ГОСУДАРСТВО И ПРАВО, 2017, № 10, с. 5–18

© 2017 г.
А.Н. САВЕНКОВ

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ В ФИНАНСОВО-КРЕДИТНОЙ СФЕРЕ КАК ВЕКТОР ОБЕСПЕЧЕНИЯ ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ

Савенков Александр Николаевич *– доктор юридических наук, профессор, член-корреспондент РАН, заслуженный юрист РФ, врио директора Института государства и права РАН (Россия, Москва) (E-mail: an61s@yandex.ru).*

Savenkov Alexander N. *– Doctor of Law, Professor, corresponding member of the Russian Academy of Sciences, honoured lawyer of the Russian Federation, acting Director of the Institute of state and law of Russian Academy of Sciences (Russia, Moscow) (E-mail: an61s@yandex.ru).*

Аннотация*: в статье исследуются новые вызовы и угрозы безопасности в финансово-кредитной сфере, анализируются проблемы противодействия киберпреступности в условиях глобализации. Определены основы правового регулирования этой деятельности, а также высказаны предложения по совершенствованию инструментов правового воздействия в целях предупреждения и пресечения криминальной активности в информационной сфере. Рассмотрены вопросы влияния глобализации на киберпреступность, значение и недостатки Будапештской конвенции о киберпреступности 2001 г., поддержана необходимость принятия Конвенции ООН как универсального инструмента по противодействию киберпреступности. Проведен анализ динамики и тенденций киберпреступности, исследованы вызовы и угрозы проблем обеспечения информационной безопасности в финансово-кредитной сфере. Рассмотрен международный опыт по защите информационного пространства от кибератак. Указывается на необходимость дальнейшего совершенствования законодательной базы в целях борьбы с киберугрозами, в том числе в финансово-кредитной сфере, и расширения комплексного противодействия киберпреступности путем организации широкомасштабного сотрудничества на государственном уровне, в частности, посредством создания единой системы обеспечения безопасности финансово-кредитных правоотношений в глобальных информационных сетях.*

Abstract: *the article deals with some issues in security of the financial and credit sector, issues of countering the threats from cybercrime in the context of globalization. Determine the basis of legal regulation of this activity, as well as suggestions for improving the legal instruments in order to influence the prevention and suppression of criminal activities in the information sphere. The article deals with such issues as influence of globalization on cybercrime, significance and disadvantages of The Budapest Convention on Cybercrime, 2001, the need to adopt The United Nations Convention as a universal instrument for combating cybercrime. The cybercrime dynamics and tendencies, the challenges and threats to information security of the financial and credit sector are analyzed in the article. We consider international experience on protection of information space from cyber-attacks. The necessity of further improvement of the legislative framework to combat cyber threats, including in the financial and credit sector, and expand integrated cybercrime by organizing large-scale cooperation on the state level, in particular through the creation of a unified system of security of the financial and credit relations in the global information networks.*

Ключевые слова*: киберпреступность, киберугрозы, компьютерная преступность, международная информационная безопасность, противодействие преступности, вредоносное программное обеспечение, криптовалюта, цифровая экономика, финансово-кредитная сфера.*

Key words: *cybercrime, cyber threats, computer crime, international information security, combating crime, malicious software, cryptocurrency, the digital economy, the financial and credit sector.*

В правовом государстве в условиях глобализации, усиливающейся динамики развития информационного общества, "электронного государства", цифровой экономики, роста вызовов и угроз информационной безопасности особую роль играют формирование и реализация государственной политики, направленной на учет современных информационных тенденций развития всех сфер жизни общества и государства, выработку научно обоснованных, выверенных, взвешенных подходов регулирования новых информационных отношений.

При этом очевидно, что внедрение во все сферы нашей жизни информационно-коммуникационных технологий и использование их в преступных целях носят транснациональный характер.

Глобализация современного мира не в последнюю очередь связана с развитием сети Интернет. Данное обстоятельство является как благом для человечества, так и несет в себе определенные

риски, в том числе в сфере обеспечения информационной безопасности, поскольку именно возможности сети Интернет используются международными преступными синдикатами для совершения различных противоправных действий в информационной сфере практически любым субъектом, в любой стране, в отношении личности, общества, государства; обусловливают сложный субъектный состав правонарушения; ставят в повестку дня специальные вопросы юрисдикции и экстерриториальности. Лица, занимающиеся хищениями в финансово-кредитной сфере, находятся в разных регионах нашей страны или за рубежом и применяют для взаимодействия исключительно электронные средства коммуникации. Пример – вирус-вымогатель *Petya*, атаковавший целенаправленно инфраструктуру ряда государств, в том числе России, через спам-рассылку по электронной почте.

Противодействие киберпреступности – проблема международного масштаба. Вопрос о базовых принципах правового обеспечения информационной безопасности в условиях формирования и развития киберпространства, его трансграничности имеет не только научное, но и практическое значение. Действуют ли общепризнанные принципы международного права в киберпространстве? Следует согласиться, что масштаб и технологический уровень деструктивного использования информационно-коммуникационных технологий неуклонно возрастает. При этом отсутствие необходимой международной правовой базы, регулирующей деятельность государств в сфере их использования, на сегодняшний день есть одна из ключевых проблем безопасности[1].

Автоматическое применение существующих международно-правовых норм в киберпространстве представляется неприемлемым, но вместе с тем отдельные нормы современного международного права вполне могут быть использованы для правового регулирования киберпространства. Так, п. 1–2 ст. 19 Международного пакта о гражданских и политических правах 1966 г.[2] закрепляет право каждого гражданина беспрепятственно придерживаться своих мнений и свободно их выражать, включая свободу искать, получать и распространять всякого рода информацию и идеи независимо от государственных границ, устно, письменно или посредством печати или художественных форм выражения, или иными способами по своему выбору, что очевидно распространяется и на киберпространство. Пункт 3 указанной статьи устанавливает правовые рамки этой свободы, налагая особые обязанности и ответственность, сопряженные с устанавливаемыми законом некоторыми ограничениями, необходимыми для охраны государственной безопасности, общественного порядка, здоровья или нравственности населения, уважения прав и репутации других лиц. Понятны и применимы также общепризнанные принципы международного права, такие как уважение суверенитета государств, невмешательство в их внутренние дела, уважение прав человека и основных свобод.

Угрозы противоправного применения информационных и телекоммуникационных технологий в виртуальном пространстве уже звучат не парадоксально, носят реальный характер, представляют серьезную опасность, поэтому проблема борьбы с киберпреступностью обсуждается на самом высоком государственном уровне и занимает значительное место во внутренней политике государств.

Так, в Концепции внешней политики Российской Федерации, утвержденной Указом Президента РФ от 30 ноября 2016 г. № 640[3], отмечено, что современный мир характеризуется стремительным ростом уровня, расширением характера и географии таких имеющих трансграничную природу вызовов и угроз, как киберпреступность. На пресс-конференции по итогам переговоров с госсекретарем США Р. Тиллерсоном российский министр иностранных дел С.В. Лавров дал понять, что Москва рассматривает киберпространство как сферу, где российско-американское сотрудничество необходимо[4].

На сегодняшний день американские спецслужбы теоретически имеют возможность планировать и осуществлять кибератаки не только на российские банки, иные гражданские объекты, но и на военные, а также на объекты критически важной инфраструктуры – атомной энергетики, топливно-энергетического комплекса, транспорта и др. В ее основе перечень уязвимостей и закладок, поставляемых в Россию западными независимыми вендорами аппаратных средств

[1] См.: *Полякова Т.А.* Базовые принципы правового обеспечения информационной безопасности // Труды ИГП РАН. 2016. № 3 (55). С. 17.

[2] См.: Международный пакт о гражданских и политических правах. Принят резолюцией 2200 А (XXI) Генеральной Ассамблеи от 16 декабря 1966 года // http://www.un.org/ru/documents/decl_conv/conventions/pactpol (Дата обращения: 22.06.2017 г.).

[3] См.: Собрание законодательства РФ. 2016. № 49. Ст. 6886.

[4] См.: Противоботство сверхдержав. Россия предлагает изменить правила борьбы с киберпреступностью в мировом масштабе // http://www.kommersant.ru/doc/3270121 (Дата обращения: 22.06.2017 г.).

и программного обеспечения *(ISV, Independent Software Vendor)*; знание критических уязвимостей в распространенных средствах шифрования сетевого трафика (пакеты *OpenSSL, OpenSSH*, технологии *IPSec* и *OpenVPN*, протоколы *ESP, AH, ISAKMP, Oakley* и др.), а также повсеместное использование американских стандартов шифрования (стандарт *Advanced Encryption Standard (AES)*) и алгоритма *RSA* – криптографический алгоритм с открытым ключом. Сюда добавляется многочисленный набор таких эксплойтов-кит, как *Rig EK, Terror EK*, троянов – *Ztorg, Conficker, Cryptowall, CryptoLocker* и др., руткитов *(rootkit)* – *TDSS, Sinowal, Whistler*, специальных банковских вредоносных программ – *Zeus, Tinba, Ramnit* и другого вредоносного программного обеспечения[5].

Для поставляемых на российский рынок технических средств, включая сетевое оборудование, создан и активно используется объемный спектр программно-аппаратных врезок, имплантов и модулей со скрытыми функциями. США намерены вложить около 7 млрд долл. на обеспечение кибербезопасности в рамках проекта бюджета на 2017 финансовый год. По мнению министра обороны США Э. Картера, за пять лет этот показатель составит 35 млрд долл.[6]

Безусловно, глобализация меняет не только экономические и культурные отношения, движение капитала и различных ресурсов, но и формирует новые вызовы и угрозы, прежде всего при использовании ИКТ в финансово-кредитной сфере.

В связи с указанными вызовами и угрозами в России отмечается тенденция активного развития системы документов стратегического планирования, которые направлены на борьбу с киберпреступностью. В соответствии с Федеральным законом "О стратегическом планировании в Российской Федерации"[7] указами Президента РФ утверждены новая Стратегия национальной безопасности Российской Федерации[8] и Доктрина информационной безопасности Российской Федерации[9], а ранее – и Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года[10].

Соотношение понятий информационной безопасности и кибербезопасности

Кибербезопасность, ее обеспечение, включая противодействие киберпреступности, становятся актуальной проблемой во всем мире, хотя решение этих вопросов в зарубежных государствах отличается различными подходами: от полных запретов и блокировок сайтов до придания правового статуса и обязательности требований по информационной безопасности.

Понятие "кибербезопасность" в настоящее время отсутствует в законодательстве Российской Федерации, как и понятие "киберпространство". В России традиционно используется термин "информационная безопасность".

В новой Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646, информационная безопасность Российской Федерации определена как 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 также отмечается, что возможности трансграничного оборота информации все чаще используются для криминальных и иных противоправных целей.

Вместе с тем понятие "кибербезопасность" как "сохранение конфиденциальности, целостности и доступности информации в киберпространстве" содержится в Стандарте 27032:2012 (ISO/IEC 27032:2012)[11]. При этом киберпространство определяется как "комплексная среда в результате взаимодействия людей, программного обеспечения и услуг в сети Интернет с помощью технологии устройств и сетей, подключенных к нему, и не существующим в материальной (физической) форме".

Понятие "киберпреступность" используется в настоящее время в различных значениях. При

[5] См.: http://www.cxotoday.com/story/ransomware-doubled-in-second-half-of-2016-check-point/ (Дата обращения: 22.06.2017 г.).

[6] См.: http://www.rbc.ru/opinions/politics/18/10/2016/58061e999a79475012a7061c (Дата обращения: 22.06.2017 г.).

[7] См.: Росс. газ. 2014. 3 июля.

[8] См.: Собрание законодательства РФ. 2016. № 1 (Ч. II). Ст. 212.

[9] См.: Собрание законодательства РФ. 2016. № 50. Ст. 7074.

[10] Утверждены Указом Президента РФ от 24 июля 2013 г. № Пр-1753 (см.: http://www.scrf.gov.ru/ (По сост. на 24.04.2015 г.)).

[11] См.: http://www.iso.org/standard/44375.html Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности (Дата обращения: 22.06.2017 г.).

этом смешиваются такие нечеткие понятия, как *IT-crime*, *e-crime*, *high-techcrime,* применяемые в зарубежных государствах[12], однако научно обоснованного, легитимного определения указанного понятия нет.

На Десятом Конгрессе ООН по предупреждению преступности и обращению с правонарушителями (г. Вена, 2000 г.) была предпринята попытка объяснить сущность киберпреступности как любого преступления, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против неё. Однако в дальнейшем данное определение не было включено в текст Конвенции Совета Европы о преступности в сфере компьютерной информации ETS № 185[13].

Основываясь на опыте исследования и практической деятельности, возможно определить киберпреступность как умышленные общественно опасные деяния, установленные уголовным законом государства, совершенные путем неправомерного доступа к электронной информации, содержащейся в компьютерных сетях и использующие их возможности системах связи и телекоммуникаций.

В этой связи в настоящее время представляется необходимым определить научные исследования в сфере киберпреступности в качестве важного вектора развития криминологической теории.

Глобализация и поиск универсальных механизмов противодействия киберпреступности

Многие изменения, происходящие сегодня в нашей жизни, связывают с глобализацией. Это состояние современного мира пытаются осмыслить ученые практически всех отраслей науки: философии, политологии, социологии, биологии, физики и др. Юристы также пытаются познать данный феномен: что такое глобализация и глобализм? Каковы вызовы и угрозы международной и национальной безопасности на современном этапе развития общества?[14]

Как справедливо отмечает Председатель Конституционного Суда РФ, проф. В.Д. Зорькин, "глобализация – это вызов, который надо уметь достойно встретить"[15]. Однако, как оказалось, человечество не в полной мере готово (в частности, в правовой сфере) к проблемам глобализации, связанным также и с развитием киберпреступности.

Заведующий кафедрой теории государства и права и политологии МГУ им. М.В. Ломоносова, проф. М.Н. Марченко определяет глобализацию с точки зрения системного подхода как "системную, многоаспектную и разноуровневую интеграцию различных существующих в мире государственно-правовых, экономико-финансовых и общественно-политических институтов, идей, принципов, связей, морально-политических, материальных и иных ценностей, разнообразных отношений"[16]. Полагаем, что такое отношение к глобализации вполне проецируется на сложные проблемы противодействия киберпреступности в условиях трансграничности и глобального информационного общества.

Киберпреступность как явление возникла всего несколько десятилетий назад. Однако за короткое время с развитием информационных технологий феномен противоправных деяний в киберпространстве успел превратиться в глобальную проблему, поставив под угрозу не только отдельных пользователей, но и информационную безопасность целых государств[17].

Следует учитывать формы организованных киберпреступлений. Обществу противостоят хорошо организованные подпольные киберсиндикаты, располагающие значительными финансовыми и техническими потенциалами. Деятельность таких преступных групп, как правило, исключает личные контакты и реальную сплоченность участников.

---

[12] См.: *Полякова Т.А., Морозов А.В.* Организационно-правовое обеспечение информационной безопасности. М., 2013. С. 205, 206.

[13] См.: Конвенция о преступности в сфере компьютерной информации (ETS № 185) [рус., англ.] (Заключена в г. Будапеште 23.11.2001) (с изм. от 28.01.2003) // http://www.consultant.ru (Дата обращения: 22.06.2017 г.). Российская Федерация указанную Конвенцию не подписала.

[14] "На развитие государства и права важное влияние в настоящее время оказывают такие процессы, как модернизация, глобализация и интеграция, и каждый из них может иметь как положительные, так и отрицательные стороны: глобализация иногда жестко ломает привычный уклад, социокультуру, в то время как интеграция может приводить к излишней зависимости" (см.: *Чиркин В.Е.* Наднациональные и межгосударственные образования и наднациональное право // Юрид. мысль. 2015. № 4. С. 111–118). Следует согласиться, что у человечества в целом по мере перехода его к новому состоянию – глобальному – помимо всех существующих уровней трудностей и забот, которые никуда не делись, просто по определению не может не быть новых проблем, но теперь уже мирового масштаба (см.: *Чумаков А.Н.* Глобализация. Контуры целостного мира. Изд. 2-е, перераб и доп. М., 2015. С. 42).

[15] *Зорькин В.Д.* Россия и Конституция в XXI веке. Изд. 2-е, доп. М., 2008. С. 419.

[16] *Марченко М.Н.* Государство и право в условиях глобализации. М., 2016. С. 12, 13.

[17] См.: *Тропина Т.Л.* Борьба с киберпреступностью: возможна ли разработка универсального механизма? // СПС "КонсультантПлюс".

Криминологические исследования свидетельствуют о том, что преступные кибергруппы характеризуются наличием так называемой "виртуальной" интегрированности входящих в нее лиц, возможностью анонимного участия в деятельности группы, исключающей личное присутствие. Члены такого преступного сообщества, многие из которых вербуются на законспирированных площадках в сети Интернет, выполняют строго определенные функции и имеют свою специализацию. Подобная структура преступной организации позволяет совершать сложные и масштабные преступления, делая её гибкой и невосприимчивой к разрозненным действиям правоохранителей, так как потеря практически любого звена преступной цепи быстро регенерируется, а принципы формирования преступных кибергрупп существенным образом затрудняют поиск, обнаружение и особенно процессуальную фиксацию доказательств, подтверждающих осуществление противоправной деятельности, ввиду отсутствия таких правовых способов и средств в информационно-телекоммуникационных сетях. Используемая хакерами возможность получать платежи через биткоины и иные криптовалюты значительно повысила их эффективность и общественную опасность.

Кроме того, инвестируя преступные доходы в развитие криминального бизнеса, активно обмениваясь инструментами незаконного доступа к информационным ресурсам и данными об уязвимостях, преступные кибергруппы стремительно "эволюционируют". В результате за последние несколько лет вектор хакерских атак, ранее направленных на клиентов банков, переориентировался на взлом инфраструктуры самих кредитных организаций.

Отмечены случаи мощных информационных атак, направленных одновременно против интернет-ресурсов Банка России и целого ряда ведущих банков страны ("Сбербанк России", "Альфа-Банк", "Газпромбанк", "Россельхозбанк" и др.).

Известный ученый, криминолог, лауреат Государственной премии РФ В.В. Лунеев, рассматривая основные тренды различных видов преступности и исследуя сложные мировые, региональные и российские тенденции преступности XX – начала XXI в., также обращается к глобализации и отмечает, что "современная глобализация может быть определена как универсализация социального порядка, предполагающая, с одной стороны, обеспечение соответствия множества уникальных национальных порядков неким единым стандартам, с другой – формирование наднационального социального порядка, в рамках которого такие стандарты вырабатываются и поддерживаются"[18]. Он признает, что глобализация многозначна. Существует множество ее определений, но суть ее кратко выражена Международным валютным фондом: глобализация – в возрастающей степени интенсивная интеграция рынков, товаров, услуг и капиталов[19]. Отсюда следует вывод о глобальной функции финансов в сегодняшнем развитии цивилизации и необходимости усиления контроля государства за денежными потоками и обеспечения стабильности функционирования финансового рынка Российской Федерации.

Учитывая направленность настоящей статьи, в ней не рассматриваются подробно тенденции криминальной глобализации, связанные с развитием в условиях глобализации транснациональной организованной преступности. Эти вопросы заслуживают отдельного внимания и самостоятельных научных изысканий.

Исследуя стратегии борьбы с преступностью, академик В.Н. Кудрявцев еще в начале нынешнего столетия отмечал широкое использование информационных систем как преступниками, так и правоохранительными органами, и акцентировал внимание на том, что преступники, так называемые хакеры, систематически совершают хищения денежных средств, проникая в компьютерные сети и искажая финансовую информацию. При этом он справедливо полагал важным то, чтобы постоянно совершенствующиеся методы пресечения преступлений и технические возможности правоохранительных органов не стали основой тотального контроля над населением, чреватым вмешательством в личную жизнь людей, а значит, и нарушением фундаментальных прав человека[20].

В условиях трансграничности государства не всегда могут контролировать новые информационные услуги и виды деятельности, противодействовать противоправным действиям в Интернете, учитывая неясность его правовой природы, а следовательно, эффективно бороться с киберпреступностью, объединяя усилия различных государств. Это дает основание полагать, что государственный

[18] *Лунеев В.В.* Интернационализация конституционного права в условиях глобализации // Гос. и право. 2016. № 11. С. 34.

[19] См.: *Лунеев В.В.* Преступность XX века: мировые, региональные и российские тенденции. Изд. 2-е, перераб. и доп. М., 2005. С. 125.

[20] См.: *Кудрявцев В.Н.* Стратегии борьбы с преступностью. Изд. 2-е, испр. и доп. М., 2005. С. 69, 70.

суверенитет не распространяется на информационные сети и киберпространство, представляет собой некое вненациональное саморегулирующееся сообщество пользователей. Все чаще звучат утверждения, что суверенитет государств в его традиционном понимании размывается, а государственные границы постепенно превращаются в фикцию.

Вопросы государственного суверенитета в информационных сетях и киберпространстве представляют интерес и волнуют не только практиков, но и научное сообщество, в частности специалистов международного права.

Уже более 10 лет продвигаются идеи и проекты Российской Федерации об обеспечении информационной безопасности и противодействии киберпреступности, обусловливающие необходимость подготовки акта Организации Объединенных Наций, которая, в отличие от Совета Европы, наделена универсальным мандатом, позволяющим всем государствам участвовать в выработке ответов на глобальные вызовы, согласовывать правила поведения и обязательные нормы, которыми государствам предстоит руководствоваться.

Значение Будапештской конвенции Совета Европы о преступности в сфере компьютерной информации ETS № 185 оценивается по-разному. Но важно, что противодействию киберпреступности было уделено внимание на международном уровне. В ней признается обеспокоенность тем фактом, что компьютерные сети и электронная информация могут использоваться для совершения преступлений, и что доказательства, касающиеся таких преступлений, могут сохраняться и передаваться по этим сетям.

Российская Федерация не подписала и не ратифицировала указанную Конвенцию. Достаточно жесткая позиция в отношении неприемлемости п. 32b Конвенции определяется тем, что содержащиеся в нем нормы противоречат базовым принципам международного права и связаны с недопустимостью осуществления доступа к компьютерным данным другого государства без согласия компетентных органов. Отдельные положения Конвенции, например об обеспечении неотвратимости ответственности, вопросы сотрудничества по уголовным делам, ее полузакрытый характер в отношении возможности присоединения к ней государств – нечленов Совета Европы не отвечают требованиям борьбы с современными криминальными вызовами. В период ее разработки о многих из них в сфере информационной безопасности просто не было известно.

Проблемы, связанные с реализацией указанной Конвенции, объясняются тем, что не все государства, ее подписавшие, ратифицировали данную Конвенцию[21], поскольку не имплементировали ее положения в национальное законодательство. Не в полной мере реализованы задачи международного сотрудничества, не всеми созданы контакт-центры для борьбы с киберпреступностью, которые должны оперативно реагировать на запросы других государств и оказывать помощь в расследовании киберпреступлений.

При этом следует отметить региональные инструменты сотрудничества государств[22]. В настоящий момент складывается тенденция организационно-правового взаимодействия России со многими участниками региональных объединений (ШОС, БРИКС, СНГ, Союзного государства России и Беларуси, ОДКБ) по вопросу выработки общего подхода к проблеме противодействия преступности в информационной сфере (киберпреступности). Указанный подход, как уже отмечалось, обосновывается необходимостью использования универсальной площадки ООН для разработки и принятия международного правового акта в области международного сотрудничества в данной сфере[23].

Требуется новая Конвенция – и полагаю, что это должен быть именно документ ООН,– которая исключала бы наиболее противоречивые положения Будапештской конвенции, учитывала ее положительный опыт и одновременно гарантировала уважение базисных принципов международного права, учет интересов всех государств не только в связи с появлением новых организационно-правовых механизмов пресечения противоправной деятельности в информационно-телекоммуникационных сетях, но и с необходимостью выработки унифицированных подходов решения вопросов юрисдикции, поскольку традиционные правовые подходы

[21] Проект конвенции ООН “О сотрудничестве в сфере противодействия информационной преступности” был подготовлен Россией как альтернатива Будапештской конвенции Совета Европы о компьютерных преступлениях. На сегодняшний день ее ратифицировали 53 государства и подписали еще четыре, включая все страны ЕС, а также США, Японию, Австралию и Израиль (см.: Противоботство сверхдержав. Россия предлагает изменить правила борьбы с киберпреступностью в мировом масштабе).

[22] См.: *Тропина Т.Л.* Указ. соч.

[23] Подробнее см.: *Полякова Т.А.* Стратегия национальной безопасности. Актуальные правовые проблемы теории и практики обеспечения информационной безопасности // Новые вызовы и угрозы информационной безопасности / Отв. ред. Т.А. Полякова, И.Л. Бачило, В.Б. Наумов. Сб. науч. работ. М., 2016. С. 6–23.

к юрисдикции не всегда оказываются приемлемыми (экстерриториальность, совершение преступлений (кибератак) в отношении субъектов нескольких государств, например, в области облачных технологий).

Современные тенденции и динамика преступности в информационной сфере (киберпреступности) в России

Анализ основных финансовых данных показывает, что глобальный ущерб от киберпреступности для мировой экономики оценивается экспертами в размере порядка 500 млрд долл. в год[24]. По тем же оценкам, в 2016 г. убытки компаний от организованной киберпреступности в мире составили более 650 млрд долл.[25] Специалисты Сбербанка России утверждают, что потери от атак злоумышленников в информационной сфере к 2018 г. во всем мире могут вырасти до четырех раз и составят порядка 2 трлн долл.[26] По результатам анализа в данной сфере, проведенного авторитетным аналитическим ресурсом *Cybersecurity Ventures,* к 2021 г. ущерб от преступлений в сфере информационных технологий может подняться до 6 трлн долл.[27]

Вместе с тем в докладе *The Global Risks Report 2016*[28], подготовленном по итогам Давосского экономического форума, среди угроз мировой экономике в настоящее время отмечены следующие угрозы, связанные с использованием информационных технологий: *critical information infrastructure breakdown* (выход из строя критически важной информационной инфраструктуры), *cyber-attacks* (кибератаки), *adverse consequences of technological advances* (неблагоприятное использование технологических достижений), *data fraud or theft* (кража или мошенничество с данными).

Согласно докладу Европейской полицейской организации *(Europol)* число поддержанных Европейским центром по борьбе с киберпреступностью операций против киберпреступников в 2015 г. (131) возросло по сравнению с 2014 г. (72) почти в два раза. Следует отметить, что в рамках Евросоюза самым быстрорастущим центром киберпреступности является Германия[29].

По данным Банка России, начиная с четвертого квартала 2015 г. зафиксировано 21 крупное покушение на хищение денежных средств в платежной системе Банка России на сумму более 2.87 млрд руб. При этом было остановлено транзакций на 570 млн руб. и еще 1.2 млрд руб. заблокировано на счетах банков[30].

Государственная политика в сфере противодействия киберпреступности

Правовые основы противодействия киберпреступности в настоящее время в России закреплены в названных ранее документах стратегического планирования: Стратегии национальной безопасности Российской Федерации, Доктрине информационной безопасности Российской Федерации, а также в утвержденных в 2013 г. Президентом РФ Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года.

Особо следует отметить Указ Президента РФ "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации" (Выписка) от 15 января 2013 г.[31], которым предусмотрено создание государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации – информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом. В целях исполнения Указа разработана и реализуется концепция создания указанной системы (уполномоченным органом является ФСБ России) для решения задач прогнозирования, обеспечения взаимодействия, осуществления контроля степени защищенности и установления причин компьютерных инцидентов.

Уголовно-правовая политика противодействия киберпреступности обеспечивается также системой

[24] См.: http://www.vestifinance.ru/articles/71538 (Дата обращения: 20.06.2017 г.).

[25] См.: Microsoft официально представила Windows Server 2016 // http://www.cnews.ru/news/line/2016-10-14_microsoft_ofitsialno_predstavila_windows_server (Дата обращения: 20.06.2017 г.).

[26] См.: http://www.tass.ru/ekonomika/3668896 (Дата обращения: 22.06.2017 г.).

[27] См.: 2016 Cybercrime Report // http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 (Дата обращения: 17.06.2017 г.).

[28] См.: The Global Risks Report 2016 11th Edition // http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf P. 4 (Дата обращения: 20.06.2017 г.).

[29] См.: http://www.kommersant.ru/doc/3105440 (Дата обращения: 22.06.2017 г.).

[30] См.: http://www.kommersant.ru/doc/3014098 (Дата обращения: 22.06.2017 г.).

[31] См.: Собрание законодательства РФ. 2013. № 3. Ст. 178.

уголовно-правовых запретов, содержащихся в целом ряде статей Уголовного кодекса РФ[32].

Расширение сфер применения информационных технологий, с одной стороны, упрощает и повышает рентабельность многих механизмов хозяйствования, но, с другой – предоставляет значительные возможности криминальным структурам. Связанная с этим "виртуализация" банковской деятельности обусловила широкое распространение киберпреступлений, направленных на отмывание денег, хищение финансовых средств кредитных организаций и их клиентов, несанкционированный доступ к конфиденциальной информации, нарушение функционирования банковских автоматизированных систем, уничтожение программно-информационного обеспечения и баз данных[33].

Банки и их клиенты все чаще сталкиваются с увеличением *DDoS-атак (Distributed-Denial-of-Service)*[34] и иных действий хакеров. Увеличивается количество атак на пользователей с применением так называемой социальной инженерии, когда мошенники стимулируют пользователей самостоятельно устанавливать вредоносное программное обеспечение. Прогнозируется рост числа атак на счета клиентов через атаки на сами банки. Хакеры способны захватить различные внутренние системы, включая платёжные, платформы для оплаты госуслуг, мобильной связи, интернета. Захват контроля над подобной платформой позволяет выводить деньги клиентов сразу в электронные кошельки, что значительно затрудняет возможность их дальнейшего розыска и возмещения.

К сожалению, многие банковские структуры недооценивают угрозу хакерских атак, экономя на выстраивании адекватной системы защиты информации, тем самым создавая условия для масштабных хищений денежных средств. Используемые ими стандартные системы безопасности (антивирусное программное обеспечение, межсетевые экраны и средства предотвращения утечек) зачастую устарели, неэффективны для отражения гибких многовекторных кибератак, позволяющих найти индивидуальные методы преодоления отдельных элементов защиты.

Например, членами одного организованного преступного сообщества было разработано специальное вредоносное программное обеспечение на основе широко известного компьютерного вируса *Trojan*, предназначенное для хищения пользовательской информации, относящейся к банковским системам, системам электронных денег и пластиковых карт, а также создана частная виртуальная сеть сложной конфигурации. Распространение вредоносной программы осуществлялось посредством размещения ссылок на легальных ресурсах (сайтах ведущих СМИ, популярных бухгалтерских форумах). Особенности данной программы не позволяли обнаружить её действие в памяти инфицированного компьютера с помощью традиционных антивирусных средств. После установления троянского модуля зараженный компьютер регистрировался в специальной бот-сети, управление которой осуществлялось из командного центра. Таким образом, преступники получали полный контроль над компьютером жертвы, а затем с использованием протоколов удаленного доступа осуществляли перехват пользовательской информации и проникали в корпоративные и ведомственные сети, получая доступ

---

[32] См.: Собрание законодательства РФ. 1996. № 25. Ст. 2954. В первую очередь отмечается гл. 28 УК РФ, предусматривающая ответственность за компьютерные преступления: неправомерный доступ к компьютерной информации (ст. 272); создание, использование и распространение вредоносных компьютерных программ (ст. 273), а также нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274). Кстати, следует отметить, что понятие "компьютерная информация" содержится в примечании к ст. 272 УК РФ.
Последствия от деятельности киберпреступников могут также квалифицироваться по следующим статьям УК РФ: нарушение неприкосновенности частной жизни (ст. 137); нарушение тайны переписки (ст. 138); нарушение авторских и смежных прав (ст. 146); разглашение тайны усыновления (ст. 155); кража (ст. 158); незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну (ст. 183); неправомерный оборот средств платежей (ст. 187); незаконный экспорт технологий, научно-технической информации и услуг (ст. 189); государственная измена (ст. 275); шпионаж (ст. 276); разглашение государственной тайны (ст. 283) и др. Необходимо также отметить, что в 2012 г. УК РФ дополнен нормами, предусматривающими ответственность за мошенничество, связанное с использованием платежных карт (ст. 159.3), а также в сфере компьютерной информации (ст. 159.6). Правоприменительная практика по новым специальным уголовно-правовым составам в настоящее время формируется и безусловно нуждается в анализе и обобщении. Однако следует признать, что за последний год наблюдается существенный рост преступлений, предусмотренных ст. 159.6 УК РФ, по сравнению с 2015 г. (1030), – более чем в два раза по сравнению с 2016 г. (2572).

[33] См.: *Алексеева Д.Г.* Безопасное осуществление банковской деятельности: правовые проблемы // Банковское право. 2011. № 1. С. 35–40.

[34] *DDoS-атака* – распределенная атака на отказ в обслуживании. Атака на вычислительную систему с целью вывести её из строя, т.е. создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднён (см.: http://www.dtln.ru/slovar-terminov (Дата обращения: 22.06.2017 г.)).

к ПЭВМ администраторов, главных бухгалтеров, серверам управления банкоматами.

Членами другой преступной группы хищения денежных средств производились путем подмены реквизитов совершенных транзакций в межбанковской системе взаимозачетов. После проведения на территории России операций по переводу денежных средств через банкоматы с карты на карту злоумышленники посредством электронных платежных систем с территории иностранного государства, используя вредоносное программное обеспечение и сеть Интернет, инициировали отмену данных транзакций, при этом автоматически восстанавливая баланс карты-отправителя и сохраняя баланс карты-получателя.

Кроме того, учреждения банковского сектора в целях расширения клиентской базы и увеличения доходности своей деятельности нередко выпускают на рынок электронные продукты, в том числе оснащенные мобильными сервисами, которые не обеспечены актуальными средствами защиты. В последнее время отмечено значительное увеличение числа хищений денежных средств со счетов, открытых в финансово-кредитных учреждениях, путем использования вредоносной программы в сети Интернет, которая загружается на мобильное устройство пользователя, активизируется и позволяет осуществлять любые скрытые от его владельца действия, в том числе перехватывать трафик, производить отсылку *sms*, взаимодействовать с сервером. В результате использования такой вредоносной программы происходит незаконное списание денежных средств с расчетных счетов физических лиц, подключенных к мобильным приложениям, без их ведома. При этом банк идентифицирует поступающие ему команды как направленные распорядителем счета и выполняет свои обязательства по переводу денежных средств. В возмещении денежных средств пострадавшим гражданам банки отказывают, ссылаясь на положения Федерального закона "О национальной платежной системе" от 27 июня 2011 г.,[35] в соответствии с которыми оператор по переводу денежных средств (банк) обязан возместить клиенту сумму операции, совершенной без согласия клиента, но только после получения от него соответствующего уведомления, направленного не позднее дня, следующего за днем информирования банком о совершенной операции.

Появлению на рынке банковских услуг подобных продуктов, совершению иных киберпреступлений должны противостоять обновляемые государственные стандарты информационной безопасности, имеющие не рекомендательный (как в настоящее время), а императивный характер. Исключительно важно формирование в обществе культуры кибербезопасности наряду с совершенствованием законодательства в данной сфере.

Неосведомленность банков о процессах реализации, типологии и целях информационных атак, об актуальных методах реагирования на инциденты информационной безопасности, а также отсутствие обмена разведывательной информацией в финансовом секторе приводят к ситуации, при которой даже крупные кредитные учреждения, несмотря на использование передовых решений в области кибербезопасности, продолжают оставаться в роли "догоняющего".

В 2015 г. на базе Банка России создан Центр мониторинга и реагирования на компьютерные атаки в финансово-кредитной сфере, задачами которого являются в том числе информирование банковского сообщества о тактике действий злоумышленников, предоставление индикаторов для выявления попыток компрометации корпоративной сети и рекомендаций, которые помогут противостоять действиям преступников.

В то же время со стороны значительного количества представителей банковского сообщества сотрудничество в этой области носит в основном декларативный характер и не переходит в практическую плоскость, что негативно сказывается на эффективности функционирования всего механизма в целом.

Только за 2015 г. ущерб, причинённый российской экономике деятельностью киберпреступников, по оценкам экспертов, составил не менее 203.3 млрд руб. (это более 3.335 млрд долл.), что соответствует 0.25% от ВВП. Прямой финансовый ущерб составил 123.5 млрд руб. (0.15% от ВВП России), а затраты на ликвидацию последствий – более 79.8 млрд руб. (0.1% от ВВП России)[36]. Все

[35] См.: Собрание законодательства РФ. 2011. № 27. Ст. 3872.

[36] См.: http://www.kommersant.ru/doc/2962746 (Дата обращения: 20.06.2017 г.).
Вместе с тем, по данным Центробанка России, объем несанкционированных операций по переводу денежных средств по итогам 2016 г. составил 2.98 млрд руб. (в 2015 г.– 4.95 млрд руб.). При этом в 2016 г. Банком России выявлено девять случаев покушения на хищение денежных средств с корреспондентских счетов кредитных организаций, открытых в платежной системе Банка России, на сумму 2.18 млрд руб., по которым удалось предотвратить несанкционированные переводы денежных средств на сумму 0.68 млрд руб. (см.: Годовой отчет о деятельности Банка России за 2016 г. С. 181 // Официальный сайт Банка России // http://www.cbr.ru/publ/God/ar_2016.pdf (Дата обращения: 20.06.2017 г.)).

это требует решительных мер противодействия преступникам.

Председатель Банка России Э.С. Набиуллина, выступая 13 июля 2017 г. на XXVI Международном финансовом конгрессе, заявила о том, что Регтех (регулирование технологий) станет одной из приоритетных задач Банка России на ближайшие пять лет. По ее словам, дигитализация в финансовой сфере – появление финтех-компаний, внедрение *big data*, работа с открытыми интерфейсами, клауд-компьютеринг (облачные технологии), использование сложных математических моделей в системе управления рисками, системе принятия кредитных решений и т.д. – создает значительный объем рисков, которые будут иметь не финансовую, а именно технологическую природу. "Наша задача – выработать единые стандарты работы с базами данных, требования к качеству данных, к применяющимся моделям, к аутсорсингу данных и информационной безопасности", – подчеркнула она[37].

В банковском секторе вопросы обеспечения информационной безопасности являются первоочередными, при этом находятся в нескольких плоскостях. Так, специалистами отмечается ряд проблем организационного плана внутри банков (некачественно сформулированы процессы управления криптографическими ключами, неподготовленность персонала к воздействию извне, экономия на средствах безопасности, плохое сегментирование Сети на сетевом уровне и отсутствие шифрования, нерегулярное сканирование инфраструктуры на наличие уязвимостей, отсутствие риск-ориентированного подхода информационной безопасности и др.)[38]. Другой блок вопросов – культура информационной безопасности самих клиентов: передача и сообщение посторонним лицам сведений о пароле, данных о карте, переход на поддельные сайты, размещение в свободном доступе паспортных данных, слабая забота об антивирусной защите[39].

Сегодня финансово-кредитная сфера, особенно в условиях развития цифровой экономики, по сути, является кровеносной системой государства. Именно поэтому значительная часть новых вызовов и угроз информационной безопасности государства направлена на подрыв финансовой стабильности последнего. В этой связи все более очевидна роль правового регулирования и необходимость его совершенствования.

Как отмечает первый заместитель Председателя Банка России Г.И. Лунтовский, "по данным, полученным из форм обязательной отчётности об инцидентах информационной безопасности, официально предоставляемых кредитными организациями в Банк России, и данным, полученным в рамках информационного обмена, организованного Центром мониторинга и реагирования на компьютерные атаки в финансовой сфере (FinCERT) Банка России, объём несанкционированных операций со счетами юридических лиц по итогам 2016 года составил 1,9 млрд рублей"[40].

Полагаем, что в информационной сфере, учитывая сложность технологических и технических процессов, важную роль играют экспертно-аналитические оценки в сфере обеспечения кибербезопасности[41] и общие правила поведения.

Важным шагом на пути решения этой задачи стал впервые введенный в Российской Федерации приказом Федерального агентства по техническим стандартам и метрологии (Росстандарт) от 8 августа 2017 г. № 822-ст[42] национальный стандарт РФ – ГОСТ Р 57580.1–2017 "Безопасность финансовых (банковских) операций. Защита

---

[37] См.: http://cbr.ru/press/event/?id=1211 (Дата обращения: 22.06.2017 г.).

[38] См.: *Сычев А.М., Ревенков П.В., Дудка А.Б.* Безопасность электронного банкинга. М., 2017. С. 307.

[39] См.: там же. С. 308.

[40] "Для сравнения, в 2015 году аналогичный показатель составил 3.8 млрд рублей. Объём несанкционированных операций с использованием платёжных карт за 2016 год составил порядка 1.08 млрд рублей. В 2015 году – около 1.15 млрд рублей. При этом в 2016 году Банк России выявил 9 покушений на хищение денежных средств с корреспондентских счетов кредитных организаций, открытых в платёжной системе Банка России, на сумму порядка 2.18 млрд рублей. Из них на сумму порядка 1.5 млрд рублей наступила окончательность перевода денежных средств. То есть эти деньги были похищены" (см.: Вектор 2017 года // http://journal.ib-bank.ru/post/529) (Дата обращения: 14.08.2017 г.)).

[41] В частности, эксперты *IB-Group* отметили значительный рост атак на пользователей устройств на операционной системе (ОС) *Android*: объем средств, украденных с банковских счетов в Российской Федерации с помощью вирусов под мобильные устройства на *Android*, за год вырос почти в шесть раз и составил 348.6 млн руб. Ежедневно 350 пользователей гаджетов на этой ОС теряют в среднем по 4 тыс. руб. от действий кибермошенников. Прогнозируется появление специальных программ-шифровальщиков для облачных сервисов. Хакеры в первой половине 2017 г. чаще атаковали промышленные объекты, прежде всего энергетические компании, объекты транспортной инфраструктуры, аэропорты, химические производства, водоочистительные узлы (см.: Киберпреступники в России заработали за год 5.5 млрд рублей // http://tass.ru/ekonomika/3704572http://tass.ru/ekonomika/3704572 (Дата обращения: 15.06.2017 г.)).

[42] См.: http://www.cbr.ru/credit/Gubzi_docs/882-ct.pdf (Дата обращения: 14.08.2017 г.).

информации финансовых организаций. Базовый набор организационных и технических мер". Стандарт предлагает комплексный подход к планированию, реализации, контролю и совершенствованию процесса защиты информации в финансовых организациях, содержит требования к организации всех основных процессов информационной защиты, включая противодействие вредоносному коду, утечкам информации, а также нарушению целостности информационной инфраструктуры. Банк России отмечает, что переход на новые стандарты позволит финансовым организациям повысить уровень защищенности от киберпреступлений, обеспечить стабильное и бесперебойное обслуживание клиентов[43].

Криптовалюта. Проблемы правового регулирования

Одной из мировых политико-правовых проблем становится правовой режим криптовалют, поскольку последние не являются принадлежностью государственных экономик, несут угрозу исключительному конституционному полномочию государства в области финансового регулирования, денежной эмиссии (ст. 71 Конституции РФ). Кроме названных рисков криптовалюты не администрируются налоговыми и таможенными органами, активно используются для анонимных расчетов, в том числе для финансирования терроризма, экстремизма, нелегальной торговли оружием, наркотиками, а также для вывода за рубеж и отмывания денег, в том числе полученных от прямой криминальной деятельности вроде кибершантажа (*ransomware*).

В настоящее время вопрос правомерности использования различных суррогатов денежных средств (криптовалюта) является дискуссионным, требующим выработки научно обоснованного подхода к правовому регулированию и легитимности криптовалюты. Представляется особо актуальным выработка научно обоснованного определения предмета правового регулирования, понятийного аппарата и методологии исследования.

Криптовалюта – это имеющая номинальную рыночную стоимость в денежных знаках различных государств и используемая для обмена на товары, услуги, для заключения сделок и в иных целях единица зашифрованной криптографическим методом информации, создаваемая юридическими или физическими лицами в одноранговых, децентрализованных (пиринговых) компьютерных платежных системах, основанных на технологии блокчейн.

В современной мировой экономике наиболее распространенными видами криптовалют в мире являются биткоин *(bitcoin)* и эфир *(ether)*. Создан рынок биржевых торгов практически всеми известными криптовалютами. По объему торгов лидирующие места занимают китайские биржи *BTC China, OKcoin* и *Huobi* или *Bityes*. В условиях государственного инвестирования развивается японская *Bitflyer*. В десятку крупнейших в мире по объему торгов входит американский *Poloniex*. Известны европейские биржи *EXMO, Spectrocoin* и др.

Иллюстрируя сказанное конкретными примерами из зарубежного опыта, можно отметить различные наметившиеся тенденции государственной политики в отношении криптовалют. Так, с 2013 г. в Сингапуре вопрос хождения криптовалюты – решение компаний, при этом должна устанавливаться личность. В таких государствах, как Бангладеш, Китай, Кыргызстан, ввели полный или частичный запрет на использование криптовалюты на своей территории. Эквадор ввел собственную криптовалюту в обращение, запретив при этом иные виды криптовалют.

В США криптовалюта получила статус виртуальной валюты и денежного средства. Криптовалюта, а именно биткоин, также имеет легальный статус в том или ином виде в Финляндии, Норвегии, Канаде, Испании, Люксембурге, Германии, Израиле и других государствах. Кроме того, можно выделить ряд государств, которые пока не определились в отношении приемлемости криптовалюты в качестве денежного средства (Бразилия, Греция, Дания, Индия, Иордания, Индонезия, Италия).

Статья 27 Федерального закона "О Центральном банке Российской Федерации (Банке России)" от 10 июля 2002 г. (в ред. от 18 июля 2017 г.) устанавливает: "Официальной денежной единицей (валютой) Российской Федерации является рубль. Введение на территории Российской Федерации других денежных единиц и выпуск денежных суррогатов запрещаются"[44].

Сегодня на территории Российской Федерации ограничивается обращение криптовалют, что напрямую связано с отсутствием законодательного регулирования. Так, Банк России предостерегает граждан и юридических лиц, прежде

[43] См.: http://www.cbr.ru/Press/event/?id=1274 (Дата обращения: 14.08.2017 г.).

[44] http://www.consultant.ru/document/cons_doc_LAW_37570/8582f82f1cd3de663ddfdf7b65e825f9145958f8/ (Дата обращения: 22.06.2017 г.).

всего кредитные организации и некредитные финансовые организации, от использования "виртуальных валют" для их обмена на товары (работы, услуги) или на денежные средства в рублях и в иностранной валюте[45].

По мнению Федеральной налоговой службы России, операции, связанные с приобретением или реализацией криптовалют с использованием валютных ценностей (иностранной валюты и внешних ценных бумаг) и (или) валюты Российской Федерации, являются валютными операциями, порядок проведения которых установлен Федеральным законом "О валютном регулировании и валютном контроле" от 10 декабря 2003 г. № 173-ФЗ[46], и должны осуществляться через счета резидентов, открытые в уполномоченных банках[47].

Первый заместитель Председателя Правительства РФ И. И. Шувалов подтвердил факт обсуждения перспективы криптовалют в России на правительственном уровне: "Мы обсуждали этот вопрос в рамках рабочей группы по блокчейну, говорили о будущем этого сектора в России, учитывая, что он так быстро развивается в мире. Но пока это дискуссия, конкретных проектов еще нет. Необходимо подготовить соответствующее законодательство и его регулирование"[48].

Судебная практика по этой проблеме только формируется. Так, Шестой арбитражный апелляционный суд (г. Хабаровск) в постановлении от 28 июня 2016 г. по делу № А73-6112/2015 оценил критически, как не подтверждающий факт оплаты денежных средств ответчику возврат полученных им по договору займа денежных средств, но в виде не наличных 5 млн долл., а криптовалюты (виртуальных денег)[49].

В свою очередь, Арбитражный суд Вологодской области определением от 15 августа 2016 г. по делу № А13-15648/2015 удовлетворил требование финансового управляющего по делу о несостоятельности (банкротстве) к индивидуальному предпринимателю о предоставлении сведений об остатках электронных денежных средств и о переводах электронных денежных средств за трехлетний период, предшествующий дате подачи заявления о признании гражданина банкротом. В качестве электронных денежных средств были указаны: *PayPal, Яндекс.деньги, Деньги@mail.ru, Webmoney, QIWI,* а также различные криптовалюты: *Bitcoin, Litecoin*[50].

Таким образом, подходы к пониманию правовой сути криптовалюты отличаются разнообразием, не выработан универсальный правовой механизм для решения вопросов идентификации субъектов при совершении операций с криптовалютой, отслеживания таких операций, их администрирования.

Следует отметить, что сам процесс майнинга *(mining)* – получения криптовалют зачастую носит криминальный характер, поскольку это очень большая нагрузка, в том числе на процессорные мощности, что стимулирует широкое распространение вирусов для скрытого майнинга биткоинов. Советник Президента РФ по Интернету Г. Клименко заявил, что 20–30% всех компьютеров в России заражено вирусом для майнинга биткоинов, а установка вирусов для майнинга криптовалют – это сейчас самый прибыльный для хакеров бизнес[51]. Его озабоченность в целом разделяют интернет-омбудсмен Дм. Мариничев, представители "Лаборатории Касперского" и др.[52]

---

[45] Банк России указывает на анонимный характер деятельности по выпуску "виртуальных валют" и предупреждает, что использование субъектами биткоин с целью предоставления услуг российскими юридическими лицами по обмену "виртуальных валют" на рубли и иностранную валюту, а также на товары (работы, услуги) может быть расценено как незаконные действия по легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Ответственность в данном случае предусмотрена в соответствии с Законом о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (см.: Федеральный закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 7 августа 2001 г.; Информация Банка России «Об использовании при совершении сделок "виртуальных валют", в частности Биткойн» от 27 января 2014 г. // Вестник Банка России. 2014. № 11)). Схожую позицию занял Росфинмониторинг. В информационном сообщении "Об использовании криптовалют" было указано, что использование криптовалют при совершении сделок является основанием для рассмотрения вопроса об отнесении таких сделок (операций) к сделкам (операциям), направленным на легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма (см.: http://fedsfm.ru/ (По сост. на 06.02.2014 г.) // СПС "КонсультантПлюс").

[46] См.: http://www.consultant.ru/document/cons_doc_LAW_45458/ (Дата обращения: 14.08.2017 г.).

[47] См.: Письмо ФНС России от 3 октября 2016 г. № ОА-18-17/1027 // http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=QUEST&n=162766#0 (Дата обращения: 14.08.2017 г.).

[48] http://www.rbc.ru/technology_and_media/10/08/2017/598ad1909a79476bbc6c5f96?from=main (Дата обращения: 14.08.2017 г.).

[49] См.: http://sudact.ru/arbitral/doc/6cftkId4klLj/ (Дата обращения: 22.06.2017 г.).

[50] См.: http://sudact.ru/arbitral/doc/t4TwXZuzGdL5/ (Дата обращения: 22.06.2017 г.).

[51] См.: http://www.rbc.ru/technology_and_media/24/07/2017/5975d00b9a7947dce3612e8d (Дата обращения: 11.08.2017 г.).

[52] См.: там же.

Не менее сложная задача – хранение и защита криптовалют. Места обмена и владельцы последних систематически подвергаются хакерским атакам с причинением огромного ущерба. Так, в результате взлома гонконгской криптовалютной биржи *Bitfinex* ущерб ее участникам составил около 70 млн долл.[53] Крупнейшая в Южной Корее биржа криптовалют *Bithumb* подверглась хакерской атаке – со счетов клиентов похищено порядка 900 тыс. долл.

25 июля 2017 г. в Греции по требованию министерства юстиции США задержали администратора биржи *BTC-E*, подозреваемого во взломе японской биржи-конкурента *Mt. Gox*, а также в отмывании преступных денег в размере 4 млрд долл., способствовании незаконному обороту наркотиков и ведении специальной клиентской базы преступников. По данным доклада, представленного в этом году на конференции по кибербезопасности *Black Hat USA 2017*, до 95% средств, полученных вирусами-вымогателями, были затем отмыты через *BTC-E*[54].

В 2016 г. проект *The DAO*, среди учредителей которого был создатель *Ethereum* канадский программист В. Бутерин, впервые в истории смог привлечь для первичного размещения криптовалюты с помощью технологии блокчейн около 152 млн долл., но вскоре после успешного краудфандинга (*crowdfunding*)[55] подвергся хакерской атаке, в результате которой была украдена почти треть собранных средств[56].

Приведенные факты со всей очевидностью свидетельствуют в пользу того, что правовое регулирование киберпространства должно осуществляться только на основе консенсуса и учета мнений и возможностей специалистов в области права, информационных технологий и пользователей компьютерных сетей (в данном случае представителей банковского сообщества, Банка России).

Внедряемые технологии и предоставляемые клиентам электронные сервисы должны быть тщательно протестированы и отвечать всем требованиям безопасности. Представляется, что обязательное соблюдение стандартов кредитно-финансовым учреждением необходимо закрепить на нормативно-правовом уровне и увязать с процедурой выдачи лицензии Банком России. Данное положение есть важнейшее требование обеспечения безопасности в такой стратегически важной сфере, как финансово-кредитная деятельность.

Дальнейшее совершенствование законодательной базы противодействия киберугрозам в данной сфере возможно как по пути усиления уголовной ответственности преступников, что послужит дополнительной контрмотивацией для людей, вовлекаемых в преступную индустрию, так и в направлении применения наказаний в отношении компаний, безответственно относящихся к обеспечению информационной безопасности или вовлеченных в криминальные инциденты, связанные с уязвимостями применяемых технологий, действиями инсайдеров внутри кредитных организаций и т.п.

В этой связи представляется необходимым введение гражданско-правовой и административной ответственности юридических лиц, осуществляющих деятельность в финансово-кредитной сфере, за необеспечение сохранности тайны об операциях, счетах и вкладах своих клиентов. В частности, целесообразно рассмотреть вопрос о дополнении гл. 15 КоАП РФ нормой об ответственности кредитной организации, предоставляющей банковские услуги посредством информационно-телекоммуникационных сетей (в том числе в сети Интернет), за неприменение организационных мер, технических, программно-аппаратных средств защиты информации, повлекшее несанкционированное распространение, использование, уничтожение, блокирование, модификацию или копирование сведений, составляющих банковскую тайну, что влечет наложение административного штрафа на юридических лиц в размере от десяти миллионов до шестидесяти миллионов рублей.

Одним из актуальных организационно-правовых вопросов противодействия киберпреступности остается установление способов вывода денежных средств, похищенных, в частности, с корреспондентских счетов кредитных организаций. Банки-получатели денежных средств, перечисленных со счетов иных банков, должны иметь возможность фиксировать использование в таких операциях счетов фирм-однодневок. Особенно,

---

[53] См.: http://bits.media/news/birzha-bitfinex-vzlomana-vse-operatsii-ostanovleny/ (Дата обращения: 11.08.2017 г.).

[54] См.: http://forklog.com/95-dohodov-vymogatelej-bitkoinov-obnalichivalos-cherez-birzhu-btc-e/ (Дата обращения: 11.08.2017 г.).

[55] *Краудфа́ндинг* (народное финансирование, от англ. *crowdfunding, crowd* – толпа, *funding* – финансирование) – это коллективное сотрудничество людей, которые добровольно объединяют свои деньги или другие ресурсы вместе, как правило, через Интернет, чтобы поддержать усилия других людей или организаций (см.: http://dic.academic.ru/dic.nsf/ruwiki/1532274 (Дата обращения: 11.08.2017 г.)).

[56] См.: http://www.rbc.ru/finances/26/07/2017/5978309f9a7947ab4451167d (Дата обращения: 11.08.2017 г.).

если подобная финансовая активность имеет разовый характер и не предваряется соответствующей банковской и деловой активностью.

Эффективным средством борьбы с использованием фирм-однодневок может стать законодательное урегулирование вопросов блокировки банками сомнительных транзакций, включая определение механизма и сроков указанных ограничений, а также мер ответственности за их необоснованное применение.

Для повышения результативности оперативно-розыскной деятельности организациям банковского сектора необходимо принять действенные меры организационно-технического и аппаратно-программного характера по установлению лиц, обналичивающих похищенные денежные средства в банкоматах, что позволит правоохранительным органам выявлять заказчиков этих незаконных операций, а в дальнейшем – членов преступной группы, осуществляющих распределенные функции, объединенных общим корыстным мотивом. Целесообразно оборудовать банкоматы средствами физической фиксации клиентов, таймерами частоты операций, предусмотреть ограничение сумм разовой выдачи денежных средств, передачу сигналов о массовом (более 10 операций) снятии клиентами предельных сумм в течение короткого промежутка времени.

Анализ правоприменительной практики характеризуется постоянным расширением криминальной активности в области банковских, платежных электронных сервисов и диктует необходимость консолидации усилий всех заинтересованных субъектов на основе формирования единого центра борьбы с киберугрозами и мониторинга подозрительных операций на базе уполномоченного государственного органа, который позволит объединить все кредитные организации в одну сеть для противодействия попыткам взлома банковских систем. В основу работы центра может быть положен опыт ПАО “Сбербанк России”, использующего сервис, позволяющий в режиме онлайн отслеживать и отражать атаки на банк. Полезно будет привлечь к этой работе операторов сотовой связи, провайдеров сети Интернет. Руководство деятельностью центра и координацию всех мероприятий целесообразно поручить Банку России. Важнейшими звеньями этой системы являются ФСБ России, МВД России, ФСТЭК России, а также аккредитованные компании, осуществляющие деятельность в сфере информационной безопасности.

Одно из ключевых направлений обеспечения информационной безопасности – усиление государственно-частного партнерства и развитие соответствующих регионально-ориентированных программ с учетом экономической заинтересованности кредитных организаций в повышении уровня защищенности их информационных ресурсов.

Оценивая реалии и перспективы развития системы обеспечения информационной безопасности, представляется необходимым применение подходов, аналогичных тем, которые избраны в целях противодействия иным угрозам системного характера, например таким, как коррупция.

Полагаю, что указанные выше проблемы обосновывают целесообразность разработки национального плана по борьбе с киберпреступностью, который позволит объединить усилия заинтересованных органов государственной власти, участников бизнеса и банковского сектора для активизации деятельности в данной сфере не только в Российской Федерации, но и в Организации Объединенных Наций.