеющими отношение к компьютерным системам и данным, или в сборе доказательств в электронной форме по уголовным преступлениям статья 57 предусматривает создание каждым государством – участником контактного центра, работающего 24 часа в сутки 7 дней в неделю (Сеть 24/7). Там же имеется статья 52 "Сотрудничество между правоохранительными органами".

В 2013 г. в Гааге был открыт Европейский центр по борьбе с киберпреступностью. Целями его создания являются сбор и обработка данных по киберпреступлениям, проведение экспертных оценок интернет-угроз, разработка и внедрение передовых методов профилактики и расследования киберпреступлений, подготовка новых кадров, оказание помощи правоохранительными судебным органам, а также координация совместных действий заинтересованных сторон, направленных на повышение уровня безопасности в европейском киберпространстве.

Нормы, содержащиеся в национальном уголовном и уголовно-процессуальном законодательстве

Вряд ли при разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях можно будет избежать рассмотрения вопроса о том, какие именно действия нужно рассматривать в качестве использования информационно-

[126] *Якимова Е.М., Наруттo С.В.* Международное сотрудничество в борьбе с киберпреступностью // Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10. № 2. С. 376–377.

коммуникационных технологий в преступных целях. Скорее всего, будет предусмотрена формулировка в самой всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Такая формулировка будет носить наверняка более или менее общий характер. При этом государства-участники должны будут предусмотреть в своих уголовных кодексах такую же статью, возможно, сформулировав ее более подробно, но не так, чтобы она противоречила тексту конвенции. Например, в зависимости от национальной практики, могут быть предусмотрены различные формы и сроки уголовного наказания. Впрочем, можно вполне обоснованно предположить, что то или иное государство может пойти по пути уточнения уже имеющихся норм уголовного и уголовно-процессуального права, а не формулирования новых статей.

Вряд ли можно будет обойтись без включения в национальные уголовные кодексы соответствующей статьи или статей, если они там еще не предусмотрены. Иначе будет трудно заводить уголовное дело по факту нарушения требований конвенции. Если же соответствующая норма (нормы) будет предусмотрена в уголовном кодексе, это существенно упростит процедурные вопросы уголовного преследования, так как они уже более или менее подробно прописаны в соответствующих уголовно-процессуальных документах (кодексах). Единственно, в УПК будет необходимо предусмотреть норму или группу норм, связывающих статью в уголовном кодексе с разбирательством в рамках всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (в рамках соответствующего международного суда, если он будет создан).

В уголовных кодексах разных государств нередко уже содержатся соответствующие положения. Например, в УК РФ есть целая группа статей, которые касаются преступлений, совершенных с использованием информационно-телекоммуникационных сетей. Но предварительно мы отметим содержание ч. 3 ст. 1 УПК РФ, которая гласит: "Если международным договором Российской Федерации установлены иные правила, чем предусмотренные настоящим Кодексом, то применяются правила международного договора". Таким образом, если будущей международной конвенцией о противодействии использованию информационно-коммуникационных технологий в преступных целях будут установлены какие-то

процессуальные правила рассмотрения дел, касающихся киберпреступлений, то формально именно эти правила и будут применяться в случае, если они противоречат правилам УПК РФ. Однако на практике, конечно же, желательно не ставить российские следственные и судебные органы в ситуацию, когда они при рассмотрении каждого конкретного дела будут вынуждены сравнивать международные обязательства РФ с национальным уголовно-процессуальным законодательством, выявлять расхождения, давать им толкование и решать, какие именно правила должны применяться: международные или национальные. Для того чтобы не ставить собственные органы следствия и суда в такое сложное положение, необходимо внести в российское уголовное и уголовно-процессуальное законодательство ясные и четкие правила, основанные на международных обязательствах РФ применительно к будущей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Итак, рассмотрим некоторые нормы российского уголовного законодательства, касающиеся вопросов, которые могут регулироваться всеобъемлющей международной конвенцией о противодействии использованию информационно-коммуникационных технологий в преступных целях. Упомянем сначала нормы, касающиеся такого преступного деяния, как терроризм.

Статья 205 УК РФ "Террористический акт" гласит:

"Совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями".

Статья 361 УК РФ "Акт международного терроризма", в частности, гласит:

"Совершение вне пределов территории Российской Федерации взрыва, поджога или иных действий, подвергающих опасности жизнь, здоровье, свободу или неприкосновенность граждан Российской Федерации в целях нарушения мирного сосуществования государств и

народов либо направленных против интересов Российской Федерации, а также угроза совершения указанных действий".

Нужно также упомянуть содержащуюся в УК РФ ст. 205.2. Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма:

"1. Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма.

2. Те же деяния, совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет…"

Вопросам пресечения террористической деятельности посвящены также ч. 2 ст. 20, подп. "р" ч. 1 ст. 63, ч. 3 ст. 64, ч. 3.2 ст. 72, ч. 5 ст. 78, ч. 1 ст. 82, ч. 4 ст. 83, подп. "в" ч. 1 ст. 104.1, статьи 205.1, 205.3, 205.4, 205.5, 207, 211, 282.2, 361 УК РФ. Однако понятно, что все указанные статьи предусматривают уголовное наказание без участия каких-либо международных органов. Соответственно, и УПК РФ прямо не предусматривает выполнения процедур во исполнение решения какой-либо международной судебной организации, занимающейся, например, пресечением использования информационно-коммуникационных технологий в преступных целях, хотя и предусматривает общий приоритет норм международного права.

Некоторые статьи российского уголовного кодекса касаются использования Интернета или иных информационно-телекоммуникационных сетей. Например, это подп. "д" ч. 2 ст. 110 УК РФ "Доведение до самоубийства", статья 137 "Нарушение неприкосновенности частной жизни", статья 151.2 "Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего", статья 159.3 "Мошенничество с использованием электронных средств платежа", статья 159.6 "Мошенничество в сфере компьютерной информации", СТАТЬЯ 171.2 "Незаконные организация и проведение азартных игр", статья 185.3 "Манипулирование рынком", статья 228.1 "Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические

средства или психотропные вещества", статья 238.1 "Обращение фальсифицированных, недоброкачественных и незарегистрированных лекарственных средств, медицинских изделий и оборот фальсифицированных биологически активных добавок", статья 242 "Незаконные изготовление и оборот порнографических материалов или предметов", статья 242.1 "Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних", статья 242.2 "Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов", статья 245 "Жестокое обращение с животными", статья 258.1 "Незаконные добыча и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации", статья 274 "Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей", статья 280 "Публичные призывы к осуществлению экстремистской деятельности", статья 280.1 "Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации", статья 282 "Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства".

Следует подробнее упомянуть следующие нормы, содержащиеся в УК РФ:

"Статья 159.6. Мошенничество в сфере компьютерной информации

1. Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей".

"Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-

телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб".

"Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

1. Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации.

2. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации.

3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации".

Видеоконференц-связь

Существенно, что в связи с распространением коронавируса сформировалась как национальная, так и международная практика поддержания контактов и проведения переговоров в формате

удаленного доступа. В этом случае участники переговоров не встречаются лично, а общаются через информационные каналы связи, при этом перед каждым участником на экране видны в реальном времени другие представители. Мало того, такие переговоры имеют место и на высшем уровне, между главами государств и правительств. Это очень важный шаг вперед в системе международного общения. Во-первых, стала общепринятой такая практика. Во-вторых, оказалось возможным обеспечить такие каналы связи, которые более или менее не подвержены постороннему вмешательству. Значит, такую практику можно использовать и при рассмотрении судебных дел.

На самом деле в уголовно-процессуальном законодательстве России видеоконференц-связь предусмотрена уже много лет. Формально такой формат закреплен, например, в ч. 2 ст. 389.12 УПК РФ ("Осужденному, содержащемуся под стражей и заявившему о своем желании присутствовать при рассмотрении апелляционных жалобы, представления, по решению суда обеспечивается право участвовать в судебном заседании непосредственно либо путем использования систем видеоконференц-связи"). Согласно ч. 6 ст. 35 УПК РФ "По решению суда обвиняемый участвует в судебном заседании путем использования систем видеоконференц-связи". Согласно ч. 4 ст. 240 УПК РФ "Свидетель и потерпевший могут быть допрошены судом путем использования систем видеоконференц-связи". Этот вопрос регулируется также в ч. 6.1 ст. 241, ст. 278.1, ч. 1 ст. 293, ч. 8 ст. 389.13, ч. 2, 2.1 ст. 399, ч. 2 ст. 401.13 УПК РФ.

Таким образом, по крайней мере в судебной практике Российской Федерации, видеоконференц-связь – уже признанная, формально закрепленная и фактически применяемая практика. При этом важно иметь в виду, что речь идет о рассмотрении именно уголовных дел. То есть такая практика явно может быть использована международным судом, созданным для рассмотрения дел в рамках всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Использование видеоконференц-связи влечет многие практические последствия. Нет нужды в обязательном порядке создавать штаб-квартиру суда с использованием каких-то объектов недвижимости. В случае возникновения конкретного дела его участники будут пользоваться тем помещением, где имеется видеоконференц-связь. Сотрудники аппарата суда также могут работать на удаленном

доступе. Таким образом, первое последствие – это значительная экономия средств на оборудовании штаб-квартиры.

Второе последствие – участники разбирательства не будут привязаны к какому-то определенному месту проведения заседаний. Они смогут участвовать в заседании, фактически находясь где угодно, если там есть техническая возможность обеспечить видеоконференц-связь. Отсюда вытекает значительная экономия на командировочных расходах. Однако если участник разбирательства в любом случае хочет, чтобы его представитель физически присутствовал в месте нахождения судей, он сам и будет нести соответствующие расходы.

Видеоконференц-связь это значительная оперативность рассмотрения дел. Судья перед формальным назначением даты разбирательства может выяснить ближайшую дату рассмотрения, приемлемую для всех сторон. И такой датой может быть даже следующий день после получения согласия всех участников – немыслимая оперативность для судебного производства.

Отсутствие привязки к определенному месту рассмотрения конкретного дела снимает с повестки для довольно щекотливый вопрос о привилегиях и иммунитетах как штаб-квартиры суда, так и участников разбирательства. Конечно, все равно понадобятся какие-то гарантии, что стороны разбирательства не будут пытаться влиять на судей, а также сотрудников суда. Однако решение этого вопроса будет иметь достаточно простой формальный характер: выдавать иностранным участникам разбирательства служебные или дипломатические визы и распространять на них привилегии и иммунитеты, предоставленные в той или иной стране для иных лиц, пользующихся такими визами. Конечно, отдельно будет стоять вопрос о статусе лиц, числящихся подозреваемыми или обвиняемыми. И отдельно нужно будет предусмотреть нормы, регулирующие взаимоотношения государства с собственными гражданами, участвующими в судебном разбирательстве.

Подозреваемые и обвиняемые

Если речь идет о преступлениях, то есть об уголовном преследовании, то оно может касаться только физических лиц. То есть юридические лица не могут фигурировать в качестве привлекаемых к уголовной ответственности в рамках всеобъемлющей международной конвенции о противодействии использованию информационно-

коммуникационных технологий в преступных целях. Но несомненно, что такими лицами могут быть должностные и иные лица, имеющие отношение к тем или иным юридическим лицам (учредители, руководители, сотрудники, члены наблюдательных советов, спонсоры и др.). И юридические лица могут быть привлечены к иной ответственности, нежели уголовная.

В российском проекте Конвенции ООН о сотрудничестве в сфере противодействия информационной преступности от 11 октября 2017 г. (A/C.3/72/12) сказано:

"Статья 20. Ответственность юридических лиц

1. Каждое Государство-участник принимает такие законодательные и иные правовые меры, которые необходимы для обеспечения возможности привлечения к ответственности юридических лиц в связи с преступлениями и иными противоправными деяниями, признанными в качестве таковых в соответствии с настоящей Конвенцией, если эти деяния совершены в их интересах любым физическим лицом, действующим в личном качестве или в качестве члена органа соответствующего юридического лица, занимающего в данном юридическом лице руководящую должность на основании:

a) полномочий представлять данное юридическое лицо;

b) права принимать решения от имени этого юридического лица;

c) права осуществлять контроль внутри этого юридического лица.

2. В дополнение к случаям, уже предусмотренным пунктом 1 настоящей статьи, каждое Государство-участник принимает меры, необходимые для обеспечения возможности возложения ответственности на юридическое лицо в случаях, когда отсутствие руководства или контроля со стороны физического лица, упомянутого в пункте 1, делает возможным совершение преступления или иного противоправного деяния, предусмотренного положениями настоящей Конвенции, в пользу этого юридического лица физическим лицом, действующим на основании данных ему полномочий.

3. В зависимости от применяемых соответствующим Государством-участником юридических принципов ответственность юридического лица может носить уголовный, гражданско-правовой или административный характер.

4. Привлечение к ответственности юридических лиц не исключает привлечение к ответственности физических лиц, совершивших преступление и иное противоправное деяние".

Как вообще будет проходить процесс выявления лиц, виновных в совершении преступлений, связанных с использованием информационно-коммуникационных технологий, их участие в разбирательстве и исполнение в отношении них решений суда? Сторонами суда будут государства, а теоретически – и какие-то международные организации. Для простоты изложения будем дальше говорить только о государствах, имея в виду, что теоретически речь может идти и о международных организациях. Однако вряд ли такой организацией будет организация, созданная специально для осуществления целей, предусмотренных всеобъемлющей международной конвенцией о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Видимо, преследование соответствующих физических лиц будет начинаться с установления факта использования ИКТ в преступных целях. То есть какое-то государство сначала устанавливает такой факт, потом фиксирует его в соответствующей форме. Возможно, должно быть возбуждено уголовное дело по соответствующей статье, предусмотренной в уголовном законодательстве. Например, это формально может быть заявление государства-участника в суд об установлении факта использования ИКТ в преступных целях. Возможно, будут определены процессуальные нормы, позволяющие суду предпринимать соответствующие действия для установления личности преступника. Например, это могут быть судебные поручения, касающиеся государств-участников и предусматривающие проведение каких-то оперативно-розыскных мероприятий. Но в любом случае в заявлении государства в суд должны быть обозначены какие-то более или менее значимые факты, позволяющие установить личность предполагаемого преступника. А более приемлемый и легкий вариант: в заявлении государства будет прямо обозначено лицо, которое подозревается в совершении преступления.

Формирование состава суда

Вопрос о формировании состава суда может быть решен самым различным образом. Для начала должен быть определен председатель суда. Таковым может быть представитель каждого государства-участника будущей конвенции по очереди, со сроком полномочий, например, в три года. Возможно назначение на постоянной основе председателем суда представителя того государства, которое

предоставит значимый вклад в решение организационных вопросов (финансовый взнос, выделение здания для суда, предоставление штата сотрудников суда и др.).

Когда председатель суда будет назначен, встанет вопрос о формировании в целом состава суда. Тут наиболее простым представляется вариант, используемый, например, в российском законодательстве для формирования состава третейского суда. То есть каждое государство-участник дает в суд список своих представителей, которые могут быть использованы для конкретного разбирательства. Далее государство-заявитель (то есть государство, заявившее о факте киберпреступления против него или против его организаций или физических лиц) выбирает из имеющихся списков кандидатуры судей. Такое же количество судей имеет право выбрать и лицо, обвиняемое в киберпреступлении. Если в определенный срок кандидаты не выбраны, их своих волевым решением назначает председатель суда. Далее стороны (государство-заявитель и обвиняемый) должны договориться в определенный срок о председателе судебного состава для данного конкретного разбирательства. Если они не могут договориться, эти функции выполняет председатель международного суда.

Заключение

1. Виды угроз

Итак, подведем некоторые итоги. Если подходить с точки зрения обеспечения безопасности, то проблемы использования ИКТ, в том числе цифровых технологий, можно условно разделить на следующие группы.

1. Системы связи. В этой области стоит проблема недопущения перехвата, кражи информации, вторжения в процесс передачи информации со стороны третьих лиц. Тут достигнуты достаточно весомые успехи, как на национальном, так и на международном уровне.

2. Предотвращение использования информационной среды для террористических, а также иных уголовно наказуемых и в целом противоправных целей. В этой области также достигнут существенный прогресс. Указанные угрозы одинаково нежелательны для всех государств. Соответственно, уже заключены многосторонние (в том числе Будапештская конвенция 2001 г.) и двусторонние международные соглашения для совместных действий по противодействию этим угрозам. На экспертном уровне ведется активная работа в рамках ООН, наконец, планируется разработать всеобъемлющую международную конвенцию о противодействии использованию информационно-коммуникационных технологий в преступных целях.

3. Военно-политические угрозы с использованием информационной среды, в том числе Интернета (вмешательство во внутренние дела других государств, шпионаж, подрывные операции, экспорт "цветных" революций, информационная война). В этих вопросах на международном уровне пока не сложился единый подход. Ряд государств ссылается на то, что тут пока вряд ли удастся прийти к единому мнению, что конкретно понимается под этими угрозами. Соответственно, в этой области перспективы международного сотрудничества пока достаточно неопределенные.

4. Неосторожное вторжение в устройство окружающего мира. В этой области существуют как очевидные, так и неочевидные угрозы. Очевидные, это, например, наделение используемого в военных целях искусственного интеллекта способностями самостоятельно выбирать

и уничтожать те или иные цели. К очевидным угрозам также относятся попытки изменения с помощью различных технологий генома как вирусов и бактерий, так и генома иных живых существ, в том числе и человека. Эти угрозы признаются мировым сообществом, однако пока, как правило, не рассматриваются как часть общих угроз, проистекающих из использования цифровых технологий. Соответствующие меры по обеспечению безопасности принимаются, в частности, на уровне микробиологии, в области обеспечения качества потребляемых продуктов питания (ГМО). На национальном уровне нередко запрещены некоторые виды манипуляций с геномом человека.

Неочевидные угрозы связаны также с тем, что нельзя исключать, что в основе жизни на Земле лежат исключительно цифровые технологии, а приписываемые человеку такие качества, как свобода выбора, свобода воли (или активность для иных живых существ), наличие души – на самом деле объективно не существуют. Нельзя исключать также, что отдельные общепризнанные теории происхождения жизни на Земле (теория эволюции) не совсем точны или вовсе ошибочны. Нельзя исключить, что естественный интеллект возник вовсе не в результате эволюции видов живых существ, возникших в силу случайного совпадения многих факторов. Возможно, что жизнь на Земле (соответственно, и естественный интеллект) возникла не самостоятельно, а как продукт развития (эволюции) цифровых технологий, возможно, существующих на неорганических носителях. Такая возможность рассматривается научным сообществом в целом как совершенно невероятная. Однако если, вопреки мнению авторитетных ученых, дело обстоит именно так, это означает, что неосторожное вторжение человека в эту область (в том числе совершенствование ИКТ, в том числе цифровых технологий, формирование обширной единой информационной среды, создание искусственного интеллекта) чревато угрозой уничтожения самой жизни на органических носителях на нашей планете. Можно ли пренебрегать даже самыми маловероятными угрозами, если речь идет об обеспечении безопасности или даже выживании человечества?

В качестве комментария к вышеупомянутой возможности существования неочевидных угроз отметим, что современная наука пока не смогла найти бесспорные доказательства, что жизнь на Земле (или где-то еще, например, на Марсе) возникла случайно. Пока не удалось создать жизнь в лаборатории из органических или каких-либо

еще материалов. Пока не удалось доказать, что одни биологические виды могут свободно трансформироваться в другие, причем принципиально отличающиеся по устройству, например, растения в животных и наоборот (хотя теория эволюции именно это и предполагает). Пока мы наблюдаем не массовое превращение одних видов в другие, а как раз наоборот, массовое исчезновение биологических видов, причем в достаточно тепличных условиях, существующих на Земле.

Наверное, можно более или менее обоснованно утверждать, что современная наука пока не доказала, что у человека действительно имеется такое качество, как "свобода воли", и не выяснила, каков ее физический носитель. Все "доказательства" тут пока не носят объективного характера, а являются исключительно нашими субъективными ощущениями.

Однако один факт совершенно очевиден: на Земле существует огромное многообразие живых организмов, устроенных исключительно сложно. Откуда-то и как-то они все взялись. Откуда и как?

2. Перспективы будущего устройства глобального информационного пространства и порядка его использования

Пока, как уже было указано, мировое сообщество достигло определенного прогресса в выработке универсальных норм международного права, регулирующих противодействие использованию ИКТ в преступных и иных противоправных целях – принята Будапештская конвенция 2001 года. В конце 2019 года ГА ООН приняла резолюцию, предусматривающую разработку всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Однако тут имеются серьезные проблемы. Во-первых, США и их союзники не поддержали указанную резолюцию ГА ООН. Это значит, что они не будут принимать участия в разработке новой конвенции и, более того, скорее всего, будут противодействовать ее заключению. Дело тут не только в том, что уже существует Будапештская конвенция. Добившись большинства при принятии указанной резолюции, Россия и Китай, по сути, бросили вызов США, попытались поставить под сомнение лидирующее

положение этой страны в вопросе использования ИКТ. Вряд ли США легко согласятся на столь существенные репутационные потери.

Во-вторых, при разработке новой конвенции, без сомнения, возникнут существенные проблемы поиска общеприемлемых определений и формулировок. Например, такие проблемы возникнут с определением кибертерроризма, которые проистекают из неопределенности того, что вообще следует считать терроризмом. По мнению автора, он достаточно четко обозначил эти проблемы в соответствующем разделе данной работы.

Важный вопрос, это военно-политическое использование киберпространства, то есть информационная война, подрывные операции, вмешательство во внутренние дела других государств, шпионаж. Пока очевидно, что ключевой мировой игрок в этой области – США – стремятся установить такой порядок использования глобальной Сети, который опирается на полное доминирование этой страны, а не на, например, баланс сил. По мнению американцев, их технические и политические возможности намного превосходят возможности стран, которые они рассматривают в качестве оппонентов.

Такой подход США означает следующее: во-первых, пока нет никаких перспектив урегулирования этого вопроса с помощью заключения международных договоров, приемлемых для подавляющего числа стран.

Во-вторых, в ближайшее время в использовании глобального информационного пространства будет существовать силовое противоборство между основными центрами силы, возможно, между США и их союзниками с одной стороны, и Россией и Китаем и их союзниками – с другой стороны. Не исключено, что сформируются и иные центры силы, например, из государств с населением, исповедующим преимущественно Ислам. По результатам этого силового противоборства и будет складываться фактический порядок использования киберпространства.

Конечно, можно призывать использовать киберпространство в мирных целях. Но такие призывы в лучшем случае – элемент пропаганды, в худшем – опасное заблуждение, недостижимая утопия.

Существенный вопрос: как следует России дальше публично формулировать свою политику в вопросе о военно-политическом использовании ИКТ. Пока российские официальные власти чаще отказываются признавать (но не всегда), что используют

киберпространство в военно-политических целях. Смысл такой тактики, в общем, понятен: не нагнетать страсти, не давать повода обвинять страну в агрессивной политике, не провоцировать ухудшение отношений с тем или иным государством. Однако тут следует учитывать, что страна, пострадавшая от кибератаки, может более или менее точно установить, кто являлся организатором атаки. Частично это можно выяснить с помощь соответствующих технических средств. Частично – за счет информации, получаемой от агентов, внедренных в структуры, отвечающие за использование ИКТ. В результате вместо сдерживания страстей получается как раз наоборот – их дополнительное разжигание, ведь РФ, будучи разоблаченной, приобретает имидж страны, действующей "исподтишка", "подло". Мало того, не исключено, что американские политики рассматривают такую тактику России как признак слабости, как страх разозлить США. Значит, надо еще поднажать!

Возможно, более рациональным было бы не отрицать, что в киберсреде сложилась самая настоящая гонка "кибервооружений", и Россия вынуждена в ней участвовать. Открытость в этом вопросе может оказаться полезней, чем отрицание очевидного.

В зависимости от результатов указанной гонки кибервооружений и будет складываться будущий порядок использования киберпространства. Возможно, США и их союзники сохранят тут доминирующее положение. В таком случае вряд ли следует рассчитывать на заключение международных договоров, регулирующих военно-политическое использование ИКТ. Однако, скорее всего, доминирование сохранить не удастся, в каких-то областях, а возможно, и в целом, сложится более или менее стабильный баланс сил. Если в каких-то вопросах этот баланс сил будет не в пользу США, в таком случае они, как обычно, выступят за заключение международных договоров, сдерживающих успехи других стран. Однако в такой ситуации возникает хороший вопрос: нужно ли будет этим странам (в том числе России) соглашаться на такие сомнительные договоры?

Пока США ясно обозначают, что рассматривают Россию, Китай, Индию в качестве потенциальных противников США в киберпространстве. Не исключено, что в такой ситуации, учитывая состояние российско-американских отношений, есть смысл рассмотреть вопрос о заключении российско-китайского договора о

взаимопомощи в военно-политическом использовании киберпространства.

ТРОФИМОВ Владимир Николаевич, доктор юридических наук, член Национальной Ассоциации международной информационной безопасности, действительный член Российской академии естественных наук.
Сотрудник Договорно-правового отдела МИД СССР, сотрудник Правового департамента МИД РФ, советник аппарата Комитета по международным делам Верховного Совета РФ, руководитель аппарата Комитета по международным делам Государственной Думы РФ.

Другие работы автора:
Международно-правовой статус Антарктики, М., Прометей, 1990, 153 с. - ISBN 5-7042-0339-6
Военная и экологическая безопасность. Международное право и сила. М., Прометей, 1991, 131 с. - ISBN 5-7042-0552-6
Международное право. Словарь - справочник. М., 1998, 363 с.
Большой юридический словарь (в соавторстве), М., 1997, 790 с.
Применение антимонопольного законодательства: Сборник судебной практики с комментариями, М., Wolters Kluwer, 2006, 505 с.
Недействительность сделок. Сборник судебной практики с комментариями, М., Wolters Kluwer, 2008, 340 с.
Искусственный интеллект: добро и зло как запретный плод. М., Дашков и Ко, 2011, 441 с. - ISBN 978-5-394-01580-9
Коллаборационисты: мнимые и настоящие. Субхас Чандра Бос, Махатма Ганди, Шарль де Голль, Андрей Власов, Михаил Горбачев. М., Ваш Формат, 2015, 198 с. - ISBN 978-5-9905971-9-8
Саботаж. М., "Делибри", 2018, 767 с. - ISBN 978-5-4491-0134-1

Связь с автором: dialog-partner@list.ru

см. также: koob.ru/trofimov_v/

Трофимов Владимир Николаевич

Применимость международного права к киберпространству: иллюзия или реальность?

ИЗДАТЕЛЬСТВО «ЮСТИЦИНФОРМ»
юридическая, экономическая и деловая литература;
журналы «Право и экономика», «Вестник арбитражной практики»,
«Журнал предпринимательского и корпоративного права»
Главный редактор В.А. Вайпан
Генеральный директор В.В. Прошин

Редактор В.Ю.Шишкина
Корректор О.Ю.Дзюба
Подписано в печать 17.02.2021.
Формат 60x90/16. Бумага офсетная. Печ. л. 11,4.
Тираж по требованию.

Юстицинформ
119607, г. Москва, ул. Лобачевского, 94, оф. 7.
Тел.: (495) 232-12-42
http://www.jusinf.ru E-mail: info@jusinf.ru