Краснодарский университет МВД России

З. И. Хисамова

МЕЖДУНАРОДНЫЙ ОПЫТ УГОЛОВНО-ПРАВОВОГО ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ЦИФРОВОЙ ЭКОНОМИКИ

Краснодар
2018

УДК 343.3/.7
ББК 67.408
Х49

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Рецензенты:

В. И. Тюнин, доктор юридических наук, профессор (Санкт-Петербургский университет МВД России);

М. С. Репкин, кандидат юридических наук (Следственное управление Следственного комитета Российской Федерации по Краснодарскому краю).

Хисамова З. И.

Х49 Международный опыт уголовно-правового противодействия преступлениям в сфере цифровой экономики / З. И. Хисамова. – Краснодар : Краснодарский университет МВД России. – 2018. – 116 с.

ISBN 978-5-9266-1356-5

В монографии представлен сравнительно-правовой анализ международного уголовного законодательства об ответственности за преступления, совершаемые с использованием информационно-телекоммуникационных технологий, анализируется опыт уголовно-правового противодействия IT-преступлениям в странах Западной Европы, США, Аравийского полуострова, Юго-Восточной Азии и странах СНГ. Предлагаются пути имплементации и рецепции передового зарубежного опыта в указанной сфере отечественным уголовным законодательством.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 343.3/.7
ББК 67.408

ISBN 978-5-9266-1356-5

Введение

Мир находится на пороге новой цифровой эры. Цифровая экономика становится все более важной частью глобальной экономики, открывая новые возможности для бизнеса и устойчивого развития всего мирового сообщества. Цифровизация сегодня касается не только технологического сектора и цифровых компаний, но и производственных цепочек в самых разных секторах глобальной экономики. Благодаря цифровой экономике появились возможности и инструменты для преодоления ряда хронических проблем, сдерживающих процесс развития.

В целях реализации Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента РФ от 9 мая 2017 г. № 203, в июле прошлого года была принята программа «Цифровая экономика Российской Федерации».

Указанная программа «направлена на создание условий для развития общества знаний в Российской Федерации, повышение благосостояния и качества жизни граждан нашей страны путем повышения доступности и качества товаров и услуг, произведенных в цифровой экономике с использованием современных цифровых технологий, повышения степени информированности и цифровой грамотности, улучшения доступности и качества государственных услуг для граждан, а также безопасности как внутри страны, так и за ее пределами»[1].

Переход к цифровой экономике сопряжен с необходимостью решения целого ряда политических, экономических и социальных задач в целях минимизации возможных негативных последствий для общества. Особую роль в указанном процессе занимает создание эффективной системы правового регулирования цифровой экономики, в том числе и системы противодействия преступлениям в указанной сфере.

На совещании по вопросу использования цифровых технологий, состоявшемся 10 октября 2017 г., Президент РФ отметил проблемы, связанные с использованием IT-технологий: «…это возможность отмывания капиталов, полученных преступным путем, ухода от налогов и даже финансирование терроризма и, конечно, распространение мошеннических схем, жертвами которых могут, безусловно, стать рядовые граждане. <...> Нам нужно, опираясь на международный опыт, вы-

[1] Об утверждении программы «Цифровая экономика Российской Федерации»: распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р. Доступ из справочной правовой системы «КонсультантПлюс».

строить такую регуляторную среду, которая позволит систематизировать отношения в этой сфере, защитить, безусловно, интересы граждан, бизнеса, государства, дать правовые гарантии для работы с инновационными финансовыми инструментами»[1].

Несмотря на то, что скорость цифрового преобразования в разных странах различна, для мирового сообщества становится очевидной необходимость модернизации действующей системы мер противодействия посягательствам, связанным с использованием IT-технологий. Ввиду этого в рамках настоящего исследования нами предпринята попытка проанализировать мировые тенденции противодействия посягательствам в IT-сфере; оценить состояние уголовного законодательства стран, являющихся мировыми лидерами по уровню развития цифровой экономики; провести компаративное исследование отечественного уголовного законодательства в рассматриваемой сфере.

Необходимость обращения к зарубежному опыту предопределена также тем, что анализ результатов законотворческой деятельности в других странах позволяет представить отечественную правовую систему в соотношении с правовыми системами иностранных государств. При сравнительно-правовом исследовании удается достигнуть исключительного отображения целого ряда признаков и характерных черт, которым зачастую не придается особого значения. Особенно это касается правоотношений в сфере цифровой экономики, которая возникла в последние десятилетия и, соответственно, не имеет исторического базиса, на котором бы строилась современная система уголовно-правовой защиты.

В настоящем исследовании автор обратился к мировому опыту противодействия преступлениям в IT-сфере, уделив особое внимание странам, занимающим передовые позиции по развитию цифровой экономики.

Монография содержит анализ нормативных актов, стратегий и перспективных планов развития цифровой экономики в мире, материалов правоприменительной практики, научных исследований, публикаций средств массовой информации, контента информационного пространства сети Интернет.

[1] Совещание по вопросу использования цифровых технологий в финансовой сфере. URL: http://www.kremlin.ru/events/president/news/55813

Глава 1. Международно-правовые основы регулирования цифровой экономики и обеспечения информационной безопасности

1.1. Цифровая экономика как сегмент экономики и объект уголовно-правового регулирования

Цифровая экономика является одним из главных двигателей роста и развития мировой экономики, открывая безграничные возможности для бизнеса и государственного сектора. Информационные и телекоммуникационные технологии оказывают существенное влияние на развитие традиционных отраслей экономики. Внедрение цифровых технологий в глобальные производственные процессы в различных отраслях оказывает повсеместное влияние на характер производства.

«Цифровая экономика сегодня – это не отдельная отрасль, по сути – это уклад жизни, новая основа для развития системы государственного управления, экономики, бизнеса, социальной сферы, всего общества. И, конечно, формирование цифровой экономики – это вопрос национальной безопасности и независимости России, конкурентности отечественных компаний, позиций страны на мировой арене на долгосрочную перспективу, по сути на десятилетия вперед»[1].

«Само понятие «цифровизация» свидетельствует о новой стадии совершенствования управления производством товаров и услуг и самого производства на основе «сквозного» применения современных ИТ, начиная от Интернета вещей и заканчивая технологиями электронного правительства»[2].

Как отмечает Н. Никифоров, «цифровая экономика – это такой экономический уклад, в котором данные представляют собой самостоятельную экономическую сущность… цифровая экономика – это экономика данных. Цифровая экономика – про то, как мы создаем, передаем, собираем, храним данные, защищаем их, а самое главное – анализируем и на основе этих данных принимаем такие решения, которые

[1] Выступление Президента РФ В.В. Путина // Материалы заседания Совета по стратегическому развитию и приоритетным проектам 5 июля 2017 г., Московская область, Ново-Огарево // Официальный сайт Президента РФ.

[2] Паньшин Б. Цифровая экономика: особенности и тенденции развития // Наука и инновации. 2016. № 3(157). С. 17–20.

делают нашу экономику эффективнее, управление – более эффективным, а значит, и повышают качество жизни»[1].

По оценкам экспертов, цифровая экономика несет в себе огромные изменения для более чем 50% различных отраслей. Сегодня разные страны мира все активнее переходят к формированию новой индустрии – Интернета вещей.

Вместе с тем, несмотря на широкое и повсеместное использование термина «цифровая экономика», единого общепринятого определения для него нет.

Впервые данный термин был употреблен в работе[2] Н. Негропонте в 1995 г., посвященной цифровизации, где виртуальная реальность и ее составляющие рассматривались в антитезе с движением атомов и понятиями сырья, веса и производства.

Мировая цифровизация набирает невиданные обороты. В исследовании Digital Evolution Index[3], проведенном учеными университета Тафтса в сотрудничестве с MasterCard Inc. на основе анализа 170 индикаторов, в том числе качества и состояния законодательства, отмечается, что несколько скандинавских стран, Швейцария и Южная Корея опережают США и Японию по уровню цифрового развития экономики (рис. 1). В топ-10 вошли такие страны, как Норвегия, Швеция, Швейцария, Дания, Финляндия, Сингапур, Южная Корея, Великобритания, Гонконг и США. Наша страна наряду с Китаем, Малайзией, Боливией, Кенией и Турцией была отмечена в числе стран, продемонстрировавших наибольший прогресс в информационно-технологическом развитии[4].

---

[1] Выступление Минкомсвязи Н. Никифорова // Материалы заседания Совета по стратегическому развитию и приоритетным проектам 5 июля 2017 г., Московская область, Ново-Огарево // Официальный сайт Президента РФ.

[2] Negroponte N. (1995). Being Digital. Knopf. Paperback edition, 1996, Vintage Books.

[3] Bhaskar Chakravorti and Ravi Shankar Chaturvedi Digital planet 2017. How competitiveness and trust in digital economies vary across the world. The Fletcher School, Tufts University, July, 2017.

[4] Самые цифровые страны мира. URL: https://hbr-russia.ru

Рис. 1. Темпы развития цифровой экономики в мире
(по данным Digital Evolution Index 2017)

Признанием значимости роли цифровой экономики является ежегодное увеличение ее доли в ВВП государств. По данным Бостонской консалтинговой группы (The Boston Consulting Group), доля цифровой экономики в ВВП Российской Федерации составляет 2,8%, или 75 млрд долл. Большая часть (63 млрд долл.) приходится на сферу потребления (интернет-торговля, услуги, поиск онлайн с целью покупки офлайн). На текущий момент по уровню развития цифровой экономики наша страна находится на 39-м месте (рис. 2), и ее отставание от стран – лидеров цифрового развития оценивается в 5–8 лет[1].

[1] Россия онлайн? Догнать нельзя отстать. URL: http://image-src.bcg.com/Images/BCG-Russia-Online_tcm27-152058.pdf

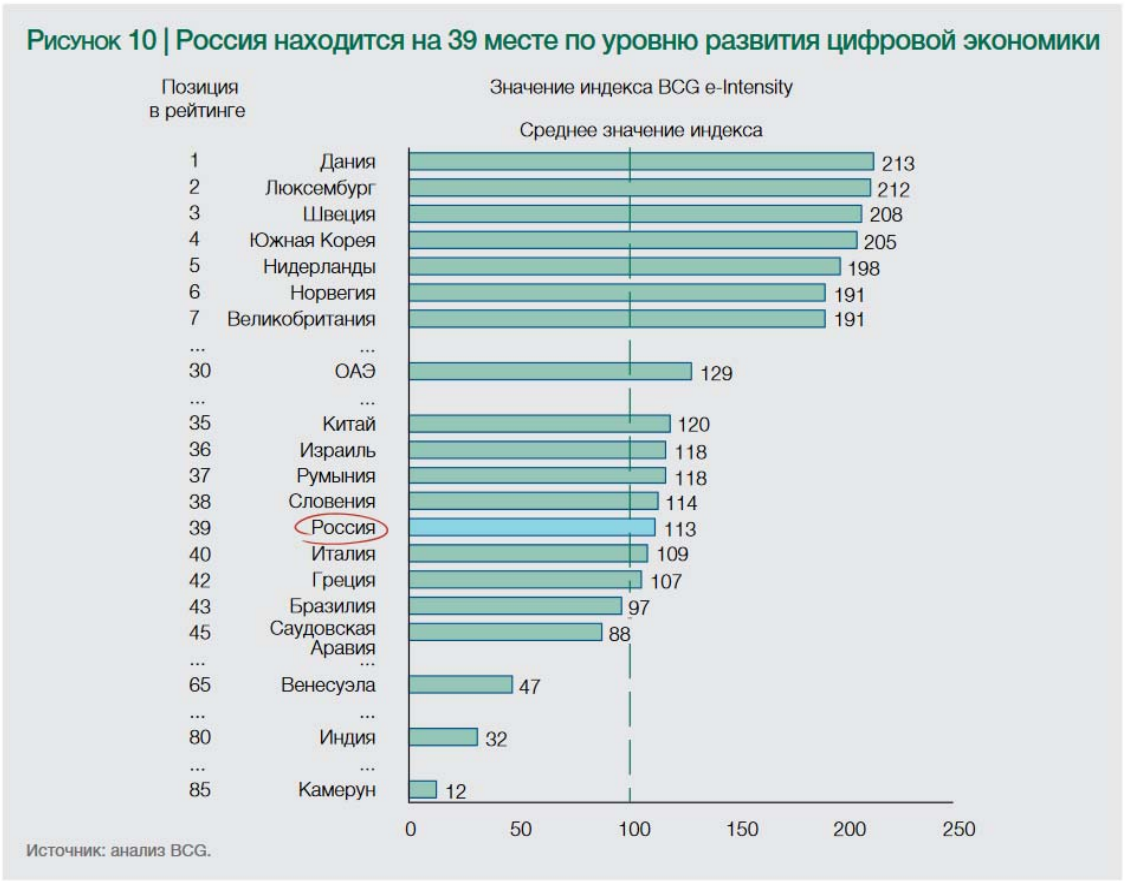


Рис. 2. Рейтинг стран по уровню развития цифровой экономики

Вместе с тем, согласно исследованию «Глобальный индекс кибербезопасности» (Global Cybersecurity Index)[1], которое ежегодно проводится Международным союзом электросвязи (ITU), в вопросах обеспечения информационной безопасности отставание нашей страны не столь значительно.

Аналитики Бостонской консалтинговой группы видят три сценария дальнейшей цифровизации России[2].

1. *Без адресного стимулирования цифровой составляющей экономики (венесуэльская модель).* При таком сценарии развития событий доля цифровой экономики в ВВП будет оставаться неизменной, что в конечном счете приведет к разрыву от передовых цифровых стран на 15–20 лет.

2. *Сценарий умеренного роста (ближне-восточная модель)*, при котором предполагается полномасштабное внедрение уже начатых

[1] URL: http://itu.int

[2] Россия онлайн? Догнать нельзя отстать. URL: http://image-src.bcg.com/Images/BCG-Russia-Online_tcm27-152058.pdf

инициатив, в частности, в области развития и охвата государственных сервисов (госуслуги, медицина, образование) и оптимизации механизмов управления без их дублирования в офлайн. Указанный сценарий представляется также недостаточным при сохранении и наращивании текущих темпов цифровизации странами-лидерами и азиатскими странами, однако он позволит удержать текущие позиции и создаст добавленную стоимость для экономики в размере 0,8–1,2 трлн руб. в год, а сама цифровая экономика достигнет 3% ВВП.

3. *Сценарий интенсивной цифровизации (азиатская модель)*, в рамках которого предполагается комплексное использование возможностей цифровой экономики и расширение ее перспективных направлений (Интернет вещей, большие данные, развитие IT-продуктов и сервисов с высоким экспортным потенциалом).

Реализация этого трудоемкого и фундаментального сценария потребует полноценной цифровой трансформации экономики страны. Однако в современных условиях данный путь является единственно верным и позволит сохранить конкурентоспособность отечественной экономики на мировом уровне. Цифровизация позволит диверсифицировать российскую экономику и раскрыть ее потенциал не только в сырьевом секторе, но и во многих других.

Для реализации столь масштабных трансформаций и преобразований необходимо тесное взаимодействие и формирование законодательной основы, где каждому участнику системы отведена своя значимая роль. При этом в рамках цифровой экосистемы у государства особая роль – своевременная законодательная реакция, роль инвестора и соинвестора в инфраструктуру, модератора межотраслевого диалога, а также роль ответственного владельца ряда крупнейших предприятий и лидера изменений[1]. Отсутствие единого курса у всех участников отечественного экономического сообщества может привести к быстрому росту отставания российской экономики, которое в ближайшем будущем вырастет на несколько десятков лет. И наверстать такое отставание будет крайне трудно.

Аналитики Российской ассоциации электронных коммуникаций (РАЭК) приходят к выводу, что в условиях строительства цифровой экономики в отношениях общества и государства должны учитываться следующие тенденции: трансграничный характер цифровой экономики; особое внимание к вопросам кибербезопасности; стимулирование и поддержка таких направлений, как импортозамещение, экспорт

[1] Россия онлайн? Догнать нельзя отстать. URL: http://image-src.bcg.com/Images/BCG-Russia-Online_tcm27-152058.pdf

информационных технологий, обеспечение равных условий ведения деятельности интернет-компаниям в Российской Федерации, развитие инфраструктуры доступа и хранения данных, реформа налогообложения отрасли цифровых технологий, стимулирование безналичных платежей и всех видов массовых цифровых коммуникаций и сервисов; законотворчество на упреждение (большие данные и искусственный интеллект, автономные платформы и Интернет вещей, робототехника, блокчейн); при оценке регулирующего воздействия должны учитываться долгосрочные планы и прогнозы развития (на 10–20 лет)[1].

В своем выступлении на Петербургском экономическом форуме В.В. Путин выделил основные направления развития цифровой экономики в России: «Это ликвидация правовых барьеров, которые препятствуют внедрению передовых технологий; создание опорной инфраструктуры (линии связи, центры хранения и обработки данных); серьезное совершенствование всей системы образования, включая обеспечение всеобщей цифровой грамотности, а также запуск инструментов поддержки отечественных компаний, которые являются центрами компетенций в сфере цифровых и других сквозных технологий».

Как отмечается в Докладе о мировых инвестициях за 2017 год, многие страны разрабатывают стратегии развития цифровой экономики[2]. В основе таких инициатив лежит стремление использовать цифровые возможности в целях позитивного развития государства. Не стала исключением и Россия. Указом Президента РФ от 9 мая 2017 г. № 203 была утверждена Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы.

В указанной Стратегии цифровая экономика характеризуется как «хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг»[3]. Чуть позже (28 июля 2017 г.) была принята и программа «Цифровая экономика Российской Федерации».

---

[1] Доклад С. Плуготаренко. URL: https://www.shopolog.ru/metodichka/analytics/cifrovaya-ekonomika-rossii-2017-analitika-cifry-fakty

[2] Доклад о мировых инвестициях, 2017 год. Инвестиции и цифровая экономика. Основные тенденции и общий обзор // ООН ЮНКТАД. С. 4.

[3] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента РФ от 9 мая 2017 г. № 203. Доступ из справочной правовой системы «КонсультантПлюс».

В Стратегии в числе основных задач при реализации национальных интересов в области цифровой экономики указывается на необходимость создания безопасной национальной платежной инфраструктуры, обеспечивающей «безопасность проведения в сети Интернет финансовых операций, прозрачность трансграничных платежей (идентификация плательщика, получателя, назначение платежа)»[1]. Особое внимание в указанном процессе уделяется также и необходимости создания на международном уровне новых механизмов партнерства, «призванных с участием всех институтов общества выработать систему доверия в сети Интернет, гарантирующую конфиденциальность и личную безопасность пользователей, конфиденциальность их информации, исключающую анонимность, безответственность пользователей и безнаказанность правонарушителей в Сети»[2].

Создание регуляторной среды названо в числе первоочередных задач в рамках программы «Цифровая экономика Российской Федерации». Это вполне закономерно, ведь цифровизация неуклонно ведет к существенным изменениям и трансформациям в правовом регулировании традиционных экономических отношений, а отсутствие благоприятного правового режима для возникновения и развития IT-технологий будет «тормозить» и, более того, вредить возникающей на основе IT-технологий экономической деятельности.

В рамках реализации указанного направления планируется достижение двух основных целей:

устранение ключевых правовых ограничений и создание отдельных правовых институтов, направленных на решение первоочередных задач формирования цифровой экономики, что потребует существенных системных поправок во многие законодательные акты;

создание постоянно действующего механизма управления изменениями и компетенциями (знаниями) в области правового регулирования цифровой экономики для формирования комплексного законодательного регулирования отношений, возникающих в связи с развитием цифровой экономики, что означает приведение базовых законодательных актов к единому знаменателю в понятийном аппарате и отражению в них общих принципов регулирования цифровой экономики[3].

---

[1] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента РФ от 9 мая 2017 г. № 203. Доступ из справочной правовой системы «КонсультантПлюс».

[2] Там же, п. 34, подп. «д».

[3] Вайпан В.А. Основы правового регулирования цифровой экономики // Право и экономика. 2017. № 11. С. 5–18.

Основными сквозными цифровыми технологиями, которые требуют нового нормативного правового регулирования, являются такие недавно возникшие явления экономической жизни, как большие данные, нейротехнологии и искусственный интеллект, системы распределенного реестра (блокчейн), квантовые технологии, новые производственные технологии, промышленный интернет, компоненты робототехники и сенсорика, технологии беспроводной связи (в том числе сети связи пятого поколения, без которых, например, невозможно создание беспилотного транспорта), технологии виртуальной и дополненной реальностей[1].

Стоит отметить, что в указанной программе в числе факторов, препятствующих развитию цифровой экономики России, среди иных угроз отмечены следующие:

проблема обеспечения прав человека в цифровом мире, в том числе при идентификации (соотнесении человека с его цифровым образом), сохранности цифровых данных пользователя, а также проблема обеспечения доверия граждан к цифровой среде;

угрозы личности, бизнесу и государству, связанные с тенденциями к построению сложных иерархических информационно-телекоммуникационных систем, широко использующих виртуализацию, удаленные (облачные) хранилища данных, а также разнородные технологии связи и оконечные устройства;

наращивание возможностей внешнего информационно-технического воздействия на информационную инфраструктуру, в том числе на критическую информационную инфраструктуру;

рост масштабов компьютерной преступности, в том числе международной[2].

Следует особо подчеркнуть, что регуляторике подлежат не только позитивно направленные отношения в цифровой экономике, но и общественные отношения, ставящие под угрозу экономическую безопасность государства и перспективы развития цифровой экономики.

---

[1] Вайпан В.А. Указ. соч. С. 5–18.

[2] Об утверждении программы «Цифровая экономика Российской Федерации»: распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р. Доступ из справочной правовой системы «КонсультантПлюс».

В теории уголовного права принято считать, что необходимым условием криминализации какого-либо явления является его общественная опасность – способность деяния причинять вред отношениям и интересам общества, находящимся под охраной уголовного закона[1].

Анализ динамики исследуемых криминальных нарушений показывает, что в 2017 г. в структуре зарегистрированных посягательств экономической направленности преобладали отдельные деяния против собственности, среди которых доминировали мошенничества в IT-сфере (72,7%) [2]. По данным заместителя председателя правления Сбербанка Станислава Кузнецова, возможный ущерб экономике России от киберугроз в 2018 г. оценивается более чем в 1,1 трлн руб. При этом мировой ущерб к концу текущего года может составить около 1,5 трлн долл.[3] Несмотря на высокую латентность рассматриваемых посягательств и несовершенство статистической отчетности, процент раскрытых выявленных посягательств остается ничтожно малым – порядка 5%. В ближайшей перспективе при уменьшении количества регистрируемых преступлений против собственности прогнозируется увеличение числа «интеллектуальных» мошенничеств и иных преступлений, связанных с использованием информационно-телекоммуникационных технологий, средств сотовой связи, дистанционного банковского обслуживания и увеличением безналичного денежного оборота. Опасность негативных проявлений в цифровой экономике связана также с их способностью причинять кумулятивный ущерб различным группам наиболее значимых общественных отношений.

---

[1] См.: Кудрявцев В.Н. Социологический аспект преступления // Вопросы борьбы с преступностью. М., 1973. Вып. 18. С. 11; Кузнецова Н.Ф. Избранные труды. СПб., 2003. С. 425; Наумов А.В. Российское уголовное право: курс лекций: в 2 т. Т. 1. Общая часть. 3-е изд., перераб. и доп. М.: Юридическая литература, 2004. С. 156; Козлов А.П. Понятие преступления. СПб., 2004. С. 709; Российское уголовное право: в 2 т. Т. 1. Общая часть: учеб. / под ред. Л.В. Иногамовой-Хегай, В.С. Комисарова, А.И. Рарога. М.: ТК Велби: Проспект, 2006. С. 57; Трайнин А.Н. Избранные труды. СПб., 2004. С. 24; Павлухин А.Н., Нестеров П.Н., Эриашвили Н.Д. Общественно опасное поведение и его уголовная противоправность / под ред. А.Н. Павлухина. М.: Юнити-Дана: Закон и право, 2007. С. 21; и др.

[2] Антонян Ю.М., Бражников Д.А., Гончарова М.В. и др. Комплексный анализ состояния преступности в Российской Федерации и расчетные варианты ее развития: аналитический обзор. М.: ВНИИ МВД России, 2018. С. 32–37.

[3] Выступление С. Кузнецова на пресс-конференции по случаю открытия Международного конгресса по кибербезопасности. URL: https://www.gazeta.ru/tech/2018/07/06/11827759/putin_cybercongress.shtml

С сожалением приходится констатировать, что отечественная уголовная политика характеризуется замедленной реакцией законодателя на возникающие угрозы для экономики и социальной стабильности в обществе, «связанные с развитием и внедрением во все аспекты жизнедеятельности информационно-телекоммуникационных технологий, несоразмерностью нарушений закона и ответственности за них, игнорированием многовекового опыта государств с развитой рыночной экономикой, отсутствием приоритетов в правой защите, коллизионностью уголовного закона и законодательства экономического блока, противоречивостью правоприменительной практики. Так, негативные проявления в большинстве своем не могут пресекаться уголовно-правовыми методами, независимо от объема создаваемой ими опасности, поскольку либо имеет место пробел – запреты на такие действия в законе отсутствуют, либо правоприменитель не может правильно оценить поведение лица в конкретной ситуации»[1]. Как правило, должны пройти годы, прежде чем будут приняты нормы, запрещающие очевидно опасные для общества деяния, либо законодатель отреагирует на изменения в структуре общественных отношений. Стоит отметить, что определенный прогресс все же наблюдается. Однако в попытке «вовремя среагировать и предотвратить» общественно опасные явления и их негативные последствия законодательное регулирование зачастую приобретает фрагментарный, уместнее будет сказать, «локальный характер». Яркий тому пример – Федеральный закон от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации», внесший изменения в ст. 158, 159.3 и 159.6 УК РФ. Отечественный законодатель в своем стремлении урегулировать и пресечь новые виды преступных посягательств вновь пошел по пути «непродуманных» и бессистемных изменений уголовного закона. Отсутствие системного подхода к совершенствованию норм с учетом их взаимосвязи и дифференциации ответственности в зависимости от степени общественной опасности деяний и наступивших последствий привело к тому, что «не успевший себя проявить» уголовный закон уже нуждается в корректировке.

«Низкая эффективность норм Особенной части УК РФ объясняется как наличием в самом его тексте пробелов и противоречий принципиального характера, так и отсутствием опыта применения законодательных новелл. Эти два обстоятельства при отсутствии официаль-

[1] Чупрова А.Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. ... д-ра юрид. наук. М., 2015. С. 136.

ных разъяснений уголовного законодательства со стороны управомоченных на то органов способствовали тому, что в ряде регионов усилилась тенденция несогласованности в деятельности органов предварительного следствия и суда»[1].

Особенностью большого числа преступлений в сфере цифровой экономики является их транснациональный характер и огромные суммы причиненного ущерба. Большую озабоченность вызывает и феномен транснациональной блокчейн-преступности, который уже можно характеризовать как самостоятельное направление в рамках киберпреступности. В 2017 г. весь мир подвергся атаке вируса WannaCry, когда сотни тысяч компьютеров по всему миру были заблокированы. Вымогатель, угрожавший стереть всю информацию с диска, требовал оплату в биткоинах (первой децентрализованной цифровой валюте)[2].

В своем выступлении на Международном конгрессе по кибербезопасности Президент РФ В.В. Путин отметил важность выработки единых правил игры, международных стандартов, которые бы учитывали права и интересы всех государств мира в сфере киберпространства; необходимость выработки комплексных решений по предупреждению правонарушений против граждан в цифровой сфере и потребность в консолидации усилий всего международного сообщества для нейтрализации возрастающих киберугроз[3].

Несмотря на то, что большинство экспертов отмечают необходимость совершенствования законодательства в свете всеобъемлющей цифровизации, в уголовном законодательстве России проблемы противодействия высокотехнологическим преступлениям в цифровой экономике пока не нашли своего адекватного отражения.

«Новации в законодательстве, регламентирующем отношения в этом сегменте экономики и охраняющем законные интересы их субъектов, вызываются необходимостью устранения имеющихся законодательных пробелов, связанных с возникновением новых общественных отношений, а также корректировки редакции уже содержащихся в УК РФ норм об ответственности за преступления»[4].

---

[1] Звечаровский И.Э. Новый УК: проблемы применения // Законность. 1999. № 1. С. 10.

[2] Путин выступил на Международном конгрессе по кибербезопасности. URL: https://www.gazeta.ru/tech/2018/07/06/11827759/putin_cybercongress.shtml

[3] Путин призвал выработать единые международные правила игры в цифровой сфере. URL:http://tass.ru/ekonomika/5352758

[4] Чупрова А.Ю. Указ. соч. С. 124.

Сферы, внедряемые в цифровую экономику, принято делить на «хабы». На сегодняшний день выделяются такие «хабы», как государство и общество; маркетинг и реклама; финансы и торговля; инфраструктура и связь; медиа и развлечения; кибербезопасность; образование и кадры; стартапы[1]. Отношения в каждом из «хабов» могут быть подвержены угрозам криминального характера. Преступления в цифровой экономике разнородны и включают различные группы криминальных деяний, совершаемых с использованием IT-технологий. Однако наиболее криминогенными на сегодняшний день выступают такие «хабы», как финансы и торговля, инфраструктура и связь.

Технология блокчейн (технология, базирующаяся на децентрализованных сетях с открытым исходным кодом, использующая криптографические средства проверки транзакций и обеспечения работы сети) и основанные на ней продукты, такие как криптовалюты, нашли широкое применение в инвестиционной сфере. Более того, они вошли в обиход не только крупных компаний, но и простых граждан[2]. «По состоянию на начало июля 2018 г. общая капитализация криптовалютного рынка составила примерно 280 млрд долларов, что на порядки больше, чем в мае 2017 года. На рынке крипторесурсов продолжает доминировать биткойн, на долю которого приходится примерно две пятых от общей капитализации рынка криптовалют. При этом его доля снижается. В начале 2017 года. на биткойн приходилось почти четыре пятых»[3].

Блокчейн-технология, безусловно, имеет громадные перспективы за пределами инвестиционно-финансовой сферы для хранения распределенных ресурсов различного рода, проведения референдумов и голосований, осуществления нотариальных и иных юридических функций, повышения надежности логистических сетей и т. п. Однако стоит напомнить, что указанная сфера пока законом никак не урегулирована. Рассмотрение находящихся в Госдуме трех законопроектов по урегулированию цифрового рынка отложено на октябрь 2018 г.[4], а при

---

[1] Российская ассоциация электронных коммуникаций. URL: http://raec.ru

[2] Сурова Н.Ю. Новые технологии для экономики будущего: рейтинг проектов и механизмы регулирования в сфере цифровой экономики // Банковское дело. 2017. № 12. С. 24–26.

[3] Овчинский В., Ларина Е. Криптовалюта, блокчейн и преступность. URL: http://zavtra.ru/blogs/kriptovalyuta_blokchejn_i_prestupnost_

[4] В настоящий момент на рассмотрении Государственной Думы находятся проекты федеральных законов «О цифровых финансовых активах», «Об альтернативных способах привлечения инвестиций (краудфандинге)» и «О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации».

отсутствии легальных оснований правоотношения в сфере блокчейн-технологий и криптовалют не подлежат судебной защите.

Как справедливо отмечают В. Овчинский и Е. Ларина, «любая инновация, а тем более высокая технология, используется как в законных, так и в криминальных целях. Мало кто знает, что, например, автомобиль в США впервые был использован сначала преступниками, чтобы гарантированно оторваться от погони, а уж затем поступил в распоряжение правоохранителей. Блокчейн-технологии, как и технологический пакет, включающий математические, программные, юридические, финансово-экономические и социальные инновации, также используются с одной стороны бизнесом, государствами, гражданским обществом, а с другой – преступниками и террористами»[1].

Депутат Госдумы А.Г. Аксаков, выступивший инициатором разработки отдельных законопроектов по цифровой экономике, отмечает, что на рынке ICO[2] «очень много мошенничества, злоупотреблений, в том числе связанных с финансированием всевозможных неблагоугодных, запрещенных законом дел, и поэтому очевидно, что рынок криптовалют, блокчейн как технологию необходимо соответствующим образом легализовать, приняв законодательный акт. До 90 процентов ICO – это, к сожалению, мошеннические операции, и, соответственно, необходимо прописать нормы, которые защищали бы наших граждан от недобросовестных участников этого рынка»[3].

В докладе ФБР за апрель этого года отмечается, что более 85% существующих токенов не подкреплены инновационными решениями и реализуются путем создания ненужных рынку проектов. Сотрудники ФБР считают, что причиной этого является беспрепятственный запуск ICO-проектов и помешать этому не способны даже решения правительства[4].

«Дешевые и необратимые переводы денежных средств, запутанные цепочки транзакций и отсутствие надлежащей законодательной

---

[1] Овчинский В., Ларина Е. Указ. соч.

[2] Initial coin offering (ICO) (с англ. – первичное предложение монет, первичное размещение монет) – форма привлечения инвестиций в виде продажи инвесторам фиксированного количества новых единиц криптовалют, полученных разовой или ускоренной эмиссией.

[3] Аксаков А.Г. Вопросы законодательного обеспечения реализации программы «Цифровая экономика Российской Федерации»: выступление на заседании Государственной Думы 12 января 2018 г. // Государственная Дума. Стенограмма заседаний. 2018. Бюл. № 91(1639).

[4] URL: http://hodlweek.com/bitguide/prestupnost-kriptovaliuta-i-blokchein

основы приводят к тому, что с каждым годом увеличивается количество преступлений, связанных с использованием криптовалюты»[1].

К основным признакам криптовалют, делающим их привлекательными для использования в преступных целях, принято относить анонимность транзакций, быстрый транснациональный перевод в обход финансовых организаций и отсутствие систем налогообложения.

Первый, получивший широкое распространение случай использования криптовалют в преступных целях, – это использование биткоина для нелегальных сделок (купли-продажи оружия, наркотических средств, скупки краденого) на сайте Silk Road[2].

По мнению Э.Л. Сидоренко, преступления, совершаемые с использованием криптовалют, можно условно разделить на две группы:

1) общественно опасные деяния, в которых криптовалюты выступают как средства совершения преступлений (используются для вымогательств либо как средство оплаты оружия, наркотиков, порнографии и др.);

2) посягательства, совершенные в отношении криптовалют (речь идет преимущественно о преступлениях, связанных с созданием финансовых пирамид, финансированием терроризма и хищением денежных средств)[3].

Можно отчасти согласиться с мнением экспертов, однако, на наш взгляд, криптовалюты стали использоваться и для совершения «традиционных» мошенничеств. Всеобщая «истерия» относительно майнинга и получения быстрой сверхприбыли от инвестирования в криптовалюты стали объектом внимания слоев населения, весьма далеких от технологических новинок. И. Петров приводит интересные примеры: «В начале октября проходимцы сумели продать жителю подмосковного Обнинска две монетки за 1 тыс. рублей. «Интеллигентного вида цыгане», как описал злоумышленников сам пострадавший, утверждали, что монетки и есть те самые биткоины, о которых говорят по телевизору и пишут в газетах. Молодой житель Зеленограда вел по Интернету переговоры о покупке криптовалюты на одном из сайтов, перевел деньги со своего мобильного, но взамен ничего не получил. Жертвой псевдоброкеров в октябре стала семья выходцев из Средней Азии. «Под предлогом обмена на криптовалюту и получения процента

---

[1] Сидоренко Э.Л. Криминологические риски оборота криптовалюты // Экономика. Налоги. Право. 2017. № 6. С. 147–154.

[2] В США арестовали «повелителя» темной стороны интернета. URL: https://www.rbc.ru/society/02/10/2013/570410869a794761c0ce255e

[3] Сидоренко Э.Л. Указ. соч.

от сделки» она добровольно отдала знакомому «эксперту» 420 тыс. рублей. С деньгами мужчина вскоре скрылся»[1].

Отдельным видом преступной деятельности, на наш взгляд, является совершение «традиционных» компьютерных преступлений, таких как неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для получения криптовалют.

По мнению зарубежных экспертов, скрытый майнинг[2], или криптоджекинг, в ближайшее время станет наиболее распространенным видом киберпреступности. Суть криптоджекинга заключается в скрытой установке на телекоммуникационные устройства жертв специальных программ, занимающихся майнингом. В июле 2018 г. в магазине Google Chrome было обнаружено очередное вредоносное расширение для майнинга криптовалют. В начале апреля Google объявил о том, что начнет блокировать любое расширение для браузера Chrome, предназначенное для майнинга криптовалют, в своем веб-магазине.

Поливариативная природа криптовалют и токенов создает все большие возможности для их преступного использования. И количество угроз с каждым годом будет расти[3]. Однако отсутствие единых норм, регулирующих указанную отрасль, стало реальной проблемой для всего мирового сообщества. Трансформация традиционных преступлений и широкое использование IT-технологий при их совершении стали обыденным явлением. Возможности, предоставляемые всеобщей цифровизацией, без промедления берутся на вооружение преступниками. Уже известны случаи совершения преступлений с использованием Интернета вещей.

Цифровая экономика и преступные проявления в ней – это глобальное явление, развивающееся по большей части на наднациональном уровне. Указанное обстоятельство предопределяет необходимость гармонизации подходов к нормативному регулированию, способных предупредить и предотвратить возникающие угрозы в IT-сфере. В связи с этим как никогда востребованным представляется изучение положений действующих международных договоров и нормативных решений, направленных на противодействие преступлениям в цифровой сфере.

---

[1] Петров И. Криминальный биткоин. Как криптовалюта ворвалась в криминальную летопись страны. URL: https://iz.ru/684876/ivan-petrov/kriminalnyi-bitkoin

[2] Майнинг – деятельность по созданию новых блоков в блокчейне для обеспечения функционирования криптовалютных платформ.

[3] См. подробнее: Сидоренко Э.Л. Указ. соч; Бычков А.И. Проведение расчетных операций: способы, специфика и риски. М., 2016.

1.2. Международно-правовые основы противодействия преступлениям в сфере цифровой экономики

Регламентация правоотношений в цифровой экономике на международном уровне осуществляется Организацией Объединенных Наций и другими международными организациями, имеющими представительства в разных регионах мира.

Право на информацию является неотъемлемой компонентой права человека на свободу, закрепленного Всеобщей декларацией прав человека, принятой Генеральной Ассамблеей ООН 10 декабря 1948 г. Декларацией был установлен запрет на произвольное вмешательство в личную и семейную жизнь, произвольные посягательства на неприкосновенность жилища, тайну корреспонденции или на честь и репутацию человека. Тем самым Декларация провозгласила право на защиту личной информации от неправомерного доступа[1].

Международные принципы создания информационного общества и подходы к его созданию определены Окинавской хартией глобального информационного общества (2000), Декларацией принципов «Построение информационного общества – глобальная задача в новом тысячелетии» (2003), Планом действий Тунисского обязательства (2005)[2].

Вопросы безопасности в информационной среде стали предметом обсуждения достаточно давно. На восьмом Конгрессе ООН по предупреждению преступности и обращению с правонарушителями прозвучал призыв к государствам активизировать борьбу с преступлениями, совершаемыми с использованием компьютерных технологий. Впервые он был внесен в повестку дня ООН, когда в 1998 г. Российская Федерация представила проект резолюции на заседании Первого комитета Генеральной Ассамблеи. Проект был принят без голосования (A/RES/53/70)[3]. С тех пор Генеральный секретарь ООН ежегодно представляет Генеральной Ассамблее доклад, содержащий позиции по данной теме. В рамках созданных групп правительственных экспертов, занимающихся анализом существующих и потенциальных киберугроз и

---

[1] Ефремова М.А. Уголовно-правовая охрана информационной безопасности: дис. ... д-ра юрид. наук. М., 2017. С. 118.

[2] Всемирная встреча на высшем уровне по вопросам информационного общества. URL: http://www.un.org/ru/events/pastevents/wsis.shtml

[3] Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности: резолюция Генеральной Ассамблеи ООН A/RES/53/70 от 4 янв. 1999 г. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lan

возможных совместных мер по их нейтрализации, ежегодно готовятся доклады.

В предисловии к новому докладу «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» Генеральный секретарь ООН написал: «Я с удовлетворением отмечаю, что в этом докладе подчеркивается ключевая роль Устава Организации Объединенных Наций и международного права, а также важность ответственного поведения государств. Содержащиеся в нем рекомендации указывают на то, как увязать вопросы безопасности ИКТ с существующими нормами международного права и договоренностями, которые регулируют межгосударственные отношения и служат основой для международного мира и безопасности... Организация Объединенных Наций играет лидирующую роль в налаживании диалога между государствами-членами по проблеме безопасности в сфере использования ИКТ и в дальнейшем развитии международного сотрудничества в этой области»[1].

Резолюцией Генеральной Ассамблеи ООН 68/167, принятой 18 декабря 2013 г., было вновь подтверждено право на неприкосновенность личной жизни, в соответствии с которым никто не должен подвергаться произвольному или незаконному вмешательству в его или ее личную и семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность жилища или тайну корреспонденции, и право на защиту закона от такого вмешательства или таких посягательств, как это предусмотрено ст. 12 Всеобщей декларации прав человека и ст. 17 Международного пакта о гражданских и политических правах; презюмирована тождественность прав человека в офлайновой среде правам в онлайновой среде и необходимость их защиты должным образом от всех видов преступных посягательств. Кроме того, особо была отмечена необходимость «уважения и защиты всеми государствами права на неприкосновенность личной жизни, в том числе в контексте цифровой коммуникации, и предотвращения нарушения указанных прав, в том числе путем обеспечения того, чтобы касающееся этого национальное законодательство соответствовало их международным обязательствам по международному праву прав человека»[2].

---

[1] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. URL: https://www.un.org/disarmament/ru

[2] Право на неприкосновенность личной жизни в цифровой век: резолюция Генеральной Ассамблеи ООН A/RES/68/167 от 18 дек. 2013 г.. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/49/PDF/N1344949.pdf?OpenElement

Необходимость создания оперативной и эффективной системы международного сотрудничества, должным образом учитывающей специфические потребности борьбы с преступностью в сфере компьютерных технологий, отмечалась и на 23-й Конференции министров юстиции стран Европы (Лондон, 8–9 июня 2000 г.). При этом на 21-й Конференции Комитету министров было рекомендовано «обеспечить большую согласованность положений национального уголовного права разных стран, сделать возможным использование эффективных средств расследования преступлений в сфере компьютерной информации, поддержать проводимую Европейским комитетом по проблемам преступности (ЕКПП) работу по предупреждению таких правонарушений»[1].

Впоследствии данная рекомендация также была закреплена в Резолюции Генеральной Ассамблеи ООН 55/63 «Борьба с преступным использованием информационных технологий». В указанной Резолюции отмечается значительный прогресс в разработке и внедрении информационных технологий и телекоммуникационных средств. Кроме того, подчеркивается необходимость предупреждения преступного использования информационных технологий в связи с появлением новых возможностей для преступной деятельности с использованием IT-технологий, совершенствования национального законодательства в области противодействия IT-преступлениям и хранения данных, имеющих отношение к преступным посягательствам в рассматриваемой сфере, сотрудничества правоохранительных органов при расследовании трансграничных преступлений и совершенствования кадровой подготовки для борьбы с преступным использованием информационных технологий[2].

По мнению А.А. Чеботаревой, на сегодняшний день в системе международной информационной безопасности сформировано две модели: евроатлантическая и евразийская. Россия, наряду с другими государствами – участниками Шанхайской организации сотрудничества (ШОС), последовательно реализует подходы евразийской системы[3].

Евроатлантическая система международной информационной безопасности связана с понятием киберпреступности и основана на нормах и принципах Конвенции Совета Европы о преступности в

---

[1] Чеботарева А.А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе: дис. ... д-ра юрид. наук. М., 2017. С. 169.

[2] Борьба с преступным использованием информационных технологий: резолюция Генеральной Ассамблеи ООН 55/63 от 22 янв. 2001 г. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/563/19/PDF/N0056319.pdf?OpenElement

[3] Чеботарева А.А. Указ. соч. С. 168.

сфере компьютерной информации, принятой в Будапеште 23 ноября 2001 г.[1]

По своей сути указанная Конвенция является первым международным договором о преступлениях, совершаемых с использованием IT-технологий (сети Интернет, компьютеров и компьютерных сетей). Принятие Конвенции было обусловлено угрозой, которую несет использование IT-технологий для совершения преступлений в период повсеместного внедрения цифровой экономики и продолжающейся глобализации. В ней рассматриваются, в частности, такие вопросы, как нарушение авторского права, мошенничество с использованием компьютеров, детская порнография и нарушения безопасности сетей. Она содержит также ряд полномочий и процедур, таких как досмотр компьютерных сетей и перехват данных. Кроме того, в Конвенции приведен перечень нарушений, в том числе и в сфере экономики, которые должны быть криминализированы в национальных уголовных законах.

Главная цель Конвенции, изложенная в ее преамбуле, состоит в том, чтобы проводить в приоритетном порядке общую политику в сфере уголовного права, направленную на защиту общества от компьютерных преступлений, в том числе путем принятия соответствующих законодательных актов и укрепления международного сотрудничества.

Договор о принятии Конвенции открыт для подписания странами – членами Совета Европы и странами, которые не являются членами, но приняли участие в ее составлении, а также другими странами.

На сегодняшний день Конвенция ратифицирована и действует на территории 60 государств мира, еще четыре страны подписали ее, а еще семи государствам было предложено присоединиться к ней. Около 140 стран использовали текст Конвенции для создания своих внутренних законов, и свыше 160 стран сотрудничает с Советом Европы в области противодействия киберпреступности. Рассмотрим более подробно ее положения.

Конвенция состоит из трех глав: первая глава посвящена разъяснению использованных в Конвенции терминов, вторая – мерам, которые следует принять на национальном уровне (нормы материального и процессуального права), третья – положениям, обеспечивающим международное сотрудничество. Необходимо отметить, что Конвенция выходит за рамки сугубо законодательных вопросов и декларирует прин-

[1] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г). Доступ из справочно-правовой системы «Гарант».

ципы для международного сотрудничества правоохранительных органов стран-участниц в борьбе с компьютерной преступностью. Однако, учитывая предмет настоящего исследования, детальному анализу были подвергнуты непосредственно положения норм материального права.

В первой главе Конвенции даются определения понятий «компьютерная система», «компьютерные данные», «поставщик услуг», «данные о потоках». Указанные понятия толкуются в Конвенции достаточно широко и могут быть применены к новым IT-технологиям.

Нормы, подлежащие инкорпорации в национальное законодательство, разделены на три блока.

К преступлениям против конфиденциальности, целостности и доступности компьютерных данных и систем отнесены следующие деяния:

противозаконный доступ, осуществляемый преднамеренно, с нарушением мер безопасности и намерением завладеть компьютерными данными или иным злым умыслом;

неправомерный перехват – умышленно осуществленный с использованием технических средств перехват не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы;

воздействие на данные, выражающееся в их умышленном неправомерном повреждении, удалении, ухудшении качества, изменении или блокировании;

воздействие на функционирование системы и противозаконное использование устройств – умышленное создание серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных;

противозаконное использование устройств, под которым понимаются незаконные производство, продажа, приобретение для использования, импорт, оптовая продажа, владение или иные формы предоставления в пользование устройств, включая компьютерные программы, предназначенных для совершения преступлений; противозаконное использование компьютерных паролей, кодов доступа или аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе.

Вторая группа криминальных явлений связана с использованием компьютерных средств для совершения подлога и мошенничества.

К подлогам относятся умышленный и неправомерный ввод, изменение, уничтожение или блокирование компьютерных данных, влеку-

щие за собой нарушение их аутентичности, с намерением, чтобы данные рассматривались или использовались в юридических целях в качестве аутентичных, независимо от того, поддаются ли они непосредственному прочтению и являются ли они понятными.

Как мошенничество характеризуется лишение другого лица его собственности путем любого ввода, изменения, удаления или блокирования компьютерных данных; любого вмешательства в функционирование компьютерной системы с мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица.

К преступлениям, связанным с содержанием данных, относятся следующие деяния:

правонарушения, связанные с детской порнографией, – деяния, связанные с оборотом детской порнографии посредством компьютерных сетей: производство детской порнографической продукции в целях распространения через компьютерную систему; предложение или предоставление в пользование детской порнографии через компьютерную систему; распространение или передача детской порнографии через компьютерную систему; приобретение детской порнографии через компьютерную систему для себя или для другого лица и владение детской порнографией, находящейся в компьютерной системе или на носителях компьютерных данных (п. 1 ст. 9 Конвенции о преступности в сфере компьютерной информации);

правонарушения, связанные с нарушением авторских и смежных прав, определенных в международных актах, когда такие действия совершаются умышленно, в коммерческом масштабе и с помощью компьютерной системы[1];

правонарушения, связанные с распространением информации расистского и другого характера, подстрекающей к насильственным действиям, ненависти или дискриминации отдельного лица или группы лиц, основывающимся на расовой, национальной, религиозной или этнической принадлежности.

Следует отметить, что правонарушения, связанные с проявлением расизма и ксенофобии, не были включены в первоначальный текст Конвенции и были введены Дополнительным протоколом к ней. Этот протокол расширяет сферу действия Конвенции о кибер-

[1] Конвенция о преступности в сфере компьютерной информации ETS № 185.

преступности, включая ее существенные, процедурные и посвященные международному сотрудничеству положения, охватывая также правонарушения, связанные с расистской и ксенофобской пропагандой. Таким образом, помимо гармонизации существенных правовых аспектов такого поведения, протокол направлен на расширение возможностей сторон по использованию средств в области международного сотрудничества, изложенных в Конвенции[1]. К деяниям, рекомендованным для инкорпорации в национальное законодательство, отнесены распространение расистских и ксенофобских материалов посредством компьютерных систем; мотивированная угроза расизма и ксенофобии; расистское и ксенофобское мотивированное оскорбление; отрицание, чрезвычайная минимизация, одобрение или оправдание геноцида или преступлений против человечества.

Покушение, соучастие или подстрекательство к совершению указанных преступлений также признаются уголовно наказуемыми деяниями. Уголовная ответственность юридического лица, согласно Конвенции, должна наступать за уголовное преступление, которое совершается в его пользу любым физическим лицом, действующим самостоятельно или как часть одного из органов соответствующего юридического лица и занимающим ведущее положение в нем на основании полномочий представлять данное юридическое лицо, права принимать решения от имени этого юридического лица, права осуществлять контроль внутри этого юридического лица. Статьей 13 Конвенции государствам-участникам рекомендовано применять за совершение перечисленных в Конвенции деяний такие меры наказания, как лишение свободы и денежные штрафы[2].

Перечень вышеизложенных преступлений не является исчерпывающим, и в законодательстве любого государства, подписавшего Конвенцию, могут быть предусмотрены иные деяния, признаваемые преступными. Следует отметить, что на территории стран Евросоюза на основе положений Конвенции о киберпреступности приняты директивы[3], значительно ужесточающие ответственность

---

[1] Об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем: дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации № 189 от 1 марта 2006 г. URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/189

[2] Конвенция о преступности в сфере компьютерной информации ETS № 185.

[3] См.: Об атаках на информационные системы и о замене Рамочного решения 2005/222/ПВД Совета ЕС: директива Европейского парламента и Совета ЕС

за преступные посягательства в IT-сфере. Анализ содержания указанных нормативных правовых актов будет изложен в рамках параграфа, посвященного вопросам противодействия преступлениям в цифровой экономике на территории стран Западной Европы.

Российская Федерация, наряду со странами, входящими в ШОС, не ратифицировала Конвенцию Совета Европы о преступности в сфере компьютерной информации ввиду определенных нареканий к ее содержанию. В основном критике подвергаются положения Конвенции, касающиеся процессуальных аспектов и международного сотрудничества, трансграничного доступа к хранящимся компьютерным данным без согласия другой стороны, возможности вмешательства во внутренние дела других государств посредством несанкционированного проведения оперативно-розыскных действий в национальном киберпространстве, положения, нарушающие принцип суверенитета государств, принцип уважения основных прав и свобод человека[1].

Евразийская модель международной информационной безопасности формируется на основе инициатив, предпринимаемых в рамках ШОС. В заявлении глав государств – членов ШОС по международной информационной безопасности выражена «озабоченность тем, что в настоящее время появляется реальная опасность использования ИКТ в целях, способных нанести серьезный ущерб безопасности человека, общества и государства в нарушение основополагающих принципов равноправия и взаимного уважения, невмешательства во внутренние дела суверенных государств, мирного урегулирования конфликтов, неприменения силы, соблюдения прав человека. При этом угрозы использования ИКТ в преступных, террористических и военно-политических целях, несовместимых с обеспечением международной безопасности, могут реализовываться как в гражданской, так и в военной сферах и привести к тяжелым политическим и социально-экономическим

№ 2013/40/ЕС; О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза: директива Европейского Парламента и Совета ЕС (ЕС) 2016/1148 от 6 июля 2016 г.; О противодействии терроризму, о замене Рамочного Решения 2002/475/ПВД Совета ЕС и об изменении Решения 2005/671/ПВД Совета ЕС: директива Европейского Парламента и Совета ЕС 2017/541 от 15 марта 2017 г. Доступ из справочно-правовой системы «Гарант».

[1] См. подробнее: Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. 2007. № 2. С. 23.

последствиям в отдельных странах, регионах и в мире в целом, к дестабилизации общественной жизни государств»[1]. Кроме того, главы государств приняли решение о создании группы экспертов государств – членов ШОС по международной информационной безопасности для выработки плана действий по обеспечению международной информационной безопасности и определению возможных путей и средств решения проблемы киберпреступности в рамках ШОС.

Главным шагом в реализации указанных заявлений стало подписание 16 июня 2009 г. межправительственного Соглашения государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности.

В Соглашении приведены следующие основные угрозы в области обеспечения международной информационной безопасности, а также раскрыто их понимание (приложение 2 Соглашения):

1) разработка и применение информационного оружия, подготовка и ведение информационной войны;

2) информационный терроризм;

3) информационная преступность;

4) использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств;

5) распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств;

6) угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.

В числе основных направлений сотрудничества указано «противодействие информационной преступности, которая определяется как использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных 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

[1] Заявление глав государств – членов ШОС по международной информационной безопасности (г. Шанхай, 15 июня 2006 года). URL: http://rus.sectsco.org/load/44842

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.»[1].

Стоит отметить, что Соглашение не предусматривает обязательные для имплементации в национальное законодательство нормы, не налагает на стороны обязательства по предоставлению информации в рамках сотрудничества и не является основанием для передачи информации. Однако его несомненным преимуществом является декларирование принципов и механизмов сотрудничества в области противодействия угрозам при обеспечении международной информационной безопасности.

Необходимо также подчеркнуть, что 1 июня 2001 г. в Минске странами СНГ было заключено Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации, текст которого содержит ряд уголовно-наказуемых деяний[2]. Положения указанного Соглашения, наряду с иными нормативными актами, устанавливающими ответственность за преступления, совершаемые с использованием IT-технологий, будут рассмотрены в рамках параграфа, посвященного законодательству стран, входящих в Евразийский экономический союз.

В докладе группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности указывается, что в течение прошедшего десятилетия усилия по борьбе с угрозой киберпреступности прилагались на международном уровне, в частности, в рамках ШОС, Организации американских государств, Форума азиатско-тихоокеанского экономического сотрудничества, Регионального форума Ассоциации государств Юго-Восточной Азии (АСЕАН), Экономического сообщества западноафриканских государств, Африканского союза, Европейского союза, Организации по безопасности и сотрудничеству в Европе и Совета Европы, а также в форме двусторонних усилий государств[3]. «Однако

---

[1] Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. URL: http://rus.sectsco.org/documents/20090616/203974.html

[2] Собрание законодательства РФ. 2009. № 13. Ст. 1460.

[3] URL: https://www.un.org/disarmament/ru

необходимо заметить, что данное сотрудничество осуществляется в основном в сфере информационно-правового обеспечения процессуального взаимодействия правоохранительных органов стран по предупреждению и расследованию компьютерных преступлений, а исследования ведутся в плоскости криминологической науки. Тем временем уголовно-правовые вопросы определения понятия и видов компьютерных преступлений, особенностей их криминализации в национальных уголовных законах, уголовной ответственности за совершение данных деяний остаются без ответа»[1].

Особую озабоченность представляет и отсутствие международных актов, направленных на урегулирование статуса криптовалют. В докладах международных организаций, таких как Интерпол, Европол, ФАТФ[2], высказывается обеспокоенность относительно роста преступлений, связанных с криптоиндустрией. В отчете ФАТФ «Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ», опубликованном в 2014 г., отмечались только потенциальные риски использования криптовалют и токенов. При этом рассмотрение конкретных мер, направленных на противодействие новому направлению киберпреступности, используемому в целях легализации преступно нажитых средств, было отложено. На сегодняшний день исследования криптоиндустрии экспертами ФАТФ продолжаются. Однако радует тот факт, что вопрос использования криптовалют и технологии блокчейн в преступных целях был внесен Управлением по наркотикам и преступности ООН в повестку 14-го Конгресса ООН по предупреждению преступности и уголовному правосудию[3].

Проведенный анализ показывает, что мировое сообщество достаточно давно осознало важность обеспечения информационной безопасности и противодействия посягательствам в IT-сфере. При этом следует отметить, что, несмотря на усилия ООН и других межгосударственных органов, глобального соглашения по обеспечению

---

[1] Дубко М. Международное сотрудничество в сфере уголовно-правовой борьбы с неправомерным завладением компьютерной информацией // Центр исследования компьютерной преступности. URL: http://www.crime-research.ru/articles

[2] ФАТФ – межправительственная организация, которая занимается выработкой мировых стандартов в сфере противодействия отмыванию преступных доходов и финансированию терроризма, а также осуществляет оценки соответствия национальных систем ПОД/ФТ этим стандартам.

[3] URL: http://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_27/ECN152018_11_r_V1801147.pdf

кибербезопасности на сегодняшний день так и не принято. Во многом это объясняется отсутствием единства во взглядах на обеспечение международной информационной безопасности.

Необходимость разработки нового универсального документа сегодня очевидна для всего мирового сообщества. На 12-м Конгрессе ООН по предупреждению преступности и уголовному правосудию некоторые страны высказали мнение, что присоединение к Конвенции Совета Европы о киберпреступности будет содействовать развитию международного сотрудничества и унификации национального законодательства разных стран в области киберпреступности. Некоторые страны предложили разработать новый международный правовой документ о противодействии киберпреступности. Другие придерживаются мнения, что унификации законодательства может способствовать разработка международных типовых положений на уровне ООН. Ряд стран рекомендовали разработать международные стандарты следственных действий правоохранительных органов, связанных с экстерриториальными данными, в том числе в целях уточнения взаимосвязи между такими расследованиями и принципами национального суверенитета. Другие предложили усилить оказание технической помощи правоохранительным органам, прокуратуре и судебным органам в вопросах предотвращения и противодействия киберпреступности.

По итогам Конгресса была принята Салвадорская декларация о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире. В Декларации было рекомендовано Комиссии по предупреждению преступности и уголовному правосудию «рассмотреть вопрос о созыве совещания межправительственной группы экспертов открытого состава для проведения всестороннего исследования проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора, включая обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве, с целью изучения возможных путей укрепления существующих национальных и международных правовых или других мер по противодействию киберпреступности и выработки предложений о таких новых мерах»[1].

Российская Федерация принимает активное участие в формировании системы международной информационной безопасности в рамках реализации стратегических задач, сформулированных в Стратегии

[1] URL: http://www.un.org/ru/documents/decl_conv/declarations/salvador_declaration

развития информационного общества в Российской Федерации на 2017–2030 годы. Так, в ООН в качестве официального документа 72-й сессии Генеральной Ассамблеи была внесена обновленная редакция российского проекта конвенции ООН о сотрудничестве в сфере противодействия информационной преступности, разработанная Советом безопасности РФ совместно с МИД России[1]. Проект конвенции имеет более широкую сферу применения в отличие от Конвенции Совета Европы, направлен на регулирование деятельности государств по обеспечению международной информационной безопасности и сохраняет преемственность с принятыми ранее документами ООН[2].

Однако на сегодняшний день универсальный документ ООН пока не принят. Как справедливо отмечает М.А. Ефремова, разработка такой конвенции должна вестись под эгидой ООН. Это позволит, с одной стороны, максимально учесть озабоченность всех стран мира по поводу противостояния новым угрозам, а с другой – придать документу действительно глобальный масштаб, без которого борьба с киберпреступностью не может быть достаточно эффективной[3]. Однако, к сожалению, заключение универсального международного договора о противодействии IT-преступлениям в условиях развития глобального цифрового общества, который бы учитывал уже накопившийся опыт международных соглашений в данной области и особенности национального законодательства всех стран-участниц, довольно сложная и трудоемкая задача.

[1] Об основных итогах реализации в 2017 году государственной политики Российской Федерации в области международной информационной безопасности (12 февраля 2018 г.). URL: http://www.scrf.gov.ru/news/allnews/2353

[2] Ефремова М.А. Указ. соч. С. 130.

[3] Там же.

Глава 2. Опыт противодействия преступлениям в сфере цифровой экономики мерами уголовно-правового характера

В Салвадорской декларации Управлению ООН по наркотикам и преступности в сотрудничестве с государствами-участниками, соответствующими международными организациями и частным сектором было рекомендовано «оказывать государствам техническую помощь и помощь в подготовке кадров в деле совершенствования национального законодательства и наращивания потенциала национальных органов в целях противодействия киберпреступности, в том числе предупреждения, выявления и расследования таких преступлений во всех формах и преследования за их совершение, а также в целях укрепления безопасности компьютерных сетей»[1]. Однако для отдельных государств мира вопрос принятия национального законодательства по противодействию преступлениям в IT-сфере по-прежнему остается актуальным.

В 30 из 168 стран уголовное законодательство о преступлениях, совершаемых с использованием IT-технологий, отсутствует вовсе[2]. В процентном соотношении ситуация выглядит следующим образом: 72% стран имеют законодательство в указанной сфере, 9% – законодательство разрабатывается, 19% – законодательство отсутствует, 1% – нет сведений[3].

Во Всестороннем анализе состояния преступности, подготовленном Управлением ООН по наркотикам и преступности[4], приведены результаты опроса стран о состоянии уголовного законодательства в области киберпреступности. В вопроснике были выделены 14 деяний, которые обычно включаются в понятие киберпреступности: незаконный доступ; незаконный перехват; незаконное вмешательство; распространение и использование средств неправомерного использования компьютеров; нарушение конфиденциальности; мошенничество или подлог; преступления, связанные с использованием персональных данных; преступления, касающиеся авторских прав и товарных знаков;

---

[1] URL: http://www.un.org/ru/documents/decl_conv/declarations/salvador_declaration

[2] Комиссия Организации Объединенных Наций по торговле и развитию. URL: http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

[3] Информация Управления ООН по наркотикам и преступности. URL: http://cybrepo.unodc.org

[4] Всестороннее исследование проблемы киберпреступности: проект, февраль 2013 года. URL: http://www.unodc.org

спам; причинение личного вреда; расизм и ксенофобия; распространение детской порнографии; вовлечение несовершеннолетних и груминг; преступления, связанные с содействием терроризму.

Страны-респонденты сообщили о том, что указанные деяния широко криминализированы, за явным исключением преступлений, связанных со спамом, и в некоторой степени – преступлений, связанных со средствами неправомерного использования компьютеров, расизмом и ксенофобией, а также использованием Интернета с целью вовлечения или груминга детей.

По мнению экспертов, приведенные данные отражают определенный базовый консенсус в отношении понимания подлежащих наказанию видов деяний, связанных с киберпреступностью.

В исследовании также сообщается, что в некоторых странах под уголовно-правовым запретом находятся дополнительные преступления, не упомянутые в вопроснике. Они главным образом касались данных, хранящихся в компьютере, включая криминализацию непристойных материалов, азартных игр в режиме онлайн и онлайновых незаконных рынков, таких как рынки торговли наркотиками и людьми.

В том, что касается указанных 14 деяний, страны сообщили, что в отношении основных киберпреступлений против конфиденциальности, целостности данных и доступности компьютерных систем применяются специальные нормы, предусматривающие ответственность за киберпреступления. Ответственность за мошенничество или подлог, а также посягательства, связанные с хищением персональных данных, предусмотрена как нормами за преступления в IT-сфере, так и нормами, направленными на противодействие общеуголовной преступности. В отношении остальных приведенных посягательств в основном применяются общие нормы уголовных законов.

Однако национальные подходы к криминализации киберпреступлений имеют существенные различия. Преступления, связанные с незаконным доступом к компьютерным системам и данным, различаются в зависимости от объекта преступления (данные, система или информация). В отдельных странах криминализирован доступ как таковой и наличие умысла на причинение ущерба необязательно. В иных странах ситуация складывается противоположным образом. Различаются подходы к наличию умысла в составе преступления при криминализации вмешательства в функционирование компьютерных систем или данные. В большинстве стран ответственность предусматривается за преднамеренное вмешательство, в то время как в других

странах – и за вмешательство по неосторожности. Деяния, характеризуемые как вмешательство, охватывают деяния от повреждения или удаления до изменения, блокировки, ввода или передачи данных. Криминализация незаконного перехвата данных различается в зависимости от того, ограничивается ли правонарушение перехватом не предназначенных для общего пользования данных или не ограничивается им, а также в зависимости от того, ограничивается ли преступление перехватом при помощи технических средств.

Не во всех странах криминализированы средства неправомерного использования компьютеров. В тех странах, где они криминализированы, имеются различия в зависимости от того, связано ли преступление с хранением, распространением или использованием программного обеспечения (такого, как вредоносные программы) и (или) компьютерных кодов доступа (например, паролей потерпевшей стороны). С точки зрения международного сотрудничества такие различия могут влиять на двойную уголовную ответственность.

В ряде стран приняты специальные положения в отношении компьютерного мошенничества, подлога и использования персональных данных. В других странах используются общие положения в отношении мошенничества или хищения либо за основу берутся преступления, отражающие составные элементы деяния, такие как незаконный доступ, вмешательство в данные и подлог. Весьма широкое распространение получила криминализация правонарушений, связанных с содержанием данных, особенно преступлений, касающихся детской порнографии. Однако существуют расхождения в определении понятия «ребенок», в определении ограничений, касающихся «визуальных» материалов или исключения имитируемых материалов, а также в отношении охватываемых деяний.

Что касается IT-преступлений, связанных с авторскими правами и товарными знаками, страны чаще всего сообщают, что в случае деяний, совершенных умышленно и в коммерческих масштабах, они применяют общие уголовно-правовые нормы за преступления.

Наиболее развитым законодательством в рассматриваемой сфере на сегодняшний день обладают страны Европейского континента, Северной Америки и Тихоокеанского региона. Во многом это объясняется тем, что государства указанных регионов являются лидерами цифрового развития.

Первые изменения в традиционном уголовном законодательстве зарубежных стран, направленные на противодействие преступности с

использованием IT-технологий, касались защиты данных. Первый закон о защите информации был принят в США в 1906 г. (тогда как в нашей стране первое законодательное обращение к данной проблеме произошло лишь в конце 1980-х гг.). В середине 70-х гг. прошлого столетия в ряде западноевропейских стран также появились специальные нормы, обеспечивающие защиту данных. Так, в 1973 г. в Швеции несанкционированное приобретение хранящихся данных было признано преступлением, в период с 1977 по 1979 г. в ФРГ, Австрии, Дании, Норвегии были приняты законы о защите данных. Впоследствии аналогичные нормы появились в уголовном законодательстве Дании и ФРГ (1986), Франции (1988), Великобритании (1990)[1].

В рамках настоящей главы вниманию читателей представлен подробный анализ состояния уголовного законодательства стран, имеющих, согласно рейтингу Международного союза электросвязи, высокий индекс кибербезопасности.

2.1. Уголовная ответственность за преступления в сфере цифровой экономики в США

Соединенные Штаты Америки входят в топ-10 стран с развитой цифровой экономикой. Вполне закономерно, что Интернет и цифровая экономика являются важнейшей частью американской экономики. Они являются источником роста, фактором, стимулирующим глобальную торговлю, и ключевым элементом конкурентоспособности США. На долю секторов, связанных с Интернетом и IT-технологиями, уже приходится более десяти процентов ВВП США, и эта цифра не отражает их истинного потенциала. По оценкам экспертов, оцифровка имеет потенциал для увеличения годового ВВП США до 2,2 трлн долл. к 2025 г.

Для реализации указанных задач в 2016 г. в США была принята и начала реализовываться национальная программа Digital Economy Agenda[2], в которой намечен курс США на поддержку преобразующего влияния Интернета и раскрытия его роли в качестве глобальной платформы для общения, выражения людей как личностей, торговли и инноваций.

[1] См.: Stein Schjolberg. The history of cybercrime 1976–2014. Oslou. P. 7.

[2] Commerce Department Digital Economy Agenda. URL: https://www.ntia.doc.gov

Программа включает в себя следующие ключевые направления:

1. *Глобальный свободный обмен информацией.*

Бесплатный и открытый глобальный Интернет с минимальными барьерами для трансграничного потока данных и услуг является основой успеха цифровой экономики. Это позволит предприятиям и их работникам продавать свои товары кому угодно по всему земному шару, общаться с клиентами, а также развивать свои навыки.

2. *Доверие и безопасность.*

Цифровая экономика имеет шансы на процветание и успех только в том случае, если предприятия и потребители будут уверены, что их деятельность безопасна и конфиденциальна.

3. *Доступ и навыки.*

Американским предприятиям и потребителям для процветания в цифровой глобальной экономике и конкуренции с зарубежными компаниями также требуется общая инфраструктура и квалифицированные работники. Тем не менее, интернет-покрытие в стране остается неравномерным, и в отдельных местностях США до сих пор нет доступа к сети Интернет. Американским работникам будут нужны новые навыки и инструменты, если они хотят пользоваться всеми благами, доступными благодаря развитию современной цифровой экономики.

4. *Инновации и новые технологии.*

Цифровизация бизнеса может играть определенную роль в поддержке инноваций. Бизнес стремится увеличить свои обороты и работать с новыми технологиями, такими как беспилотные автомобили и летательные аппараты, в самом начале их жизненного цикла, что позволит решить множество долгосрочных политических проблем.

Выделение указанных компонент в рамках национальной программы неслучайно. Учитывая цель настоящего исследования, остановимся на вопросах доверия и безопасности. Бурное развитие цифровой экономики поднимает экономику стран на совершенно новый уровень с созданием высокооплачиваемых рабочих мест, повышением производительности и обеспечением будущего процветания. Однако со все большей цифровизацией американской экономики в обществе нарастает страх перед IT-технологиями и уменьшается доверие к ним, что несомненно замедляет или даже тормозит темпы роста цифровой экономики.

Опрос, проведенный для ESET компанией Google Surveys в марте 2017 г., показал, что значительное число американцев видят риски в цифровых технологиях, а некоторые реагируют на них изменением по-

ведения. Например, в 2016 г. Национальное управление телекоммуникаций и информации (NTIA), работая с данными опроса в США 2015 г., обнаружило, что 45% онлайн-домохозяйств в Америке воздерживались от участия в определенных онлайн-действиях из-за соображений конфиденциальности или безопасности. Это включало такие действия, как финансовые онлайн-транзакции, покупка товаров или услуг в Интернете, размещение в социальных сетях или выражение мнений по спорным или политическим вопросам через Интернет. Кроме того, общественное восприятие рисков, безопасности и конфиденциальности влияет на один из самых обсуждаемых элементов процветающего цифрового будущего – Интернета вещей (IoT). Например, 50% опрошенных потребителей в США высказали опасения по поводу кибербезопасности IoT-устройства, что отпугнуло их от покупки такого устройства.

На вопрос: «Считаете ли вы, что проблемы с цифровыми технологиями, такие как взлом компьютеров и перебои в работе сети, представляют риск для вашей безопасности и благополучия?» – треть из 1000 опрошенных взрослых американцев ответила утвердительно, указав на высокий риск. Умеренный риск был выбран 35% опрошенных, только один из восьми респондентов не видел «почти никакого риска», а менее одного из пяти – только «небольшой риск» [1].

Недоверие к достижениям цифровой экономики становится реальной проблемой для передовых стран и обсуждается на самом высоком уровне. В докладе Президентской комиссии по повышению национальной кибербезопасности в 2016 г. отмечалось: «Компьютерные технологии имеют огромный потенциал для улучшения жизни всех американцев. Каждый день мы видим новые свидетельства того, насколько трансформативными могут быть эти технологии и как они могут положительно повлиять на нашу экономику и качество жизни на рабочем месте... Наша жизнь обогащается цифровыми устройствами и сетями, а также новаторами, которые нашли творческие способы использовать технологии... Однако наша цифровая экономика и общество достигнут полного потенциала только в том случае, если американцы будут доверять этим системам для защиты своей безопасности и конфиденциальности»[2].

[1] Will cybercrime and other cybersecurity issues undermine the digital economy? URL: https://www.welivesecurity.com/2017/04/26/will-cybercrime-and-other-cybersecurity-issues-undermine-the-digital-economy/

[2] URL: https://www.whitehouse.gov/issues

С целью преодоления складывающегося в обществе и бизнес-сообществе предубеждения против использования IT-технологий в США был запущен Щит конфиденциальности ЕС–США (EU–U.S. Privacy Shield Framework), предназначенный для устранения нормативных и торговых барьеров для американских компаний. В целях развития электронной коммерции была также запущена пилотная программа «Цифровой атташе» (Digital Attache) для оказания помощи и поддержки предприятиям США на иностранных цифровых рынках.

Однако раскрытие полного потенциала цифровой экономики невозможно без обеспечения должной степени информационной безопасности, особое место в которой занимают нормы превентивного и запретительного характера.

В Стратегии кибербезопасности, принятой Министерством государственной безопасности США 15 мая 2018 г.[1] и рассчитанной на 5 лет, отмечается, что с каждым годом число злоумышленников, желающих использовать киберпространство в преступных целях, растет. При этом мотивы преступной деятельности могут варьироваться от шпионажа, политических и идеологических интересов до финансовой выгоды. Особую озабоченность вызывают и транснациональные преступные организации, деятельность которых создает реальный риск критическим инфраструктурам США.

Число киберинцидентов в федеральных системах, о которых сообщалось Министерству госбезопасности, увеличилось более чем в десять раз за период с 2006 по 2015 г. В 2015 г. громкая атака на Федеральное агентство привела к компрометации кадрового учета более четырех миллионов федеральных служащих и в конечном итоге затронула почти 22 млн человек. Растущая взаимосвязь киберсистем и физических систем в критической инфраструктуре также создает потенциальный риск того, что вредоносная кибератакивность приведет к прямым физическим последствиям. Инциденты с вымогателями, такими как WannaCry и NotPetya, демонстрируют обратную сторону быстрых темпов внедрения IT-технологий в жизнь общества.

В рамках указанной Стратегии намечено выполнение семи целей: оценка рисков, возникающих при обеспечении кибербезопасности; защита информационных систем федерального правительства; защита критически важных государственных инфраструктур; предотвращение и пресечение преступного использования Интернета; эффективное реагирование на киберинциденты; повышение

[1] URL: https://www.dhs.gov/sites/default/files/publications/DHSCybersecurityStrategy_1.

безопасности и надежности кибернетической экосистемы; совершенствование управления деятельностью DHS в области кибербезопасности.

Соединенные Штаты Америки на сегодняшний день обладают наиболее развернутым и проработанным законодательством, касающимся информационной безопасности в целом и уголовно-правового регулирования отношений в сфере использования IT-технологий в частности. Первый закон о защите информации был принят в США в 1906 г. На сегодняшний день в США насчитывается около 500 нормативных актов по защите информации[1]. Однако первый законопроект, устанавливающий уголовную ответственность за преступления в сфере информационных технологий, появился в 1977 г. (Computer Crime Bill)[2]. Закон «О компьютерном мошенничестве и злоупотреблении устройствами для несанкционированного доступа» 1984 г. (Counterfeit Access Device and Computer Fraud and Abuse Act 1984)[3] впервые ввел запрет на несанкционированный доступ и использование компьютеров и компьютерных сетей. Затем на его основе в октябре 1986 г. был принят Закон «О мошенничестве и злоупотреблении с использованием компьютеров» (Computer Fraud and Abuse Act)[4]. Данный документ впоследствии претерпел неоднократные изменения. В частности, в 1994 г. в Закон были внесены изменения для противодействия использованию и распространению вредоносного кода, предназначенного для изменения, повреждения или уничтожения данных на компьютере (вирусы, черви и другие программы). В 1996 г. Законом «О защите национальной информационной инфраструктуры» (National Information Infrastructure Protection Act 1996)[5] было расширено определение понятия «компьютерное преступление».

---

[1] См., например: Закон «О свободе информации» (1967); Закон «О секретности» (1974); Закон «О праве на финансовую секретность» (1978); Закон «О доступе к информации о деятельности ЦРУ» (1984); Закон «О безопасности компьютерных систем» (1987); директивы президентов США: политика в области защиты систем связи (1977, Д. Картер), Национальная политика США в области безопасности систем связи автоматизированных информационных систем (1984, Р. Рейган).

[2] Stein Schjolberg. Op. cit. P. 7.

[3] Public Law 98-473, Counterfeit access device and computer fraud and abuse act 1984, October 12, 1984. URL: http://www.gpo.gov.

[4] Public Law 99-474, Computer Fraud and Abuse Act, October 16, 1986. URL: http://www.gpo.gov

[5] Title II, Public Law 104-294, National Information infrastructure protection act, October 11, 1996. URL: http://www.gpo.gov

Положения Закона «О мошенничестве и злоупотреблении с использованием компьютеров» были включены в гл. 47 раздела 18 Уголовного кодекса США[1]. Статьи 1028–1030 упомянутого Кодекса предусматривают ответственность за широкий спектр противоправных деяний, в частности, за «мошенничество и сопряженную деятельность с использованием документов, удостоверяющих личность, средств аутентификации и информации» (ст. 1028), за «мошенничество и сопряженную деятельность с использованием средств доступа» (ст. 1029). К сопряженной деятельности законодателем отнесены «изготовление, торговля и хранение оборудования для изготовления средств доступа, продажа информации о средствах доступа или приложений для их получения» (ч. 3, 4 ст. 1029). Примечательно, что ч. 7 предусмотрена ответственность «за сознательное и с намерением обмануть использование, производство, сбыт и хранение телекоммуникационного инструмента, который был изменен для получения несанкционированного доступа к телекоммуникационным услугам»; частями 8, 9 и 10 – за аналогичные действия, «совершенные с целью обмана при помощи сканирующего устройства и аппаратного или программного обеспечения, предназначенного для неправомерного получения телекоммуникационных услуг либо доступа к банковскому счету кредитной карты, без ведома владельца с целью оплаты одной или более сделок»[2].

С.А. Боженок справедливо отмечает, что при конструкции ст. 1029 был применен «подход, основанный на поведении лиц, совершающих незаконные действия»[3]. Такой подход дает возможность предусмотреть ответственность за большинство видов манипуляций со средствами доступа. Кроме того, большое значение имеет использование обобщенного понятийного аппарата, что значительно расширяет сферу действия данной нормы и позволяет квалифицировать по указанной статье новые формы преступных действий, тем самым делая ее универсальной.

Стоит отметить, что и отечественным законодателем выбран аналогичный подход. Об этом свидетельствуют изменения, внесенные Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» в ст. 158, 159.3 и 159.6 УК РФ.

---

[1] URL: http://www.law.cornell.edu/uscode/text/18/1028

[2] URL: http://www.energy.gov/sites/prod/files/cioprod/documents/computerfraud-abuseact.pdf

[3] Боженок С.А. Зарубежный опыт уголовно-правовой борьбы с преступлениями, совершаемыми с использованием банковских карт // Гражданин и право. 2006. № 4. С. 72–76.

В ст. 1030 Закона «О мошенничестве и злоупотреблении с использованием компьютеров» криминализированы семь видов преступных деяний:

несанкционированный доступ к компьютеру для получения информации о национальной безопасности с целью нанести вред США или в пользу иностранного государства;

несанкционированный доступ для получения защищенной финансовой или кредитной информации;

несанкционированный доступ к компьютеру, используемому Федеральным правительством;

несанкционированный доступ к защищенному компьютеру с целью совершения мошенничества;

умышленное повреждение защищенного компьютера;

торговля паролями и другой информацией, которая может быть использована для получения доступа к защищенному компьютеру;

угроза атаки защищенного компьютера с целью вымогательства денег или чего-либо ценного.

Понятие «защищенный компьютер» определяется в Законе как компьютер, используемый финансовым учреждением или правительством Соединенных Штатов, либо компьютер, используемый в межгосударственной или внешней торговле или коммуникации.

Статьей 1030 (a) (1) запрещается доступ к компьютеру без разрешения или сверх разрешенного доступа для получения информации о национальной обороне, внешних сношениях или ограниченных данных, как это определено в Законе «Об атомной энергии» 1954 г., который охватывает все данные, касающиеся разработки, производства или использования атомного оружия и производства ядерного материала. Следует отметить, что ст. 1030 (a) (1) требует доказательств того, что лицо сознательно осуществляло доступ к компьютеру без разрешения или сверх разрешенного доступа с целью получения секретной или защищенной информации.

Статьей 1030 (a) (2) предусмотрена ответственность за преднамеренный доступ к компьютеру без разрешения или сверх разрешенного доступа для получения записей финансового учреждения или для получения личных данных владельцев платежных карт, покупателей и иных сведений, предусмотренных Законом о кредитной отчетности.

Этой статьей также запрещен доступ для получения информации от любого департамента или агентства Соединенных Штатов

либо любого защищенного компьютера, участвующего в межгосударственных или иностранных коммуникациях. Статьей 1030 (a) (2), охватывающей широкий спектр компьютеров, криминализирован несанкционированный доступ к любому федеральному компьютеру или любому компьютеру, принадлежащему финансовой организации. Статья о защите компьютеров, участвующих в межгосударственной или внешней коммуникации, является самой объемной из всех. Она потенциально может охватывать почтовые серверы, маршрутизаторы и даже персональные компьютеры, если можно убедительно доказать, что они используются в межгосударственной связи.

Статьей 1030 (a) (3) охватывается несанкционированный доступ к любому федеральному правительственному компьютеру. Несмотря на внешнюю схожесть частей (a) (2) и (a) (3) ст. 1030, охватываемые ими деяния различны. Статьей 1030 (a) (2) охватывается доступ к компьютерам федерального правительства с целью получения защищенной информации, а ст. 1030 (a) (3) – полностью несанкционированный доступ к федеральным компьютерам независимо от того, была ли получена какая-либо информация или нет.

Статья 1030 (a) (4) охватывает компьютерное мошенничество и использование компьютера с целью совершения мошенничества. При этом уголовная ответственность наступает только в том случае, если размер причиненного ущерба превышает 5 тыс. долл. США в любой годичный период. Указанный порог был принят Конгрессом США для предотвращения признания мошенничеством каждого случая нарушения целостности компьютерной информации.

Статья 1030 (a) (5) является, пожалуй, наиболее широко используемой статьей Закона «О мошенничестве и злоупотреблении с использованием компьютеров». Она охватывает взлом и распространение вредоносного кода, например вирусов и червей, которые наносят или пытаются нанести ущерб защищенным компьютерам. Деяние признается преступным, если был поврежден компьютер или предпринята попытка его повреждения, что повлекло финансовые потери более 5 тыс. долл., потерю или изменение медицинских данных, физический вред здоровью человека, угрозу безопасности правосудия или здоровья населения, угрозу национальной обороне или национальной безопасности.

Статьей 1030 (a) (6) охватывается торговля паролями или аналогичной информацией, которая может использоваться для доступа к компьютерам. Деяние признается преступным, если такая торговля затрагивает межгосударственную или иностранную торговлю либо компьютер, о котором идет речь, используется правительством США.

Статьей 1030 (a) (7) предусмотрена ответственность за использование межгосударственных или иностранных средств связи для атак на защищенный компьютер с целью вымогательства денег или других ценных вещей. Указанная статья охватывает использование любого межгосударственного или международного метода связи при передаче атак в отношении компьютеров, компьютерных сетей, их данных и программ, включая почту, телефон или любую компьютерную связь.

На сегодняшний день в США существует самая жесткая система защиты информации, включающая в себя контроль за обеспечением режима секретности в учреждениях и организациях; специальную проверку лиц, получивших доступ к закрытой информации.

Если в период с конца 2000 по 2009 г. основные законотворческие инициативы Конгресса США были направлены на создание действенной системы правоохранительных органов по обеспечению информационной безопасности государства (например, Закон «О национальной безопасности» 2002 г.[1], согласно которому было создано Агентство национальной безопасности – АНБ), создание центров изучения киберпреступности (Закон «О научных исследованиях и разработках в области кибербезопасности» 2002 г.)[2] и стандартов по обеспечению информационной безопасности (Федеральный закон «Об управлении информационной безопасностью» 2002 г.)[3], то с 2010-х гг. основные усилия были направлены на интеграцию усилий общества, бизнеса и государства в лице правоохранительных органов по обеспечению информационной безопасности, информационного обмена о происшествиях в IT-сфере (Закон «Об оценке рабочей силы в области кибербезопасности» 2014 г.[4], Национальный закон «О кибербезопасности» 2014 г.[5], Федеральный закон «О модернизации информационной безопасности» 2014 г.[6]).

Как уже отмечалось, американское общество весьма настороженно относится к вопросам сохранности персональных данных и не

---

[1] Titles II and III, Public Law 107-296, Homeland security Act, November, 25, 2002. URL: http://www.gpo.gov

[2] Public Law 107-305, Cybersecurity Research and development Act, November, 27, 2002. URL: http://www.gpo.gov

[3] Title III – Information security, Public Law 107-347, Homeland security Act, November, 25, 2002. URL: http://www.gpo.gov

[4] Public Law 113-246, Cybersecurity workforce assessment Act, December, 18, 2014. URL: http://www.gpo.gov

[5] Public Law 113-282, National cybersecurity Act, December, 18, 2014. URL: http://www.gpo.gov

[6] Public Law 113-283, Federal information security modernization Act, 18, 2014. URL: http://www.gpo.gov

чувствует себя в сети защищенным. Во многом это объясняется объективными причинами. Спровоцированная после терактов 11 сентября 2001 г. волна законотворческих инициатив по расширению полномочий правоохранительных органов по слежке и перехвату данных привела к серьезным нарушениям и перегибам в указанной сфере. Принятый в 1986 г. Закон «О конфиденциальности электронных коммуникаций» (Electronic Communications Act), запрещавший несанкционированное прослушивание телефонных разговоров, незаконный перехват сохраненных или переданных электронных сообщений, претерпел в 2002 г. значительные изменения после принятия Закона «Об укреплении кибербезопасности» (Cyber Security Enhancement Act (CSEA).

Указанный Закон был принят вместе с Законом «О национальной безопасности» 2002 г., предоставил широкие полномочия правоприменительным органам и ужесточил наказания за большинство преступных деяний в IT-сфере. Масштабы слежки за гражданами и иностранными резидентами специальными службами США были преданы широкой огласке после скандального разоблачения агента АНБ Э. Сноудена в 2013 г. Ввиду этого поиск баланса между защитой персональных данных и обеспечением национальной безопасности в условиях развивающейся цифровой экономики продолжает оставаться наиболее животрепещущей проблемой.

18 декабря 2015 г. был принят Закон «Об обмене информацией в целях кибербезопасности» (Cybersecurity Information Sharing Act of 2015)[1], согласно которому все государственные учреждения и частные компании обязаны представлять всю информацию, касающуюся кибербезопасности, в соответствующие компетентные органы[2]. Конгресс США рассматривает также законопроект об информационной безопасности, который предусматривает ужесточение наказания за киберпреступления и фактическое уравнивание их общественной опасности с реальными преступлениями[3]. Особое внимание в данном законопроекте уделяется экономическому шпионажу и хищениям интеллектуальной собственности. При этом ряд санкций за уже существующие составы преступлений увеличивается с 15 до 20–30 лет при проникнове-

[1] Public Law 114-113, Cybersecurity Act of 2015, December, 18, 2015. URL: http://www.gpo.gov

[2] Commission on enhancing national cybersecurity. Report on securing and growing the digital economy, December 1, 2016.

[3] Законодательство о киберпреступлениях в зарубежных странах // РИА Новости. URL: http://www.ligainternet.ru/publications/publication.php?ID=2065

нии в компьютерные сети инфраструктуры США (телесети, энергосети, транспортные каналы связи, системы управления водоснабжением).

Под уголовно-правовой охраной раздела 17 Кодекса США находится интеллектуальная собственность. В 1998 г. был принят Закон «Об авторском праве в цифровую эпоху» (Digital Millennium Copyright Act – DMCA). Основной его целью было изменение раздела 17 Кодекса Соединенных Штатов, а также реализация Договора Всемирной организации интеллектуальной собственности (ВОИС) об авторском праве и Договора о записях и фонограммах, которые были разработаны для обновления мировых законов об авторском праве с целью работы с новой технологией.

Указанным Законом, в частности, был введен запрет на обход технологических мер, предназначенных для защиты авторских прав. Ответственность предусмотрена также за производство и продажу устройств или программ, основной целью которых является обход технологических мер. Под технологическими мерами следует понимать технологии контроля доступа, при этом формы их выражения могут быть различными – от защиты от копирования до необходимости введения специальных код-ключей. Закон предусматривает гражданско-правовые, а также уголовные наказания за нарушение авторских прав.

Данный Закон включает также положения, предусматривающие широкий иммунитет от ответственности для интернет-провайдеров (например, интернет-провайдеры не несут ответственности за передачу материалов, нарушающих авторские права, через их сеть и компьютеры, если интернет-провайдер не контролирует содержание материалов в своей сети и никакие копии не хранятся в системе поставщика услуг).

Для противодействия IT-преступлениям могут также применяться положения Закона «Об экономическом шпионаже» (Economic Espionage Act – EEA) 1996 г. Указанным Законом криминализировано незаконное получение коммерческой тайны для передачи ее иностранному правительству или иностранному агенту. Закон также содержит положения, квалифицирующие в качестве преступления умышленное хищение коммерческой тайны или попытку такого хищения с целью принести пользу кому-либо, кроме владельца коммерческой тайны.

Закон определяет хищение коммерческой тайны как «копирование, дублирование, создание эскизов, рисование, фотографирование, загрузку, фильтрацию, уничтожение, фотокопирование, тиражирование, передачу, доставку, отправку по почте, пересылку коммерческой

тайны без разрешения». Хотя этот Закон и не направлен конкретно против компьютерных преступлений, тем не менее, он охватывает использование компьютеров.

Помимо уже упомянутых законодательных актов, за совершение преступных деяний в IT-сфере могут применяться также и нормы законов о «традиционных» кражах и мошенничествах.

Учитывая специфику системы права в США, в которой уголовное законодательство регулируется каждым штатом самостоятельно в дополнение к федерельному законодательству, считаем целесообразным рассмотреть опыт уголовно-правового противодействия отдельных штатов преступлениям в цифровой экономике.

На уровне штатов принято считать, что кража информации или денег в электронной форме во многом аналогична краже в любой другой форме. Таким образом, законы штата, направленные против IT-преступлений, сосредоточены на хищении информации или денег с помощью компьютера или информационно-телекоммуникационных технологий.

Практически во всех штатах основным условием привлечения лица к уголовной ответственности за совершение IT-преступления является наличие умысла на его совершение. Необходимо умышленно, сознательно или намеренно обращаться к компьютерным данным и намереваться украсть, уничтожить или изменить компьютерную информацию; украсть пароли или иным образом мешать компьютерам или сетям. Только несколько штатов явно не запрещают доступ к определенным компьютерным файлам. В большинстве штатов простой доступ (с намерением совершить преступление) признается преступлением. Однако в различных штатах аналогичные деяния могут признаваться проступком либо преступлением.

Законы штата Калифорния (ст. 502 УК Калифорнии «Преступления в сфере компьютерной информации») включают положения, направленные на защиту компьютеров, компьютерных систем и компьютерных сетей физических лиц, предприятий и организаций по всему штату. В Калифорнии криминализированы многие деяния, связанные с компьютерами, влияющие на функциональность, использование или конфиденциальность компьютерных данных, компьютеров, компьютерных систем и компьютерных сетей.

Лицо, которое получает доступ к компьютеру, компьютерной системе или компьютерной сети и изменяет, нарушает, удаляет, уничтожает или иным образом изменяет любую часть информации, может быть обвинено в компьютерном преступлении. Квалификация деяния

зависит от цели неправомерного доступа. Например, прокурору может потребоваться доказать, что обвиняемый хотел осуществить мошенничество или вымогательство либо взять под контроль информацию, деньги или имущество, которые ему не принадлежат.

Предусмотрена ответственность также и за использование вредоносных программ. Кроме того, законы штата Калифорния криминализируют несанкционированное получение или копирование данных и информации с компьютера, компьютерной системы или компьютерной сети. Например, под указанную норму подпадают действия лица, которое берет оцифрованные бизнес-записи из организации либо копирует продукт работы из компьютерной сети работодателя без разрешения[1]. Статьей 502.5 предусмотрена также конфискация имущества, используемого в целях совершения IT-преступления.

Ответственность за указанные деяния предусмотрена в виде штрафа или тюремного заключения либо и того, и другого. Максимальный размер штрафа может составлять от 1 до 10 тыс. долл. США. Срок тюремного заключения в зависимости от тяжести содеянного может варьироваться от одного года до трех лет. Судом также может быть назначена выплата потерпевшему, компенсирующая ущерб от преступления.

В штате Нью-Йорк ответственность за IT-преступления предусмотрена ст. 156 УК. В частности, в законе перечислены пять отдельных преступлений, связанных с компьютерами: несанкционированный доступ к компьютеру; компьютерное вторжение или атака; несанкционированное использование компьютера; незаконное дублирование материалов, связанных с компьютером; незаконное получение информации и данных.

При этом понятие «компьютер» в законодательстве штата Нью-Йорк довольно обширное. Оно охватывает устройства, которые могут автоматически выполнять арифметические, логические операции, операции хранения или извлечения с компьютерными данными, а также включает периферийное оборудование, такое как внутренние и внешние диски, факсы, модемы и принтеры, которые предназначены для хранения, извлечения или передачи результатов компьютерных операций, программ или данных.

В зависимости от тяжести содеянного и вида посягательства наказание может варьироваться от одного года тюрьмы или штрафа до 1 тыс. долл. (за несанкционированное использование компьютера

[1] California Computer Crime Laws. URL: https://statelaws.findlaw.com/california-law/california-computer-crimes-laws.html

и взлом компьютера четвертой степени) до 15 лет тюремного заключения или штрафа до 5 тыс. долл. либо двойной прибыли обвиняемого от совершения преступления (за компьютерное мошенничество первой степени).

В штате Иллинойс ответственность за IT-преступления предусмотрена Законом «О предотвращении компьютерных преступлений» (Computer Crime Prevention Law – ICCPL). Закон разбит на три основные категории:

несанкционированное использование компьютера, которым охватывается получение незаконного доступа к компьютеру, программе или данным без разрешения владельца, создание или распространение компьютерных вирусов;

незаконное манипулирование компьютером с намерением нарушить или вмешаться в работу или функционирование государственного учреждения или коммунальных служб либо создание серьезной вероятности смерти или нанесения телесных повреждений другим лицам;

компьютерное мошенничество (любое преступление, связанное с использованием компьютера для мошеннического получения денег, товаров или услуг от другой стороны).

В зависимости от штата перечень посягательств в IT-сфере, признанных преступлениями, может варьироваться. Проведенный нами анализ показал, что в основном под уголовно-правовым запретом в большинстве штатов находятся следующие преступные деяния:

неправомерный доступ к компьютеру, системе или сети;

внедрение вируса или другой вредоносной программы в компьютерную систему;

изменение, повреждение, использование, раскрытие, копирование программ или данных;

использование компьютера в схеме для обмана;

вмешательство в доступ или использование чужого компьютера;

использование шифрования при совершении преступления;

кибербуллинг;

фальсификация информации об источнике электронной почты;

кража информационной услуги у провайдера.

Законы штатов не только заполняют пробелы в федеральном законодательстве, но могут также устанавливать де-факто национальные стандарты. Например, предписание штата Массачусетс о конфиденциальности данных, направленное на противодействие риску краж или мошенничества с идентификационной информацией или приобрете-

нием (использованием) ее для несанкционированных целей. Так, компании, занимающиеся обработкой конфиденциальных персональных данных, должны иметь письменные правила обеспечения информационной безопасности при работе с данными, передаваемыми извне, и конкретные минимальные требования административного, технического и физического контроля[1].

Отдельное внимание в США уделяется и противодействию использованию технологий блокчейн и криптовалют в преступных целях. В 2012 г. ФБР впервые выразило обеспокоенность возможностью осуществления незаконной деятельности в платежной системе Bitcoin, а в августе 2014 г. Бюро финансовой защиты потребителей обратило внимание на риски, связанные с использованием криптовалют. Согласно ежегодному отчету об обороте наркотических средств в США за 2017 г., биткоин явился главным средством расчетов при торговле наркотиками в мире. Так, установлено, что деньги, полученные наркоторговцами в США, обращаются в биткоины, на которые наркоторговцы беспрепятственно покупают китайские товары. Кроме того, подпольные китайские банки покупают наличность у наркоторговцев в США, Европе и Австралии за биткоины и продают эту наличность за биткоины китайским гражданам[2].

Использование криптовалют в преступных целях признано реальной угрозой. В начале июля 2018 г. Австралийская комиссия по преступности (ACIC), Австралийское налоговое управление (ATO), Канадское налоговое агентство (CRA), Служба расследования налоговых преступлений Нидерландов (FIOD), Управление Ее Величества по налогам и таможенным пошлинам (HMRC) и Отдел криминальных расследований Налогового управления США (IRS-CI) создали Международный Альянс J5. Основная функция органа – сотрудничество в сфере противодействия транснациональной организованной преступности и уменьшение растущей угрозы для налоговых органов, создаваемой криптовалютами и киберпреступностью[3].

Контент-анализ периодических изданий свидетельствует о том, что основная угроза в обороте криптовалюты приходится на мошенни-

---

[1] Alan Charles Raul. Touring the World of Cybersecurity Law // RSAConference 2016, February 29 – March 4.

[2] URL: https://telegram.org/#/im?p=@cryptoelina

[3] Международный альянс J5 взялся за налоговые преступления с Биткоином. URL: https://2bitcoins.ru/mezhdunarodnyj-alyans-j5-vzyalsya-za-nalogovye-prestupleniya-s-bitkoinom

ческие ICO. В США на деятельность ICO распространяются требования о рынке ценных бумаг. Осенью 2017 г. в США было возбуждено первое уголовное дело за первичное размещение ICO.

Итак, проведенный анализ показал, что США обладают наиболее проработанным и учитывающим все возможные на сегодняшний день посягательства в IT-сфере уголовным законодательством. Во многом это объясняется восполнением пробелов федерального законодательства законами штатов. Однако желание государства предотвратить совершение преступлений с использованием IT-технологий привело к чрезмерному ужесточению уголовной ответственности и перегибам со стороны правоприменителей, что негативным образом сказывается на развитии в стране цифровой экономики.

С учетом опыта США разрабатывается и европейское законодательство по борьбе с подобными посягательствами, также предусматривающее ответственность за максимальное количество преступлений, совершаемых в IT-сфере.

2.2. Уголовная ответственность за преступления в сфере цифровой экономики в странах Европейского континента

Значение уголовного права в превенции посягательств, связанных с использованием IT-технологий, неоднократно отмечалось европейскими законодателями и являлось неотъемлемой частью дискуссий об обеспечении информационной безопасности. Как было отмечено нами ранее, Конвенция Совета Европы о преступности в сфере компьютерной информации, принятая в Будапеште 23 ноября 2001 г., и Дополнительный протокол к ней[1] являются ключевыми актами в сфере противодействия IT-преступлениям. Вместе с тем европейские законодатели, понимая и осознавая постоянно растущую угрозу посягательств в IT-сфере, направленную на различные объекты уголовно-правовой охраны, продолжают работу по расширению спектра применения уголовно-правовых средств регулирования в различных сферах цифровой экономики. Так, с 11 по 13 июля 2018 г. в Совете Европы

[1] Об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем: дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации № 189 от 1 марта 2006 г. URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/189

планируется проведение конференции, повесткой которой является укрепление верховенства права в киберпространстве посредством принятия Протокола к Будапештской конвенции. Основное внимание в дискуссии планируется уделить расширению международного сотрудничества в борьбе с IT-преступностью, внедрению более эффективных способов обеспечения безопасности электронных доказательств, необходимых для проведения уголовных расследований, доступу к каталогу WHOIS, в котором содержится информация о доменных именах. Ожидается, что работа над Протоколом будет завершена к концу 2019 г. Как отметил Генеральный секретарь Совета Европы Турбьёрн Ягланд, «доступ к доказательствам, хранящимся на виртуальных серверах в «облаке», имеет большое значение для защиты общества и отдельных лиц от киберпреступности. Без данных нет доказательств и, следовательно, нет правосудия. Принятие нового протокола, направленного на защиту доказательств, хранящихся в «облаке», при соблюдении гарантий, установленных верховенством права, станет еще одной важной вехой в истории этого договора»[1].

Указанная работа проводится в рамках реализации принятой 30 марта 2016 г. Комитетом министров Евросоюза Стратегии управления Интернетом на 2016–2019 гг., которая пришла на замену Плана действий на 2010–2014 гг[2]. Основной целью принятия Стратегии является защита прав человека в постоянно изменяющемся цифровом пространстве и «подчинение» новых технологий интересам каждого. В рамках реализации Стратегии планируется решение следующих задач:

содействие созданию сети национальных учреждений для обеспечения правовой защиты пользователей сети Интернет, если их права и интересы были нарушены в IT-пространстве;

проведение раз в три года мониторинга состояния защиты данных и конфиденциальности в Интернете в Европе с учетом модернизации Конвенции о киберпреступности;

разработка политики в отношении роли посредников и их значения в обеспечении свободы выражения мнений и свободы средств массовой информации в свете прецедентного права Европейского Суда по

[1] Конференция по киберпреступности: доказательства в киберпространстве, данные WHOIS, кибернасилие, общемировое состояние законодательства. URL: https://www.coe.int/ru/web/portal/-/conference-on-cybercrime-evidence-in-cyberspace-whois-data-cyberviolence-global-state-of-legislation

[2] Council Document 5842/2/2010. Internal Security Strategy for the European Union: Towards a European Security Model. Brussels, 2010. P. 7–31.

правам человека с учетом передовой практики блокирования, фильтрации и удаления интернет-контента, включая доклады Генерального секретаря по этому вопросу;

периодический мониторинг состояния свободы СМИ и Интернета в соответствии со стандартами Совета Европы, в частности, посредством подготовки докладов Генерального секретаря Совета Европы о состоянии демократии, прав человека и верховенства права в Европе;

создание платформы между правительствами и основными Интернет-компаниями и ассоциациями;

сотрудничество с правительствами и другими сторонами, заинтересованными в управлении Интернетом, мобильным здравоохранением и электронным здравоохранением в целях сохранения и улучшения доступа пациентов ко всем имеющимся (качественным) медицинским услугам[1].

Необходимо отметить, что за последние два десятилетия Евросоюзом посредством принятия директив и рамочных решений была создана достаточно обширная правовая база функционирования различных сегментов цифровой экономики. Большая часть правовых актов направлена на регулирование правоотношений в области гражданского и финансового права, однако их положения создают основу для принятия норм уголовно-правового характера. Учитывая специфику проблем, рассматриваемых в рамках настоящего исследования, остановимся на рассмотрении некоторых правовых актов, устанавливающих общеевропейские стандарты обеспечения информационной безопасности, противодействия IT-преступности, регулирования правоотношений, возникающих при посягательствах в IT-сфере.

Директива Европейского Парламента и Совета ЕС (ЕС) 2016/1148 от 6 июля 2016 г. «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза» направлена на совершенствование общеевропейского сотрудничества в области обеспечения информационной безопасности сетевых и информационных систем. Текущая политика ЕС в области обеспечения безопасности критически важной информационной инфраструктуры

[1] Internet Governance – Council of Europe Strategy 2016-2019 Democracy, human rights and the rule of law in the digital world // Documents and Publications Production Department (SPDP), Council of Europe, September 2016.

построена на пяти столпах: готовность и предотвращение; обнаружение и реагирование; смягчение последствий; восстановление; международное сотрудничество[1].

В Директиве отмечается необходимость установления единой системы действий на уровне Союза, охватывающей общие минимальные требования по наращиванию потенциала и требования по планированию к операторам основных услуг и провайдерам цифровых услуг по обмену информацией, взаимодействию и обеспечению общей безопасности. Ввиду этого отмечается необходимость принятия всеми государствами – членами ЕС национальных стратегий по обеспечению безопасности указанных систем. Особо стоит отметить положения Директивы, обязывающие государства – члены ЕС идентифицировать операторов основных услуг, учрежденных на их территории в энергетической, транспортной, банковской сферах, в здравоохранении, поставке и дистрибуции питьевой воды, в инфраструктурах финансового рынка и цифровизации[2].

Директива Европейского парламента и Совета ЕС 2013/40/ЕС от 12 августа 2013 г. «Об атаках на информационные системы и о замене Рамочного решения 2005/222/ПВД Совета ЕС» наряду с Конвенцией Совета Европы о преступности в сфере компьютерной информации направлена на «сближение уголовного законодательства государств – членов ЕС в отношении атак на информационные системы путем установления минимально необходимых правил по определению преступлений и соответствующих наказаний; улучшение взаимодействия между уполномоченными органами, в том числе полиции и других специализированных правоохранительных служб государств – членов ЕС, а также включая уполномоченные специализированные агентства и органы ЕС, такие как Евроюст, Европол, его Европейский центр по борьбе с киберпреступностью и Европейское агентство по безопасности сети и информации (ENISA)»[3].

Указанной Директивой предусмотрена уголовная ответственность за создание ботнетов, а именно, за действие по установлению удаленного контроля за значительным количеством компьютеров путем заражения

---

[1] Cybersecurity: Protecting the digital economy. URL: https://www.euractiv.com/section/digital/linksdossier/cybersecurity-protecting-the-digital-economy

[2] О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза: директива Европейского парламента и Совета ЕС (ЕС) 2016/1148 от 6 июля 2016 г. // Официальный журнал Евросоюза. NL 194. 19.07.2016. С. 1.

[3] Об атаках на информационные системы и о замене Рамочного Решения 2005/222/ПВД Совета ЕС: директива Европейского парламента и Совета Европейского Союза 2013/40/ЕС от 12 авг. 2013 г. URL: https://www.coe.int/ru/web/conventions

их вредоносным программным обеспечением посредством нанесения целевых компьютерных атак. Ответственность предусмотрена за незаконный доступ к информационным системам (ст. 3), незаконное вмешательство в систему (ст. 4), незаконное нарушение сведений (ст. 5), незаконный перехват информации (ст. 6). Государства – члены ЕС с точки зрения их национального законодательства вправе самостоятельно определить, что включает в себя серьезный ущерб. Таким ущербом может быть повреждение системных служб, имеющих существенное значение для общества, крупные финансовые расходы либо потеря персональных данных или конфиденциальной информации. В Директиве также отмечается целесообразность более сурового наказания при совершении атаки на информационную систему преступной организацией, когда совершение компьютерных атак производится в крупном масштабе, тем самым поражая значительное количество информационных систем, в том числе когда предполагается создание ботнета либо атака совершается на объекты жизнеобеспечения государств – членов ЕС или ЕС в целом. Минимальное наказание за совершение указанных преступлений составляет два года лишения свободы.

Интересной в рассматриваемом аспекте также представляется Резолюция ПАСЭ 2070 (2015) «Расширение сотрудничества в борьбе с кибертерроризмом и другими широкомасштабными агрессивными действиями в Интернете». В тексте Резолюции отмечается необходимость создания систем защиты критически важной информации, не зависящих от Интернета, в целях национальной безопасности, безопасности населения и экономического благополучия государств. В указанных целях всем государствам-членам рекомендовано ввести уголовное наказание за производство, распространение и применение вредоносных программных средств, предназначенных для того, чтобы частные лица имели возможность подготовить или провести широкомасштабные кибератаки[1].

Эмиссия электронных денег на территории ЕС осуществляется на основании требований, установленных в Директиве Европейского парламента и Совета ЕС 2009/110/ЕС от 16 сентября 2009 г. «Об учреждении и деятельности организаций, эмитирующих электронные деньги, о пруденциальном надзоре за их деятельностью, а также об изменении

[1] Расширение сотрудничества в борьбе с кибертерроризмом и другими широкомасштабными агрессивными действиями в Интернете: резолюция ПАСЭ 2070 (2015). URL: https://nxtp://assembly.coe.int

директив 2005/60/ЕС и 2006/48/ЕС и об отмене Директивы 2000/46/ЕС»[1].

Стоит отметить, что в Директиве Европейского парламента и Совета ЕС 2015/849 от 20 мая 2015 г. «О предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма, об изменении Регламента (ЕС) 648/2012 Европейского парламента и Совета ЕС и об отмене Директивы 2005/60/ЕС Европейского парламента и Совета ЕС и Директивы 2006/70/ЕС Европейской Комиссии» особо подчеркивается, что «меняющийся характер угроз, связанных с отмыванием денег и финансированием терроризма, которому способствует постоянная эволюция технологий и средств, находящихся в распоряжении преступников, требует оперативной и постоянной адаптации нормативно-правовой базы в отношении третьих стран с высоким уровнем риска в целях эффективного устранения существующих рисков и предотвращения возникновения новых»[2].

В апреле 2018 г. в указанную Директиву были внесены изменения, направленные на усиление контроля за криптовалютами. Новые правила вводят обязательную регистрацию платформ и поставщиков услуг хранения криптовалют. Данная мера направлена на искоренение анонимности, присущей криптовалютам, платформам обмена ими и виртуальным кошелькам. Указанные платформы, как и банки, должны будут применять контроль клиента с должной осмотрительностью, включая требования к проверке клиентов. Государствам-членам будет отведено 18 месяцев, чтобы имплементировать новые нормы в национальное законодательство[3].

Правила обработки персональных данных определены в Регламенте Европейского парламента и Совета ЕС 2016/679 от 27 апреля 2016 г. «О защите физических лиц при обработке персональных

---

[1] Об учреждении и деятельности организаций, эмитирующих электронные деньги, о пруденциальном надзоре за их деятельностью, а также об изменении директив 2005/60/ЕС и 2006/48/ЕС и об отмене Директивы 2000/46/ЕС: директива Европейского парламента и Совета ЕС 2009/110/ЕС от 16 сент. 2009 г. // Официальный журнал Евросоюза. NL 267. 10.10.2009. С. 7.

[2] О предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма, об изменении Регламента (ЕС) 648/2012 Европейского парламента и Совета ЕС и об отмене Директивы 2005/60/ЕС Европейского парламента и Совета ЕС и Директивы 2006/70/ЕС Европейской Комиссии: директива Европейского парламента и Совета ЕС 2015/849 от 20 мая 2015 г. // Официальный журнал Евросоюза. NL 141. 05.06.2015. С. 73.

[3] Европарламент ужесточил контроль за криптовалютами. URL: https://ru.slovoidilo.ua/2018/04/20/novost/mir/evroparlament-uzhestochil-kontrol kriptovalyutami

данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)».

Охрану интеллектуальной собственности обеспечивают Директива Европейского парламента и Совета ЕС 2001/29/ЕС «О гармонизации некоторых аспектов авторских и смежных прав в информационном обществе» и Директива Европейского парламента и Совета ЕС 2004/48/ЕС от 29 апреля 2004 г. «Об обеспечении прав на интеллектуальную собственность».

Меры, предусмотренные в директивах и рамочных соглашениях, направлены на гармонизацию и унификацию законодательства на территории стран Евросоюза, а также на содействие международному сотрудничеству. И положительные результаты в указанном направлении есть. В апреле 2018 г. Европол сообщил об успешном проведении совместно с правоохранительными органами Испании, Финляндии и США операции Tulipan Blanca, в результате которой была пресечена деятельность организованной преступной группы, занимавшейся отмыванием денег от незаконного оборота наркотиков через использование криптовалют и платежных карт. В ходе расследования было установлено, что преступники приобретали кредитные карты, связанные с банковскими счетами, на которые были депонированы преступные доходы. Затем некоторые преступники отправлялись в Колумбию с кредитными картами и снимали наличные деньги с банковских счетов. В дальнейшем преступники стали использовать для отмывания криптовалюту, преимущественно биткойн. Во взаимодействии с финскими властями сотрудники полиции смогли обнаружить, что для отмывания использовалась финская криптобиржа. Преступники использовали биржу для конвертации своих незаконных доходов в биткоины, а затем в тот же день меняли криптовалюту на фиатную валюту и размещали на колумбийские банковские счета[1].

На национальном уровне в каждом государстве приняты собственные, дополняющие вышеуказанный перечень преступлений законодательные акты, предусматривающие уголовную ответственность за посягательства в IT-сфере.

Стоит отметить, что в топ-10 стран с наиболее развитой цифровой экономикой и, соответственно, с наиболее эффективной системой

[1] Illegal network used cryptocurrencies and credit cards to launder more than EUR 8 million from drug trafficking. URL: https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking

противодействия IT-преступлениям входят европейские страны, не являющиеся членами Евросоюза. Так, Норвегия и Швейцария не входят в ЕС, однако тесно с ним взаимодействуют. Они состоят в Европейской ассоциации свободной торговли, являясь тем самым частью Европейской экономической зоны, а также имеют ассоциированное членство в Шенгенской зоне. Во время референдума 2016 г. население Великобритании проголосовало за выход из Европейского союза, который она покинет в марте 2019 г.

Рассмотрим более подробно вопросы уголовно-правового регулирования IT-сферы в указанных странах.

Норвегия на протяжении длительного времени является страной с низким уровнем преступности. Особое внимание в стране уделяется и вопросам противодействия преступлениям в IT-сфере. Стратегические приоритеты Норвегии в обеспечении кибербезопасности определяются необходимостью создания безопасных, стабильных и надежных цифровых сетей, используемых во всех сферах деятельности общества – в энергоснабжении, водоснабжении, здравоохранении, работе транспорта, общественной безопасности и на финансовых рынках.

В декабре 2012 г. Кабинетом министров Норвегии была принята Стратегия кибербезопасности Норвегии (Cyber Security Strategy for Norway)[1], в которой отмечается, что общество будет продолжать развиваться за счет более широкого использования информационно-телекоммуникационных технологий, что предопределяет необходимость защиты информации и обеспечения постоянной стабильности сетей и систем. При этом особо подчеркивается, что необходима консолидация усилий государства, бизнеса и всего общества. Проблемы безопасности IT-технологий охватывают все уровни общества – от защиты отдельных мобильных телефонов до защиты систем, обеспечивающих важнейшие социальные функции.

Цифровая экономика продолжает быстро расширяться и является основной движущей силой создания стоимости, инноваций, конкурентоспособности и роста. Киберпространство способствует росту занятости населения, обеспечивая основу для инвестиций и инноваций, обеспечивая доступ к более крупным рынкам и уменьшая важность географического положения. Даже малые предприятия могут теперь привлекать клиентов во всем мире без значительных дополнительных затрат. Для реализации указанных целей и стимулирования роста норвежской цифровой экономики необходимы содействие глобальной открытости

[1] Cyber Security Strategy for Norway. URL: https://www.regjeringen.no/globalassets/upload/fad/vedlegg/iktpolitikk/cyber_security_strategy_norway.pdf

в Интернете, содействие развитию цифровых инноваций в частном и государственном секторах экономики, защита интеллектуальной собственности, поддержание роста цифровой экономики в сотрудничестве с другими государствами – членами ОЭСР[1].

В Стратегии выделены следующие основные проблемы и тенденции, характеризующие нынешнюю ситуацию:

Интернет и мобильные устройства, имеющие повсеместное распространение;

критическая зависимость инфраструктур от сбоев в работе информационно-телекоммуникационных технологий;

развитие новых сервисных платформ и отсутствие ясности при оценке рисков и уязвимостей при обеспечении собственной безопасности;

широкое привлечение зарубежных компаний для аутсорсинга при разработке систем, что приводит к ряду проблем безопасности и чрезвычайным ситуациям;

шпионаж и саботаж;

усложнение систем и сетей ИКТ, что также затрудняет для поставщиков систем установление четких и точных требований безопасности;

должностные преступления (внутренний вандализм, хищение или неправомерное использование ИКТ-ресурсов организации ее собственными сотрудниками, которые зачастую трудно обнаружить);

злоупотребление личными данными и угрозы от новых методов коммуникации;

международное внимание.

В Стратегии международной кибербезопасности Норвегии 2017 г.[2] в числе приоритетных направлений указано содействие международному сотрудничеству в области кибербезопасности в целях создания потенциала для выявления противоправных инцидентов в киберпространстве.

Сотрудничество с ЕС в области кибербезопасности имеет большое значение для Норвегии. Правительство продолжает работу по оптимизации этого сотрудничества, в том числе путем реализации Директивы по безопасности сетей и информационных систем и работы с Европейским агентством по информационной безопасности (ENISA).

В Стратегии кибербезопасности Норвегии особое внимание уделяется также вопросам противодействия преступлениям в цифровой

[1] International cyber strategy for Norway 2017. Published by Norwegian Ministry of Foreign Affairs.

[2] Там же.

экономике. Отмечается, что киберпреступность включает в себя преступления, направленные на компьютерные системы и сети, и преступления, в которых ключевые элементы цепи событий совершаются с использованием компьютеров или компьютерных сетей. Между ними нет четкого разделения. Преступники также все чаще используют новые технологии для совершения традиционных преступлений.

Основные нормы, устанавливающие уголовную ответственность за посягательства в IT-сфере, содержатся в Уголовном кодексе Норвегии[1]. Параграфом 145 предусмотрена ответственность в виде штрафа либо лишения свободы на срок до 6 месяцев за неправомерный доступ к данным или программам, которые хранятся или передаются с помощью электронных или иных технических средств. Однако наказание может быть увеличено до 6 лет, если будет установлено, что преступление совершено с целью получения незаконной выгоды для какого-либо лица.

Параграфом 145b предусмотрена ответственность в виде штрафа и (или) лишения свободы сроком до 6 месяцев за незаконную передачу компьютерного пароля или аналогичных данных, с помощью которых можно получить доступ ко всей компьютерной системе или к любой ее части. При этом норвежский законодатель в абз. 2 указанной нормы использует понятие серьезности: серьезное распространение данных о доступе наказывается лишением свободы на срок до двух лет. При принятии решения о том, является ли распространение серьезным, особое внимание уделяется тому, может ли переданная информация предоставлять доступ к конфиденциальной информации, является ли распространение обширным и существует ли опасность причинения значительного ущерба.

Параграфом 151b предусмотрена ответственность за нанесение ущерба объектам критической инфраструктуры, таким как электроснабжение, радиовещание, телекоммуникации или транспорт. За их уничтожение, повреждение, повлекшие проблемы в государственном управлении или общественной жизни, предусмотрено наказание в виде тюремного заключения на срок до 10 лет. Если указанные деяния были совершены по неосторожности, то наказание может быть в виде штрафа либо лишения свободы на срок до одного года.

Согласно результатам исследования, проведенного компанией PricewaterhouseCooper (PWC), киберпреступность в Швейцарии стала вторым самым распространенным видом экономического мошенничества. Экономические преступления, совершаемые в Интернете, стали

[1] URL: http://www.cybercrimelaw.net/Norway.html

обыденными фактами швейцарской действительности[1]. Несмотря на передовые позиции Швейцарии в области развития и внедрения цифровых технологий и цифровой экономики в целом, в вопросах обеспечения кибербезопасности страна также имеет определенные проблемы. В интервью швейцарской ежедневной газете Der Bund министр обороны Швейцарии Ги Пармелен отметил, что «Швейцария почти ежедневно подвергается электронным атакам из-за рубежа». В 2016 г. было зарегистрировано более 14 тыс. кибератак на Швейцарию[2]. В рейтинге стран, опубликованном Международным союзом электросвязи (МСЭ), Швейцария в соответствии с индексом кибербезопасности занимает 18-е место[3].

До настоящего времени в Швейцарии не было принято специального законодательства в области кибербезопасности, а также нет планов всеобъемлющего решения этого вопроса в специальном правовом документе. Кибербезопасность регулируется различными законодательными актами и нормативными указаниями. Фактически соответствующий законодательный ландшафт был проанализирован в докладе о Национальной стратегии по защите Швейцарии от киберугроз, который был одобрен Федеральным правительством в 2012 г.[4] В докладе излагается существующая схема защиты от киберпреступности и определяются основные цели усиления защиты от киберугроз. После выявления рисков, связанных с киберугрозами, в докладе освещаются основные недостатки и решается вопрос о том, как должны действовать различные заинтересованные стороны. В Стратегии подчеркиваются три основные цели: раннее выявление угроз и опасностей; повышение устойчивости критически важных объектов инфраструктуры; снижение киберрисков, особенно киберпреступности, кибершпионажа и саботажа.

В конечном итоге в докладе провозглашается 16 мер, направленных на минимизацию киберрисков и повышение кибербезопасности, одна из которых посвящена «валидации» существующих нормативных правовых актов.

---

[1] В Швейцарии воруют в киберпространстве. URL: http://nashagazeta.ch/news/12610

[2] Швейцария постоянно подвергается кибератакам. URL: http://www.swissinfo.ch

[3] Швейцария заняла 18-е место в рейтинге стран по кибербезопасности. URL: http://nashagazeta.ch/news/politique/shveycariya-zanyala-18-oe-mesto-v-reytinge-stran-po-kiberbezopasnosti

[4] National strategy for Switzerland’s protection against cyber risks. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Switzerlands_Cyber_Security_strategy.pdf

В докладе признается, что существующая разрозненная правовая база является непоследовательной и неполной, но также высказывается мнение о том, что принятие всеобъемлющего документа о кибербезопасности было бы неуместным для решения проблемы киберугроз. Вместо этого существующая законодательная база будет подвергаться постоянной корректировке с учетом конкретной подверженности киберугрозам в рамках соответствующей сферы применения каждого закона.

Вышеуказанная Национальная стратегия кибербезопасности частично дублирует другую правительственную Стратегию – «Цифровая Швейцария», утвержденную 20 апреля 2016 г.[1] В ней отмечено, что цифровая революция затрагивает не только промышленность, но и все сектора экономики, включая такие сферы, как здравоохранение, культура, СМИ, туризм. Стратегия направлена на закрепление позиций Швейцарии как страны, обладающей одной из ведущих инновационных экономик в мире. Документ выдвигает 25 задач и перечисляет 52 мероприятия для их достижения[2]. Соответствующий план действий включает, в частности, анализ последствий Стратегии кибербезопасности, включая рассмотрение аспектов международного сотрудничества, особенно с ЕС, в отношении сетевой и информационной безопасности.

Швейцария наряду с другими европейскими странами присоединилась к Будапештской Конвенции о киберпреступности. Присоединение Швейцарии к Конвенции привело к внесению некоторых незначительных поправок в УК Швейцарии и Федеральный закон о международной взаимной помощи по уголовным делам в целях приведения внутреннего законодательства в соответствие с требованиями Конвенции.

Защита данных осуществляется на основании положений Федерального закона «О защите данных» (Federal Data Protection Act, FDPA), регулирующего защиту персональных данных, включающих в себя информацию, относящуюся к идентифицированным или идентифицируемым физическим и юридическим лицам. В соответствии со ст. 7 личные данные должны быть защищены от несанкционированной обработки с помощью адекватных технических и организационных мер.

После принятия Общего Регламента о защите персональных данных в рамках ЕС в настоящее время проводится фундаментальный пе-

[1] URL: https://digitalswitzerland.com

[2] Цифровая трансформация европейской промышленности затронет каждого. URL: http://group-global.org/en/node/121984

ресмотр Федерального закона «О защите данных». Цель пересмотра законодательства заключается в усилении защиты персональных данных и приведении FDPA в соответствие новым правилам ЕС в отношении защиты данных. Проект расширяет права субъектов данных, повышает прозрачность обработки данных и ужесточает обязательства контроллеров и процессоров данных. Он согласовывает FDPA с международными правилами защиты данных, приводя его в соответствие содержанию пересмотренной Конвенции ETS 108 Совета Европы и Европейского закона о защите данных 2016/679 (EU General Data Protection Regulation 2016/679, GDPR)[1]. Таким образом, Швейцария, которая считается одной из лидирующих стран в отношении конфиденциальности данных, принимает дальнейшие меры для их защиты. Новый закон должен вступить в силу 1 августа 2018 г. и привести к широкомасштабным изменениям не только в самой FDPA, но и в других законах, затрагивающих вопросы защиты данных. В частности, юридические лица больше не будут пользоваться специальной защитой данных, будет усилена прозрачность, в большинстве случаев придется уведомлять о нарушениях, а также будут усилены уголовные санкции за преступления в области защиты данных.

Федеральный закон «О телекоммуникациях» (TCA), содержащий положения о безопасности и доступности телекоммуникационных услуг, проходит процесс пересмотра в целях проверки совместимости его положений с текущим технологическим ландшафтом. В частности, будут усилены правила против нежелательных сообщений и спама. Кроме того, также были пересмотрены Федеральный закон «О наблюдении за почтовым и телекоммуникационным трафиком» от 6 октября 2010 г., регулирующий мониторинг почтового и телекоммуникационного трафика в режиме реального времени (новый закон должен был вступить в силу 1 марта 2018 г.), и Федеральный закон «О разведывательной службе», который вступил в силу 1 сентября 2017 г. Этот Закон регулирует мониторинг потоков данных в Швейцарию и из Швейцарии в целях противодействия терроризму и обеспечения национальной безопасности[2].

Федеральный закон «Об инфраструктуре финансового рынка» (FinfrAct), вступивший в силу 1 января 2016 г., регулирует организацию и функционирование инфраструктур финансовых рынков, таких

[1] Швейцария меняет закон о защите данных. URL: http://www.towave.ru/pub/shveitsariya-menyaet-zakon-o-zashchite-dannykh.html

[2] Michael Isler, Hugh Reeves and Jürg Schneider. Cybersecurity. Switzerland. URL: https://gettingthedealthrough.com/area/72/jurisdiction/29/cybersecurity-switzerland

как фондовые биржи, многосторонние торговые системы, центральные депозиты или платежные системы[1]. В своих решениях BGer 6B_615/2014 и 6B_456/2007 Федеральный суд Швейцарии постановил, что несанкционированный доступ к защищенной паролем учетной записи электронной почты другого лица подпадает под признаки «хакерского преступления». В 2016 г. несколько хакеров и лиц, угрожающих взломать IT-системы банков, университетов и частных предприятий, были идентифицированы и арестованы в Швейцарии или за рубежом при взаимной правовой помощи иностранных властей[2].

В Уголовном кодексе Швейцарии составы, предусматривающие ответственность за посягательства в IT-сфере, отнесены к разным главам кодекса. В разделе «Преступные деяния против имущества» ответственность предусмотрена за несанкционированное получение данных (ст. 143); несанкционированный доступ к системе обработки данных (ст. 143-bis); повреждение данных (ст. 144-bis); компьютерное мошенничество (ст. 147); производство и выпуск в обращение предметов, предназначенных для незаконной расшифровки кодированных материалов (ст. 150-bis). Статьей 179-quater предусмотрена ответственность за нарушение тайны или неприкосновенности частной жизни с помощью устройства для переноски изображений, а ст. 179-novies – за получение персональных данных без разрешения. Ответственность за промышленный шпионаж предусмотрена ст. 273. В разделе «Преступные деяния против служебных и профессиональных обязанностей» содержится норма об ответственности за нарушение почтовой и телекоммуникационной тайны (ст. 321-quater)[3].

За повреждение данных при DDOS-атаках виновные привлекаются в соответствии со ст. 144-bis. Так, любое лицо, которое без разрешения изменяет, удаляет или делает непригодными для использования данные, хранящиеся или передаваемые в электронной форме, несет ответственность в виде денежного штрафа или лишения свободы сроком до трех лет. Кроме того, данные также могут считаться непригодными для использования, если они все еще существуют, но временно недоступны для авторизованных пользователей, например, из-за DDOS-атаки.

[1] WIPO Lex. URL: http://www.wipo.int/wipolex/ru/profile.jsp?code=CH

[2] URL: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/switzerland

[3] Уголовный кодекс Швейцарии от 21 дек. 1937 г. (по состоянию на 11 июля 2017 г.). URL: http://www.wipo.int/wipolex/ru/profile.jsp?code=CH

В зависимости от целей DDOS-атаки деяния могут быть квалифицированы дополнительно по нормам УК Швейцарии за вымогательство (ст. 156), наказанием за которое является лишение свободы на срок до пяти лет или денежный штраф; за принуждение (ст. 181), наказанием за которое будет денежный штраф или лишение свободы на срок до трех лет; за неправомерное использование телекоммуникационной установки (ст. 179-quater) – штраф; за воспрепятствование, нарушение или создание угрозы для функционирования телекоммуникационной службы или поставщика коммунальных услуг (ст. 239) – денежный штраф или лишение свободы на срок до трех лет.

За совершение фишинга виновные могут быть привлечены в рамках положений ст. 62 Закона Швейцарии «О защите торговой марки», ст. 67 Закона Швейцарии «Об авторском праве» – за незаконное использование товарного знака или авторского права, а также ст. 147 УК Швейцарии – за компьютерное мошенничество (несанкционированное использование данных и передача финансовых активов посредством фишинга).

Кража электронных средств может охватываться несколькими составами. Статья 143 УК Швейцарии предусматривает наказание за несанкционированный сбор данных. Максимальное наказание – лишение свободы сроком на пять лет. Кроме того, любое лицо, передающее производственную или коммерческую тайну, которая не подлежит разглашению в соответствии с законом или контрактной обязанностью, или любое лицо, которое использует указанные данные, может быть приговорено к лишению свободы на срок до трех лет или денежному штрафу в соответствии со ст. 162 УК Швецарии. Наконец, согласно ст. 67 Закона Швейцарии «Об авторском праве» умышленное и незаконное нарушение авторских прав может быть наказано лишением свободы на срок до одного года или денежным штрафом; в случае совершения преступления с целью получения коммерческой выгоды наказание составляет тюремное заключение на срок до пяти лет или денежный штраф.

Как отмечает А.Г. Волеводз, несмотря на отнесение значительного круга уголовно наказуемых деяний к преступлениям против имущества, корыстный мотив не является обязательным элементом их составов. Вместе с тем основные положения УК Швейцарии исходят из того, что данные, собранные электронным или иным подобным обра-

зом, обладают собственной стоимостью, что в случаях преступных посягательств влечет за собой обязанность загладить материальный ущерб[1].

1 марта 2017 г. в Великобритании была принята Стратегия цифровой экономики (UK Digital Strategy 2017)[2]. Основная цель принятия Стратегии – это создание после выхода из Евросоюза экономики, устойчивой к изменениям и пригодной для будущего. Отмечается, что Великобритания всегда была в авангарде цифровых инноваций – с самых первых дней изобретения вычислительной техники до развития Всемирной паутины. Сегодня экономика этой страны трансформировалась в ведущую мировую цифровую экономику. Великобритания имеет самую производительную научную базу и занимает первое место во многих ключевых глобальных показателях качества исследований.

В Стратегии выделены следующие приоритетные направления:

создание в Великобритании цифровой инфраструктуры мирового класса;

предоставление каждому доступа к необходимым цифровым навыкам (цифровые навыки и инклюзивность);

превращение Великобритании в лучшее место для начала и развития цифрового бизнеса (цифровые сектора);

оказание помощи каждому британскому бизнесу в трансформации в цифровой бизнес (широкая экономика);

превращение Великобритании в самое безопасное место в мире для жизни и работы онлайн (безопасное и защищенное киберпространство);

поддержание правительства Великобритании в качестве мирового лидера в обслуживании своих граждан в Интернете (цифровое правительство);

раскрытие возможностей использования данных в экономике Великобритании и повышение доверия общественности к их использованию.

Для достижения указанных целей 27 апреля 2017 г. был принят Закон «О цифровой экономике» (Digital Economy Act 2017), в котором детально регламентировано и раскрыто содержание понятий в сфере

---

[1] Волеводз А.Г., Волеводз Д.А. Уголовное законодательство об ответственности за компьютерные преступления: опыт разных стран // Правовые вопросы связи. 2004. № 1. С. 37–48.

[2] URL: https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy#a-safe-and-secure-cyberspace-making-the-uk-the-safest-place-in-the-world-to-live-and-work-online

обеспечения доступа к цифровым услугам; внесены изменения в нормы, регулирующие работу и развитие цифровой инфраструктуры и цифрового правительства; введены ограничения, направленные на противодействие распространению порнографии с участием несовершеннолетних в Интернете, а также ограничения, обеспечивающие защиту интеллектуальной собственности.

В целях становления Великобритании как безопасного и защищенного киберпространства была принята Национальная стратегия кибербезопасности, опубликованная 1 ноября 2016 г. (National cybersecurity Strategy 2016–2021). Основная цель Стратегии – достижение Великобританией к 2021 г. статуса безопасной и устойчивой к киберугрозам страны, уверенной и процветающей в цифровом пространстве.

В Стратегии киберпреступность рассматривается в контексте двух взаимосвязанных форм преступной деятельности:

киберзависимых преступлений – преступлений, которые могут совершаться только путем использования информационно-телекоммуникационных технологий, где устройства используются как инструмент для совершения преступления (например, разработка и распространение вредоносных программ для получения финансовой выгоды, взлома для кражи, повреждения, искажения или уничтожения информации и (или) сети);

киберпреступлений – «традиционных» преступлений, последствия и масштабы которых могут быть увеличены путем применения вычислительной техники, компьютерных сетей или других форм ИКТ (например, мошенничества и кражи данных).

В качестве отдельного направления в кибепреступности выделяется также и криптоджекинг.

В Великобритании основным законом, регламентирующим ответственность за преступления в сфере использования информационно-телекоммуникационных технологий, является Закон «О неправомерном использовании компьютера» (Computer Misuse Act 1990)[1]. Этот Закон стал своего рода реакцией на растущую тревогу по поводу того, что существовавшие в то время законы несоразмерны угрозе для общества, исходящей от хакеров. Показательным в данном аспекте оказалось дело Стивена Гоулда и Роберта Шифрина, которые в 1984 г. получили несанкционированный доступ к принадлежащему компании British Telecom почтовому сервису Prestel, подсмотрев примитивный пароль у установщика компании. Обвинение против них было выдви-

[1] Официальный сайт Правительства Великобритании. URL: http://www.gov.uk

нуто в соответствии с Законом «О подлоге и подделках» 1981 г. В апелляционном суде злоумышленники были оправданы, и оправдательный приговор был впоследствии утвержден палатой лордов[1].

Рассмотрим более подробно положения Закона «О неправомерном использовании компьютера».

Статьей 1 указанного Закона предусмотрено наказание за несанкционированный доступ к компьютерным материалам. Данную норму можно рассматривать в качестве основного преступления, так как зачастую оно предшествует совершению других, более серьезных преступлений. Преступление считается оконченным с того момента, когда лицо включило компьютер для получения несанкционированных материалов. Насколько ему удалось реализовать свой умысел, значения не имеет. Норма является общей, поэтому умысел злоумышленника не должен быть направлен на какую-либо конкретную информацию, данные или программу, хранящиеся на компьютере.

Доступ является несанкционированным, если лицо не имеет права или не получило согласия на такой доступ. Понимание британским правоприменителем содержания несанкционированного или неавторизованного доступа аналогично тому, что дается в Европейской Конвенции по борьбе с киберпреступностью.

Необходимо отметить, что под данную норму подпадают и должностные лица, которые превысили пределы своих полномочий по доступу к информации, к которой они не были допущены.

Такая практика сложилась в деле R v Bow Street Magistrates' Courts and Allison (AP) Ex parte Government Of The United States of America [Allison] [2002] 2 AC 216. Палата лордов сочла, что действия сотрудника явно подпадают под положения ст. 1 Закона «О неправомерном использовании компьютера», поскольку он преднамеренно получил доступ, на который не имел права. При этом было установлено, что работник будет виновен в правонарушении только в том случае, если работодатель четко определил пределы полномочий работника на доступ к программе или данным[2].

Статьей 2 рассматриваемого Закона предусмотрена ответственность за несанкционированный доступ с целью совершения или содействия совершению новых преступлений. Такое содействие также является подготовительным этапом при совершении иного (нового) пре-

[1] Эмм Д. Киберпреступность и закон. URL: http://cripo.com.ua

[2] The Crown Prosecution Service. URL: https://www.cps.gov.uk/legal-guidance/computer-misuse-act-1990

ступления. Лицо может быть признано виновным в совершении преступления, предусмотренного ст. 2, даже если совершение основного преступления невозможно (ч. 4 ст. 2). Человек, признанный невиновным по ст. 2 или 3 Закона судом присяжных, может быть осужден за преступление по ст. 1.

Статьей 3 Закона предусмотрена ответственность за несанкционированные действия в отношении компьютерных систем с целью нанесения ущерба или по неосторожности. Лицо признается виновным в совершении преступления, если совершает любое несанкционированное действие, в том числе получает доступ к данным. К ответственности по ст. 3 привлекаются также лица, виновные в совершении DDOS-атак.

Статьей 3ZA предусмотрена ответственность за несанкционированные действия, наносящие серьезный ущерб или создающие риск серьезного ущерба. Данная норма в первую очередь ориентирована на тех, кто стремится нанести удар по критически важной национальной инфраструктуре (в зависимости от мотивов исполнителя также может быть применено антитеррористическое законодательство). Указанная норма тождественна по своей сути ст. 274.1 УК РФ.

Статьей 3A предусмотрена ответственность за изготовление, предоставление или приобретение товаров для использования в правонарушениях, связанных с неправомерным применением компьютерных технологий, т. е. связанных с преступлениями, предусмотренными ст. 1, 3 или 3ZA. Указанная норма представляется тождественной положениям ст. 187, 272 УК РФ.

Указанной нормой предусмотрена ответственность для лиц, производящих или поставляющих «вредоносные программы». Для привлечения к ответственности по данной норме необходимо обязательное установление умысла на совершение преступления. Сами по себе указанные деяния (без преступного умысла) не криминализированы.

Законом от 3 марта 2015 г. «О тяжком преступлении» (The Serious Crime Act 2015)[1] были внесены изменения, существенно ужесточившие наказание за совершение рассматриваемых преступлений. Так, с учетом последних изменений, в Соединенном Королевстве преступными признаются следующие посягательства в сфере использования информационно-телекоммуникационных технологий: несанкционированный доступ к компьютерной информации (наказание до двух лет лишения свободы и (или) штраф); несанкционированный доступ с целью нарушить работу компьютера и иных информационных устройств

[1] The Serious Crime Act 2015. URL: http://www.nationalcrimeagency.gov.uk

(наказание до десяти лет лишения свободы или штраф); изготовление, поставка, получение устройств и оборудования для неправомерного доступа к информационным технологиям (наказание до двух лет лишения свободы и (или) штраф). Кроме того, увеличение ответственности за преступления в рассматриваемой сфере свидельствует об осознании Великобританией общественной опасности посягательств с использованием IT-технологий.

Сегодня для всех очевидно, что законодательство без необходимого механизма его применения бесполезно и носит лишь декларативный характер. Для привлечения к уголовной ответственности необходимо наличие доказательств виновности лица. Информационный характер посягательств обусловливает необходимость расширения границ полномочий правоохранительных органов, что непременно приводит к проблеме поиска баланса между соблюдением свобод граждан в информационном пространстве и обеспечением всеобщей информационной безопасности. В Великобритании, как и во всех странах мира, ответ на этот вопрос еще не найден.

Однако с сожалением приходится констатировать, что преступность в IT-сфере – неотъемлемая часть цифровой экономики. И с большей информатизацией общества границы этой преступности будут расти, постепенно полностью вытесняя «традиционную» преступность. И реагировать на нее необходимо комплексно и постоянно. Трансграничный характер указанных посягательств заставляет в числе основных задач поставить унификацию правовых норм, регулирующих IT-сферу, создание единого механизма привлечения к ответственности за посягательства в IT-сфере во всем мире, невзирая на геополитические границы.

Резюмируя вышеизложенное, можно сделать вывод о том, что уголовное законодательство европейских стран в области противодействия IT-преступности достаточно унифицировано, ввиду имплементации всеми странами положений Конвенции Совета Европы о преступности в сфере компьютерной информации. Кроме того, в некоторых директивах и решениях предусмотрена дополнительная уголовная ответственность за преступления, совершенные в отдельных сегментах цифровой экономики. Особенностью европейского законотворчества в рассматриваемой сфере является детальная интерпретация и толкование используемых понятий, что в значительной степени упрощает их применение. Отличительными признаками следует считать также универсальность принимаемых норм, которые имеют свой определенный

«срок годности», достаточный в условиях быстрого изменения и внедрения новых IT-технологий, и их постоянный пересмотр в целях соответствия возникающим угрозам.

Особое внимание в европейских странах уделяется противодействию преступлениям в криптоиндустрии. «Главная направленность этого законодательства – блокировка возможностей для высокотехнологичных преступников развернуть в Европе блокчейн-преступность или использовать криптовалюты в операциях кибепреступников или террористов»[1].

Отличительной особенностью стран, являющихся лидерами по цифровому развитию, является принятие национальных планов и стратегий в сфере обеспечения кибербезопасности. В отдельных странах приняты стратегии противодействия киберпреступности, предполагающие комплексные меры, – от повышения эффективности международного сотрудничества и совершенствования законодательной базы до создания отдельной системы подготовки кадров по борьбе с IT-преступностью, в том числе и основным ее направлением – блокчейн-преступностью.

2.3. Уголовная ответственность за преступления в сфере цифровой экономики в государствах Аравийского полуострова

Интерес к изучению опыта правового регулирования в IT-сфере в странах Аравийского полуострова предопределяется тем, что в указанных странах, придерживающихся норм мусульманского права, уголовная ответственность закреплена в нормах Корана и Сунны. Однако в век информационных технологий появились угрозы, имеющие очевидный противоправный характер, ответственность за которые не находит отражения в своде религиозных догматов, написанных в начале прошлого тысячелетия, а применение общих норм за «традиционные» преступления, такие как, например, кража или мошенничество, явно недопустимо. К тому же темпы распространения указанных преступных явлений предопределяют необходимость реакции со стороны государства

[1] Овчинский В., Ларина Е. Криптовалюта, блокчейн и преступность. URL: http://zavtra.ru/blogs/kriptovalyuta_blokchejn_i_prestupnost_

на них. Определенные изменения в этой сфере уже существуют. Все арабские страны солидарны во мнении о необходимости регулирования отношений, возникающих в киберпространстве.

В Саудовской Аравии, Объединенных Арабских Эмиратах, Судане, Иране, Катаре предусмотрена классификация уголовно наказуемых деяний на светские преступления и преступные деяния, которые считаются таковыми согласно шариату. Остановимся на содержании деяний последнего типа в соответствии с доктриной мусульманского права[1].

Первой страной Арабского региона, обратившейся к проблеме законодательного регулирования IT-сферы и противодействия киберпреступлениям, стало Королевство Иордания, начавшее обсуждение вопроса о принятии Закона «Об электронных транзакциях» в декабре 2001 г. За этим последовало принятие в феврале 2002 г. Объединенными Арабскими Эмиратами Закона «Об обмене информацией и электронной торговле». Аналогичный закон был принят в Бахрейне в сентябре 2002 г.

Несмотря на то, что все страны региона отмечали необходимость формирования законодательства о киберпространстве и киберпреступлениях, долгое время не наблюдалось консолидации усилий в данном направлении. Развитие киберзаконодательства проходило в рамках двух ключевых инициатив: в рамках Регионального плана действий, разработанного Комиссией ООН по экономике и социальному развитию Западной Азии, в котором изложены все действия, необходимые для создания информационного общества, включая законы о киберпространстве; в рамках Арабской стратегии в области информационно-телекоммуникационных технологий на период с 2007 по 2012 г., разработанной Лигой арабских государств.

После принятия вышеуказанных законов длительное время наблюдалось затишье, продолжавшееся до «прорывных» по своей сути изменений в законодательстве Королевства Саудовская Аравия в марте 2007 г., которые повлекли за собой череду изменений в законодательствах близлежащих государств.

В связи с этим рассмотрим опыт Саудовской Аравии более подробно. Уголовное законодательство Королевства Саудовская Аравия помимо Священного Корана и Сунны представлено в отдельных актах – низамах, регулирующих те сферы правоотношений, которые традиционное мусульманское право не урегулировало. Указанные акты,

[1] Петровский А.В. Мусульманское уголовное право и особенности уголовного законодательства мусульманских государств. Краснодар: КубГУ, 2013. С. 23.

принимаемые в строгом соответствии с правилами шариата, являются своего рода решением вопросов, необходимых для действия мусульманского права. Однако по своей сути они представляются весьма прогрессивными и содержат ряд элементов, присущих законотворчеству европейских стран.

Согласно данным Комиссии по коммуникациям и информационным технологиям (Communication and Information Technology Commission), количество жителей Саудовской Аравии, пользующихся Интернетом, в 2012 г. достигло 15,8 млн человек, что составляет 54,1% всего населения страны, в то время как в 2001 г. эта цифра составляла всего лишь 5%[1].

Согласно данным, представленным в ежегодном обзоре Symantec Norton Cybercrime Report, ущерб от киберпреступлений для Королевства в 2016 г. составил порядка 3,6 млрд саудовских риалов. Практически 40% жителей страны, являющихся пользователями IT-технологий, стали жертвами преступных посягательств, ущерб каждому из которых составил порядка 195 долл. (730 саудовских риалов)[2].

Наиболее резонансным случаем была кибератака на государственную нефтяную компанию «Арамко» в августе 2012 г., когда свыше 30 тыс. компьютеров компании были заражены вирусом, уничтожившим данные жестких дисков, что повлекло приостановку процесса добычи нефти[3].

Периодически подвергаются атаке сайты правительственных организаций и госучреждений, что парализует их работу.

Саудовская Аравия была одной из первых стран Аравийского полуострова, подвергшихся кибератакам, что повлекло принятие еще в 2007 г. специального королевского указа (низама), закрепляющего уголовную ответственность за киберпреступления, – Закона «О борьбе с киберпреступностью».

Указанный Закон содержит 16 статей и направлен на борьбу с киберпреступностью путем выявления таких преступлений и определения наказания за них в целях повышения информационной безопасности; защиту прав, связанных с законным использованием компьютеров и информационных сетей, а также защиту общественных интересов, морали, общих ценностей и национальной экономики (ст. 2).

---

[1] Ежегодный доклад Комиссии по коммуникациям и информационным технологиям (Annual Report of Communication and Information Technology Commission), 2013.

[2] Обзор Symantec Norton Cybercrime report, 2016. URL: http://www.symantec.com.

[3] Bushra Mohamed Elamin Elnain Cybercrime in Kingdom of Saudi Arabia: The threat today and expected future // Information and knowledge management. 2013. Vol. 3. № 12. P. 14–18.

Статьи 3–7 предусматривают уголовную ответственность за совершение различных посягательств, совершаемых в киберпространстве. Примечательно, что в зависимости от предусмотренного наказания все преступления можно условно разделить на пять групп.

К первой группе относятся наиболее тяжкие преступления, ответственность за которые предусматривает лишение свободы на срок до 10 лет и штраф до 5 млн саудовских риалов (около 1,3 млн долл.). Это деяния, связанные с использованием IT-технологий в целях поддержки и осуществления террористической деятельности. Под указанными действиями понимаются создание и использование веб-сайта террористических организаций для облегчения общения с лидерами или членами таких организаций, их финансирования, пропаганды их идеологий, пропаганды методов изготовления зажигательных устройств, взрывчатых веществ или любых других средств, используемых в террористической деятельности. Другой разновидностью наиболее тяжкого преступления признается незаконный доступ к веб-сайту или информационной системе напрямую, через информационную сеть или любой компьютер с целью получения данных, угрожающих внутренней или внешней безопасности государства или его национальной экономике.

Вторую, менее тяжкую группу преступных посягательств составляют преступления, посягающие на общественный порядок, нравственность и мораль. Так, преступными признаются производство, подготовка, передача или хранение материалов, затрагивающих общественный порядок, религиозные ценности, общественную мораль и конфиденциальность, через информационную сеть или компьютеры; создание веб-сайта в информационной сети или на компьютере для продвижения или облегчения торговли людьми; подготовка, публикация и продвижение материала для порнографических или игорных сайтов, которые нарушают общественную мораль; создание или размещение веб-сайта в информационной сети или компьютере для рекламы и демонстрации способов использования наркотических и психотропных препаратов или торговли ими.

Наказание за указанные преступления менее суровое, чем за преступления, относящиеся к первой группе, и предусматривает лишение свободы на срок до 5 лет либо штраф до 3 млн саудовских риалов (примерно 800 тыс. долл.).

Третью группу указанных преступных посягательств составляют незаконный доступ к компьютерам с целью удаления, стирания, уничтожения, утечки, повреждения, изменения или перераспределения частных данных; устранение или разрушение информационной сети;

уничтожение, удаление, утечка или изменение существующих или сохраненных программ или данных; воспрепятствование легальному доступу, совершение действий, повлекших отказ в доступе. Лицо (физическое или юридическое), совершившее указанное преступление, подлежит тюремному заключению на срок до 4 лет и (или) штрафу до 3 млн саудовских риалов (примерно 800 тыс. долл.).

Четвертую группу преступных посягательств составляет использование веб-сайтов и IT-ресурсов для совершения мошеннических транзакций, которые караются лишением свободы на срок до 3 лет и (или) штрафом до 2 млн саудовских риалов (примерно 500 тыс. долл.). Преступными признаются приобретение движимого имущества или облигаций для себя или других лиц либо подписание таких облигаций путем мошенничества или использования ложного имени или личности, а также незаконный доступ к банковским или кредитным данным, относящимся к владению ценными бумагами, с целью получения данных, информации, средств или услуг.

В пятую, наименее опасную с точки зрения саудовского законодателя группу включены преступления, связанные с неправомерным доступом, нарушением неприкосновенности частной жизни и шантажом. Так, шпионаж, перехват или прием данных, передаваемых через информационную сеть или компьютер без законного разрешения; незаконный доступ к компьютерам с намерением угрожать или шантажировать любого человека, чтобы заставить его принять или воздержаться от принятия законного или незаконного решения; незаконный доступ к веб-сайту или взлом веб-сайта с намерением изменить его дизайн, уничтожить или изменить его или занять его URL; вторжение в частную жизнь посредством злоупотребления мобильными телефонами, оборудованными камерой, и т. п.; диффамация и нанесение ущерба другим лицам с использованием различных информационно-телекоммуникационных технологий влекут наказание до 1 года лишения свободы и (или) наложение штрафа до 500 тыс. саудовских риалов (примерно 130 тыс. долл.).

Отягчающим обстоятельством признается совершение преступления организованной группой, должностным лицом либо с использованием должностных полномочий, при вовлечении несовершеннолетних для совершения преступления (при этом возраст несовершеннолетних должен быть менее 15 лет), а также при рецидиве указанных преступлений. При наличии данных обстоятельств тюремное заключение и штраф не могут быть меньше половины максимального наказания, предусмотренного статьей Закона.

Судья при назначении наказания за совершение преступления последней категории руководствуется следующим:

1) если обстоятельство совершения преступления отягчает вину и виновный не заслуживает снисхождения, то назначается высшая мера наказания;

2) если обстоятельство совершения преступления смягчает ответственность, но виновный не заслуживает снисхождения, то применяется средняя мера наказания;

3) если имеются смягчающие ответственность обстоятельства и виновный заслуживает снисхождения, то назначается минимальное наказание[1].

Примечательно, что отдельной нормой (ст. 11) предусмотрено освобождение от уголовной ответственности за добровольный отказ от совершения преступления либо за сообщение о совершенном преступлении при условии, что предоставленная информация приведет к аресту других преступников и конфискации средств, используемых при совершении преступления.

Распределение преступлений в указанной иерархии по степени их общественной опасности предопределяется прежде всего особенностями государственного устройства Саудовской Аравии – страны с мусульманским правом, которая является абсолютной теократической монархией. Данное обстоятельство предопределило признание в качестве наиболее опасных из указанных посягательств именно посягательства на государственный строй и национальную экономику, а следующими по значимости – посягательства на общественную и религиозную нравственность и мораль. Традиционный ислам признает наиболее тяжкими преступления в отношении религии и общины (преступления группы «хадд»), а преступления, затрагивающие интересы частных лиц («тазир»), караются менее жестко.

Особенностью уголовной ответственности в Саудовской Аравии является также то, что низамы, регулирующие общественные отношения, имеющие ярко выраженный прозападный характер, адаптируют указанные отношения и ответственность за их нарушение к системе мусульманского права. Так, в июне 2015 г. были одобрены изменения в вышеуказанный Закон, предусматривающие возможность публичной огласки и пристыживания преступников.

---

[1] Набиль Абдельрахман Аль-Ассуми. Преступление и наказание по уголовному праву Бахрейна и Объединенных Арабских Эмиратов: автореф. дис. … канд. юрид. наук. М., 2000. С. 112.

Так, судам предоставляется возможность публиковать сообщения о совершенном лицом преступлении в одной или нескольких местных газетах или любом другом СМИ (в том числе в Интернете), которое суд сочтет подходящим в контексте типа преступления, его серьезности и его влияния. Это касается преступлений, относящихся ко второй группе и затрагивающих общественный порядок, религиозные ценности, общественную мораль и конфиденциальность. Публикация может быть сделана только после того, как постановление получит статус «окончательного решения». Правонарушителя также могут обязать оплатить расходы на публикацию. Такая норма вполне вписывается в систему традиционного исламского права, в котором публичное сообщение о совершенном преступлении и публичное наказание (например, публичная порка) являются одними из самых строгих и унизительных. Изменения в законодательстве Саудовской Аравии также являются примером растущей готовности законодателей использовать общественные нравы в качестве сдерживающего фактора для борьбы с социальными преступлениями. Однако следует отметить, что за пределами этих легализованных форм публикации часто существуют ограничения по законам о клевете и конфиденциальности, которые запрещают прямое и публичное пренебрежение отдельными лицами или компаниями. В 2011 г. сайт DubaiNameShame и страница Twitter были закрыты после предупреждений о том, что опубликование имен и инкриминирующих фотографий плохих водителей и компаний, оказывающих плохое обслуживание клиентов в ОАЭ, было незаконным в соответствии с местными законами о клевете.

На сегодняшний день Саудовская Аравия приняла и соблюдает Арабское соглашение по киберпреступлениям (№ 126 от 2012 г.). Соглашение направлено на укрепление и активизацию сотрудничества между арабскими странами по противодействию мошенничеству с платежными картами, кибертерроризму, созданию и распространению вредоносных программ, неправомерному доступу, а также по защите авторских прав[1].

В других странах региона также наметились определенные изменения. Так, ряд стран приняли отдельные акты, регулирующие отношения в IT-сфере, например, Закон об электронных транзакциях, принятый Катаром (2010 г.); Закон о киберпреступности в Королевстве Иордания (2010 г.); Закон об электронной подписи и сетевых услугах (2011 г.), а также Закон о защите киберпреступности в Сирии (2012 г.).

[1] Sulaiman Al Amro. Cybercrime in Saudi Arabia: fact or fiction // International Journal of Computer Science Issues. 2017. Vol. 14. Iss. 2. P. 36–42.

Некоторые страны, такие как Алжир и Марокко, использовали иной подход – изменение и обновление существующих законов об интеллектуальной собственности[1]. Кроме того, 29 июня 2018 г. Марокко присоединилось к Конвенции Совета Европы о киберпреступности (СЕД № 185) и Дополнительному протоколу к Конвенции о киберпреступности, касающемуся криминализации актов расистского и ксенофобского характера, совершаемых с использованием компьютерных систем.

Сферы использования информационно-телекоммуникационных технологий весьма обширны. Нормативные акты, регулирующие их использование, условно можно разделить на несколько групп:

нормативные акты, регулирующие порядок использования электронной подписи;

нормативные акты, регулирующие порядок проведения электронных транзакций и электронную коммерцию;

нормативные акты, предусматривающие ответственность за совершение киберпреступлений.

Проведенный нами анализ свидетельствует о том, что порядок постановки электронной подписи урегулирован в законодательстве ряда арабских стран, например, в Объединенных Арабских Эмиратах, Королевстве Иордания, Королевстве Бахрейн, Тунисе, Алжире, Королевстве Саудовская Аравия, Султанате Оман, Катаре, Египте и Марокко.

Аналогичным образом можно охарактеризовать и законодательство в сфере проведения электронных транзакций и электронных платежей. Так, в Ливане Центральный банк издал различные постановления, касающиеся регуляризации электронных платежей и обмена. Кроме того, в Йемене был принят специальный закон, охватывающий электронные банковские операции[2].

Ответственность за совершение преступлений в IT-сфере предусмотрена в законодательстве большинства арабских стран. Наиболее прогрессивными следует признать законодательства ОАЭ, Королевства Саудовская Аравия и Судана. Вместе с тем в других странах региона на рассмотрении законодательных органов уже находятся нормативные акты, регулирующие указанную сферу. Например, в таких

[1] The United Nations Economic and Social Commission for Western Asia (ESWA) Cyber Legislation Digest, 25–27 March, 2015.

[2] Report of the United Nations Economic and Social Commission for Western Asia (ESWA) Cyber Legislation project. URL: http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/enUS/Default.aspx

странах, как Королевство Бахрейн, Алжир, Сирия, Султанат Оман и Египет. В Тунисе и Марокко ответственность за посягательства с использованием информационно-телекоммуникационных технологий предусмотрена в законах об электронной торговле и интеллектуальной собственности.

Несмотря на то, что в большинстве арабских стран изданы многочисленные законы и иные акты по защите отношений в киберпространстве, законодательство указанных стран по-прежнему нельзя признать удовлетворительным и отвечающим современным требованиям.

Во-первых, принимаемые законы носят одиночный, бессистемный характер. Регулируя позитивные отношения, возникающие в сфере осуществления электронных платежей, законодатели отдельных арабских стран почему-то оставляют без внимания отношения, связанные с защитой указанных отношений от преступных посягательств. Иными словами, отсутствует единая интегративная стратегия, направленная на противодействие посягательствам в IT-сфере. На наш взгляд, в указанном аспекте арабскими странами может быть использован опыт стран Западной Европы, в которых приняты и активно воплощаются планы по противодействию преступлениям в цифровой экономике. Удивительное сочетание традиционного мусульманского права, основанного на законах шариата, с формированием прогрессивного светского законодательства также является отличительной особенностью стран региона. В стремлении идти в ногу со временем, при этом не отходя от основ мусульманского права, приводит к весьма интересным решениям. Яркий тому пример – выпуск мусульманской криптовалюты OneGram: «Блокчейн-стартап из ОАЭ выпустил подкрепленную золотом криптовалюту OneGram (OGC), которая соответствует законам шариата. Благодаря этому инвесторы-мусульмане получат возможность принять участие в торговле криптовалютами. Согласно нормам шариата, экономическая деятельность должна быть связана только с реальными физическими активами, а поскольку криптовалюты к ним не относятся, мусульманский мир считает их нежелательными. Создатели OneGram решили эту проблему: каждый токен OGC подкреплен одним граммом физического золота, содержащегося в хранилище. Соответствие OneGram нормам шариата было официально подтверждено

дубайской Al Maali Consulting, консультационной фирмой, которая занимается рассмотрением финансовых инструментов в контексте законов ислама»[1].

Во-вторых, недостаточное внимание уделяется правовому просвещению населения. Например, большинство жителей арабских стран, придерживающихся мусульманского права, не знают о том, что деяния, совершаемые и использованием информационно-телекоммуникационных технологий, являются преступными и караются весьма жестко.

В-третьих, в указанных процессах играют роль слабое взаимодействие на межгосударственном уровне, отсутствие региональных инициатив по региональной интеграции и противодействию киберпреступности. Это объясняется, прежде всего, большой разницей в уровнях обеспечения кибербезопасности между отдельными странами и разрозненностью в выбранных подходах к решению проблем, возникающих в IT-сфере. Например, Королевство Бахрейн приняло различные законы и нормативные акты, касающиеся электронных транзакций и торговли, а также защиты интеллектуальной собственности, однако такие страны, как Ирак и Кувейт, вообще не рассматривали эти проблемы, несмотря на то, что они имеют проекты соответствующих законов. Большинство стран региона не охватили юридические аспекты электронных платежей, за исключением Ливана и Йемена. Остались без внимания и вопросы защиты прав потребителей в киберпространстве. Указанные инициативы реализованы только в Ливане и Тунисе. Вопросы защиты персональных данных в киберпространстве практически ни в одной стране не рассматриваются.

Обозначенные проблемы препятствуют активному внедрению стран Арабского региона в единое экономическое и информационное пространство. Решение указанных проблем возможно только при комплексном подходе и взаимодействии между всеми странами – членами Арабской Лиги.

[1] См. подробнее: URL: https://ru.insider.pro/topnews/2018-04-09/v-oae-vypustili-kriptovalyutu-onegram-kotoraya-sootvetstvuet-zakonam-shariata

2.4. Уголовная ответственность за преступления в сфере цифровой экономики в странах Юго-Восточной Азии

В Юго-Восточной Азии, в отличие от других регионов мира, наблюдается диаметрально противоположная картина между странами АСЕАН-5 (Сингапур, Малайзия, Филиппины, Таиланд, Индонезия)[1] и менее экономически развитыми Лаосом, Камбоджей, Мьянмой, Вьетнамом и Восточным Тимором.

Группировка АСЕАН-5 в начале XXI в. вплотную подошла к переходу на постиндустриальный этап развития, а для менее развитых стран АСЕАН – это еще долгий путь. Вместе с тем, создание единого информационного пространства является одной из основных задач деятельности данной организации. В ноябре 2000 г. на 4-м Саммите глав государств в Сингапуре было заключено первое Рамочное соглашение по АСЕАН, в котором были изложены принципы и меры по созданию информационной структуры и развитию электронной торговли в рамках Ассоциации. Впоследствии его положения конкретизированы в Планах действий на Вьетнамском форуме (2004 г.), Ханойском саммите (2005 г.), на 6-й министерской встрече в Брунее (2006 г.)[2].

Использование информационно-телекоммуникационных технологий признано одним из ключевых приоритетов АСЕАН в Генеральном плане по развитию IT-технологий до 2015 г.

Несмотря на неравномерность в технологическом развитии, рынок IT-технологий в странах Юго-Восточной Азии оценивается в 2018 г. примерно в 62 млрд долл. США[3]. При этом Сингапур регулярно возглавляет рейтинги по инновационному и информационно-технологическому развитию. Наиболее перспективными и быстрорастущими признаны коммуникации, медиа и услуги; банковское дело и ценные бумаги; фармакология и биомедицина; оказание государственных услуг.

Параллельно с разработкой основ функционирования единого информационного пространства была начата работа по законодательному регулированию электронной торговли, функционированию иных сегментов цифровой экономики и обеспечению их безопасности.

---

[1] Государства, выступившие за создание АСЕАН 8 августа 1967 г.

[2] Данг Хай Дан. Развитие информационных технологий в АСЕАН: автореф. дис. … канд. экон. Наук. М., 2008.

[3] Gartner Analysts. URL: https://www.gartner.com/technology/analysts.jsp

АСЕАН активно взаимодействует с Российской Федерацией по выработке единых стандартов в регулировании ICO, Интернета вещей и др.

Несмотря на единую стратегию по развитию информационно-телекоммуникационных технологий в регионе, в каждой стране имеются свои особенности.

Принятие и применение соответствующего законодательства должно способствовать региональной интеграции, имеющей решающее значение в этом контексте. АСЕАН является первопроходцем среди развивающихся стран в области гармонизации законодательства в цифровой экономике. Несмотря на то, что законодательный процесс требует времени, цифровая экономика продолжает развиваться довольно высокими темпами. В связи с этим важно постоянно анализировать достигнутый прогресс и выявлять возможные потребности, обусловливающие необходимость пересмотра законодательства.

На сегодняшний день в 9 из 10 стран АСЕАН (за исключением Камбоджи) существует соответствующее законодательство в области электронных транзакций; в 6 из 10 стран предусмотрено законодательство в области защиты покупателей в электронной коммерции, ведется работа и в области оптимизации законодательства в сфере защиты данных и регулирования интернет-контента.

Однако наибольший прогресс достигнут в области противодействия киберпреступлениям. Законы в целом приведены в соответствие международным моделям, определенным в Конвенции Совета Европы о киберпреступности. Специальные законы о противодействии киберпреступности отсутствуют только в Камбодже и Лаосе.

Проведенный анализ законодательства в сфере противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий в странах Юго-Восточной Азии, показал, что наиболее проработанным законодательством в рассматриваемой области обладают только две страны региона – Малайзия и Сингапур, а остальные государства идут по пути одной из указанных стран.

Рассмотрим особенности национального законодательства каждой из стран региона.

Сингапур является одним из общепризнанных мировых лидеров в области использования IT-технологий. Банковский сектор, государственное управление, производство активно внедряются в цифровую экономику. Вполне закономерно, что законодательное регулирование использования IT-технологий в стране находится на достаточно высоком уровне.

Островное государство имеет долгую историю инициатив в области обеспечения безопасности в IT-сфере. Первый генеральный план по кибербезопасности был опубликован еще в 2005 г. Агентство по кибербезопасности Сингапура было создано в 2015 г. как специализированное подразделение для обеспечения кибербезопасности, а в 2016 г. в стране была разработана всеобъемлющая стратегия.

Сингапур активно поддерживает глобальные усилия по искоренению киберпреступности путем участия в Вассенаарских договоренностях, во Всемирной организации по защите интеллектуальной собственности (ВОИС). Де-факто государство также присоединилось к требованиям Будапештской конвенции, хотя и не подписало ее[1]. Так, ключевой Закон «О неправомерном использовании компьютеров» 1993 г. содержит положения по защите компьютеров, компьютерных программ и данных, хранящихся в компьютерах, от несанкционированного доступа, модификации, перехвата и повреждения. Преступные посягательства, содержащиеся в указанном Законе, соответствуют положениям Конвенции Совета Европы о киберпреступности. В 2007 г. Закон претерпел значительные изменения.

Примечательно, что относительно киберпреступлений в Сингапуре широко используется принцип экстратерриториальности, или широкой территориальной юрисдикции: лицо может преследоваться по закону независимо от того, совершено ли преступление в Сингапуре, проживает ли преступник в Сингапуре, либо когда преступление или подготовительные действия осуществляются посредством компьютера в Сингапуре.

В Законе используется широкая трактовка понятия «компьютер», независимо от примененной ИКТ. Это сделано намеренно, для придания универсальности правовым нормам. Среди основных посягательств, предусмотренных Законом, отметим следующие: несанкционированный доступ к компьютерным материалам (раздел 3); доступ к компьютеру с целью совершения или содействия совершению преступления (раздел 4); несанкционированное изменение хранящихся в компьютере данных (раздел 5); несанкционированное использование или перехват компьютерных данных или процессов (раздел 6); несанкционированное воспрепятствование законному использованию компьютера (раздел 7); несанкционированное раскрытие кода доступа

[1] Hee Jhee Jiow. Cybercrime in Singapore: An analysis of regulation based on lessig's four modalities of constraint // International Journal of Cyber Criminology (IJCC). January – June 2013. Vol. 7 (1). P. 18–27.

или пароля (раздел 8); подстрекательство или попытка совершения любого из вышеперечисленных преступных действий (раздел 10).

Несмотря на универсальность правовых норм рассматриваемого Закона, позволяющую привлекать к ответственности за широкий круг преступных деяний, совершаемых с использованием IT-технологий, в Сингапуре применяются и иные законы для привлечения лиц к ответственности. Например, для привлечения к ответственности за мошенничество наряду с Законом «О неправомерном использовании компьютеров» применяется Уголовный кодекс; при посягательствах в сфере интеллектуальной собственности – законы «Об авторском праве» и «О защите торгового знака».

Кроме того, в Уголовный кодекс были внесены поправки, предусматривающие ответственность за использование компьютеров при совершении кибершантажа; преступлений сексуального характера; преступлений, нарушающих неприкосновенность частной жизни; преступлений, посягающих на национальную инфраструктуру.

Непрерывная работа по обновлению и пересмотру законодательства в Сингапуре ведется в целях своевременной и адекватной реакции государства на новые угрозы, возникающие в IT-сфере. При этом законодателем делается ставка на создание универсальных норм, применимых к новым технологиям. Особого одобрения заслуживает принцип экстратерриториальности, свидетельствующий о желании Сингапура реагировать не только на угрозы внутри страны, но и на угрозы, возникающие на мировой арене.

Наряду с Сингапуром Малайзия является крупнейшим центром Юго-Восточной Азии по инвестициям в развитие IT-технологий. Ежегодно на центры обработки данных, программное обеспечение, IT-услуги, устройства и внутренние услуги тратится около 12,6 млрд долл. при ежегодном темпе роста в 6,4%[1]. По оценкам Gartner, электронное здравоохранение и телемедицина являются ключевыми направлениями развития IT в Малайзии, особое внимание уделяется также улучшению оказания государственных услуг посредством Интернета[2].

Малайзия относится к числу стран с наибольшей плотностью распространения и использования информационных технологий среди

[1] IT-рынок Сингапура и прогнозы рынка Азии в 2017 году. URL: https://saleslabel.com/it-rynok-singapura-i-prognozy-rynka-azii-v-2017-godu

[2] Gartner Analysts. URL: https://www.gartner.com/technology/analysts.jsp

населения. По статистике, в Малайзии пользователи Интернета (в возрасте от 20 до 24 лет) проводят в среднем 22,3 часа онлайн в неделю, и примерно 64% из них становились жертвами киберпреступлений[1].

Вопросам обеспечения информационной безопасности в стране уделяется значительное внимание. Парламентом Малайзии принято 8 законов, посвященных информационной безопасности: Закон «О цифровой подписи» 1997 г., Закон «О компьютерных преступлениях» 1997 г., Закон «О защите авторских и смежных прав» 1997 г., Закон «О телемедицине» 1997 г., Закон «О телекоммуникациях и мультимедиа» 1998 г., Закон «О комиссии по телекоммуникациям и мультимедиа»1998 г., Закон «Об электронной коммерции» 2006 г., Закон «О защите персональных данных» 2010 г.

Законом «О компьютерных преступлениях» 1997 г. уголовно наказуемыми признаны четыре группы деяний:

деяния, связанные с несанкционированным доступом в любые компьютерные программы (данные) или сети (раздел 3);

деяния, связанные с несанкционированным доступом к программам и данным, хранящимся в любом компьютере, с целью совершения мошенничества или подлога (раздел 4);

деяния, совершенные с целью несанкционированного изменения содержимого любого компьютера (раздел 5);

неправомерное сообщение пароля, кода или средства доступа к компьютеру любому не уполномоченному на его получение лицу (раздел 6).

Итак, нормы рассматриваемого Закона в большей степени можно характеризовать как нормы, направленные на противодействие компьютерной преступности, которая является лишь частью киберпреступности. Наказание за совершение различных преступлений с использованием информационно-телекоммуникационных технологий предусмотрено в основном в профильных нормативных актах. Например, в законах об электронной коммерции и авторском праве. Указанные законы являются несомненным дополнением к Закону «О компьютерных преступлениях» 1997 г. и позволяют признать малазийское законодательство соответствующим общемировым стандартам.

Филиппины были в числе первых стран, в которых была предпринята попытка законодательного регулирования IT-сферы. Первый закон (Закон «Об электронной коммерции») был принят еще в 2000 г. Он до-

[1] Anwer Yusoff. Cybersecurity Standards: A Case Study on Malaysian Banking Sector // Cybersecurity Malaysia. 2013.

полнялся административными регламентами, касающимися защиты покупателей, цифровой подписи, электронной коммерции и создания электронного правительства. В 2012 г. в Филиппинах был принят профильный закон о киберпреступности – Закон «О предупреждении киберпреступности». Нормы по противодействию преступлениям в IT-сфере предусматриваются также Законом «Об электронной торговле».

Кроме того, Комиссия по ценным бумагам и биржам Филиппин опубликовала доклад, в котором предупредила о высоких криминологических рисках 14 инвестиционных проектов, которые могут принести клиентам серьезные убытки. Комиссия отметила, что подобные проекты продвигают ценные бумаги под видом токенов и рекламируют «нереалистичные доходы в размере от 10 до 200 процентов в месяц», при этом ответственность за подобные деяния может варьироваться от штрафа до 277 тыс. долл. до лишения свободы сроком до 21 года[1].

Как отмечает Э.Л. Сидоренко, «Филиппины задали новый тренд в уголовном праве – полное и безоговорочное признание криптовалют отягчающим обстоятельством, приступив к выработке конкретных уголовно-правовых мер. В стране уже разрабатываются законы, призванные ужесточить наказание за преступления, связанные с криптовалютами. Первый закон предполагает ужесточение наказания в форме повышения тяжести наказания на одну категорию, если использовались криптовалюты. Второй закон предполагает, что для признания действий определенных лиц мошенническим сговором (syndicated estafa) будет требоваться доказывание участия не 5, но лишь 2 соисполнителей деяния»[2]. Стоит согласиться с мнением эксперта в том, что подход через ужесточение наказания за общественные явления, которые не могут контролироваться государством, нельзя признать оптимальным и рациональным.

В Индонезии Закон «Об информации и электронных транзакциях» 2008 г. является ключевым актом, регулирующим IT-сферу. Он включает общие положения об электронной коммерции, а также более конкретные положения по конфиденциальности. В Законе также содержится ряд ключевых положений о киберпреступности (ст. 29–37). Так, преступными признаются незаконный доступ, незаконное вмешательство, вмешательство в данные, системное вмешательство, неправомерное использование устройства, компьютерное мошенничество,

[1] В Филиппинах ужесточат наказания за криптовалютные преступления. URL: https://yandex.ru/turbo?text

[2] Филиппины ужесточают отношение к криптовалютам и ICO // Телеграм-канал КриптоЛина. URL: https://telegram.org/#/im?p=@cryptoelina

правонарушения, связанные с нарушением авторских и смежных прав, перехват данных, вопросы юрисдикции. Эти положения являются почти точным отражением ключевых положений Европейской Конвенции о киберпреступности, которая была ратифицирована в 2001 г. Однако в Законе в весьма ограниченном объеме содержится информация, касающаяся правоприменения, соблюдения процессуальных аспектов, сбора данных о трафике и международного сотрудничества.

Закон Брунея «О неправомерном использовании компьютерных технологий» 2000 г. (в редакции 2007 г.) основан на аналогичном законе Сингапура 1993 г. Законом предусмотрены следующие противоправные посягательства: несанкционированный доступ к компьютерным материалам (раздел 3); несанкционированный доступ с целью совершения преступления или содействия его совершению (раздел 4); несанкционированная модификация компьютерной информации (раздел 5); несанкционированное использование или перехват данных (раздел 6); несанкционированное воспрепятствование использованию компьютера (раздел 7); несанкционированное раскрытие кода доступа или пароля (раздел 8); подстрекательство или попытка совершения любого из вышеперечисленных преступных действий (раздел 10).

Согласно указанному Закону ответственность варьируется от штрафов до тюремного заключения в зависимости от тяжести содеянного. Несмотря на то, что многие положения рассматриваемого Закона соответствуют положениям Конвенции Совета Европы о киберпреступности, сама Конвенция Брунеем по-прежнему не подписана.

В 2007 г. в Тайланде вступил в силу Закон «О совершении преступлений, относящихся к компьютеру», широко известный как Закон о компьютерной преступности. В нем содержатся положения о преступлениях, посягающих на компьютерные системы и компьютерную информацию, а также предусмотрена ответственность за использование компьютера в целях совершения преступления. Основные положения Закона соответствуют положениям Конвенции Совета Европы о киберпреступности. В дополнение к данному Закону также действуют локальные акты, направленные на обеспечение кибербезопасности.

В целях всестороннего регулирования криптовалют, предотвращения отмывания денег и уклонения от уплаты налогов был принят Указ о контроле над криптовалютами BE 2561, согласно которому Комиссия по ценным бумагам и биржам Тайланда (SEC) наделена полномочиями регулировать цифровые активы и деятельность лиц, осуществляющих их продажу. Физические и юридические лица, которые занимаются продажей криптовалют, обязаны зарегистрироваться в SEC в течение 90 дней

с момента вступления Закона в силу. Нарушение данного положения карается штрафом от 500 тыс. батов (около 15,6 тыс. долл.) или тюремным заключением сроком до двух лет. Все криптовалютные операции будут облагаться НДС в размере 7% и налогом на прибыль (15%)[1].

Законы о киберпреступности во Вьетнаме охватывают ограниченный круг деяний, который не столь обширен, как перечень преступлений, содержащихся в Конвенции Совета Европы о киберпреступности. В 2014 г. во Вьетнаме был принят Закон «Об информационной безопасности».

В Камбодже в проект сводного закона «Об электронной торговле» включены разделы о преступлениях против конфиденциальности, неприкосновенности информационных систем и компьютерных данных, которыми охватываются незаконные вмешательство и перехват данных, а также такие деяния, как преследование, распространение и использование вредоносного ПО и вторжение в частную жизнь.

Проведенный анализ показал, что страны Юго-Восточной Азии придерживаются европейской модели противодействия IT-преступлениям, так как в основе большинства законов лежат положения Конвенции Совета Европы о киберпреступности. Вместе с тем в некоторых наиболее развитых с точки зрения информационно-телекоммуникационных технологий странах приняты отдельные законодательные акты, регулирующие вопросы привлечения к уголовной ответственности за совершение преступлений в сфере электронной коммерции, соблюдения авторских и смежных прав.

2.5. Уголовная ответственность за преступления в сфере цифровой экономики в странах ближнего зарубежья

Исторические реалии таковы, что традиционно уголовное законодательство стран ближнего зарубежья, не так давно (в историческом плане) составлявших вместе с Российской Федерацией единое союзное государство с общим правовым полем, во многом схоже с отечественным.

Вопросы межгосударственного взаимодействия в указанном регионе осуществляются в рамках нескольких организаций: Содружества Независимых Государств, Шанхайской организации сотрудничества и

[1] В Тайланде вступил в силу закон о регулировании криптовалют. URL: https://cryptolot.ru/post_v-tailande-vstupil-v-silu-zakon-o-regulirovanii-kriptovalyut_399

Евразийского экономического союза. Стоит отметить, что в рамках деятельности каждой из приведенных организаций были приняты стратегические документы, в которых отмечается необходимость развития цифровой экономики, являющейся главным фактором конкурентоспособности и стабильного развития национальной экономики каждой из стран.

Одним из ключевых актов следует признать Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года». В документе отмечается, что «глобальная цифровая трансформация создает широкий спектр вызовов для Союза, экономик государств-членов, их хозяйствующих субъектов и граждан… без развития цифровой экономики и совместной реализации проектов в рамках цифровой повестки государства-члены лишают себя новых возможностей, оставаясь в рамках традиционных процессов, отношений и связей; происходит высвобождение огромных трудовых ресурсов и возникновение дисбалансов во всех отраслях экономик государств-членов; происходит переток трудовых ресурсов и потребителей в цифровые экономики третьих стран и в цифровые экосистемы глобальных цифровых платформ; возникает необходимость более надежной институциональной формы защиты персональных данных, с соблюдением баланса защиты в условиях их трансграничного обмена; происходит обесценивание традиционных активов государств-членов и хозяйствующих субъектов государств-членов, не прошедших цифровые преобразования и трансформацию»[1].

Кроме того, в указанном Решении подчеркивается тот факт, что отсутствие согласованной политики в цифровой сфере «может стать препятствием для достижения синергетических эффектов в развитии цифровой экономики государств-членов и цифрового пространства Союза»[2].

В документе также отмечается, что мер, принятых в национальных стратегиях и программах развития экономик, недостаточно для достижения цели масштабирования экономик государств-членов в ответ на глобальные вызовы цифровой трансформации.

---

[1] Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года: решение Высшего Евразийского экономического совета от 11 окт. 2017 г. № 12. Доступ из справочной правовой системы «КонсультантПлюс».

[2] Там же.

На сегодняшний день практически всеми членами Союза ведется активная разработка по внедрению цифровой экономики. Так, президентом Республики Беларусь 21 декабря 2017 г. был подписан Декрет № 8 «О развитии цифровой экономики», в котором дается толкование новых понятий, используемых в цифровой экономике, закреплены права юридических и физических лиц по владению криптовалютами, а также определен основной институт развития в данной сфере – Парк высоких технологий (ПВТ), который обеспечивает в целом формирование институциональной среды[1]. Стоит отметить, что Белоруссия – первая страна на постсоветском пространстве, в которой официально признано и урегулировано обращение криптовалют. Физические лица не только получили право владеть монетами, но и обменивать их на фиатные валюты, дарить и завещать. В целях привлечения инвестиций и повышения привлекательности страны для криптоиндустрии введены налоговые льготы. В частности, отменены налог на прибыль, налог на добавленную стоимость, налог при упрощенной системе налогообложения и подоходный налог с лица. Не подлежит налогообложению и майнинг. Смеем предположить, что такие «прорывные» меры могут в ближайшей перспективе вывести Беларусь в число лидеров по цифровизации экономики. Однако низкий уровень обеспечения информационной безопасности в стране, недостаточная эффективность правоохранительных органов в сфере выявления и расследования преступлений в IT-сфере, отсутствие действенных превентивных мер могут негативным образом сказаться на имидже Беларуси как «цифровой республики». Полагаем, что регуляторике должны подлежать не только позитивные общественные отношения, связанные с внедрением новых IT-технологий, но и те, которые способны причинить вред интересам общества, личности и государства.

В России в июле 2017 г. была принята программа «Цифровая экономика Российской Федерации», утвержденная распоряжением Правительства от 28 июля 2017 г. № 1632-р, а также начата активная разработка законодательства о цифровых финансовых активах.

В Казахстане постановлением Правительства РК № 827 от 12 декабря 2017 г. была утверждена Государственная программа «Цифровой Казахстан». Целями данной Программы являются ускорение темпов развития экономики Казахстана и улучшение качества жизни населе-

[1] Рябцев Н.В. Вызовы устойчивого экономического развития ЕАЭС в эпоху цифровизации национальных экономик (на примере криптовалют и блокчейн), 28 марта 2018. URL: https://www.ictsd.org/bridges-news

ния за счет использования цифровых технологий в среднесрочной перспективе, а также создание условий для перехода экономики Казахстана на принципиально новую траекторию развития, обеспечивающую создание цифровой экономики будущего в долгосрочной перспективе. В Программе также подчеркивается, что эффективная реализация мероприятий по цифровизации экономики будет обеспечена только при обеспечении единства, устойчивости и безопасности информационно-коммуникационной инфраструктуры, сохранности данных и доверии граждан к процессам, в основе которых лежат решения, основанные на использовании ИКТ[1]. Конституционным законом Республики Казахстан от 7 декабря 2015 г. № 438-V «О Международном финансовом центре «Астана»[2] (МФЦА) была создана отдельная юрисдикция, где во взаимоотношениях хозяйствующих субъектов применяется английское общее право – подход прецедентного права в разбирательствах в арбитраже и судебных разбирательствах между участниками МФЦА и контрагентом. В числе основных приоритетов МФЦА выступают установление прозрачного и понятного правового режима на основе лучших мировых практик; создание регуляторного режима, соответствующего признанным мировым стандартам и др.

В январе 2018 г. было анонсировано возможное создание в Армении Свободной экономической зоны (СЭЗ). Программа Свободной экономической зоны предусматривает создание на территории СЭЗ кластера для высокотехнологичных проектов на базе распределенного реестра, искусственного интеллекта и машинного обучения. В первой половине 2018 г. также планируется открытие международного акселератора для инновационных проектов и организация индустриальных дата-центров для блокчейн-проектов[3].

В Кыргызстане в проекте Национальной стратегии развития Кыргызской Республики на 2018–2040 гг. отмечается, что «картина будущего подразумевает однозначную цифровизацию и использование bigdata в комплексном развитии всей экономики и функционировании транспортного комплекса Кыргызской Республики, что прямо проистекает из опережающего развития цифровой инфраструктуры страны в рамках мировых трендов. В стране планируется создание региональных центров по внедрению инноваций в сфере цифровой экономики,

[1] Государственная программа «Цифровой Казахстан». URL: https://primeminister.kz/rupage/view/gosudarstvennaya_programma_digital_kazahstan

[2] URL: http://online.zakon.kz/Document/?doc_id=39635390#pos=103;-52

[3] Армения создаст свободную экономическую зону для развития блокчейн-проектов. URL: https://forklog.com/armeniya-sozdast-svobodnuyu-ekonomicheskuyu-zonu-dlya-razvitiya-blokchejn-proektov

проведению прикладных исследований и разработок с использованием «прорывных» технологий»[1].

В Узбекистане, являющемся одним из вероятных кандидатов на вступление в Евразийский экономический союз, 9 февраля 2018 г. президентом был подписан Указ «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций», в котором Министерству по развитию информационных технологий и коммуникаций в числе других задач и направлений деятельности поручено обеспечить стимулирование роста цифровой экономики.

3 июля 2018 г. президент Узбекистана Ш. Мирзиёев подписал постановление «О мерах по развитию цифровой экономики в Республике Узбекистан». Документ, который по своей сути является «революционным», важнейшими задачами по дальнейшему развитию цифровой экономики в Узбекистане определяет развитие оборота криптоактивов (включая майнинг); развитие технологии «блокчейн» (распределение реестра данных); внедрение и развитие смарт-контрактов (договор в электронной форме); подготовку квалифицированных кадров для разработки и внедрения платформ; развитие сотрудничества с международными и зарубежными организациями в сфере развития и внедрения платформ, а также для совместной реализации проектов.

Безусловно, такое стремление стран ЕАЭС к цифровизации национальных экономик вполне объяснимо и оправданно. Однако не стоит забывать, что всеобщая информатизация таит в себе и угрозы для развития государств в виде преступных посягательств посредством использования информационно-телекоммуникационных технологий. Внедрение IT-технологий без создания действенной системы защиты и регулирования отношений в рассматриваемой сфере может привести к плачевным результатам и свести положительный эффект цифровизации на нет. К сожалению, анализ упомянутых национальных стратегий построения цифровой экономики показал весьма ограниченное обращение к проблеме обеспечения информационной безопасности и противодействия киберпреступности. Концепция кибербезопасности принята только в Казахстане («Киберщит Казахстана»)[2].

---

[1] Проект Национальной стратегии развития Кыргызской Республики на 2018–2040 годы. URL: http://www.president.kg/ru/sobytiya/novosti/6015_proekt_nacionalnoy_strategii_razvitiya_

[2] Об утверждении Концепции кибербезопасности («Киберщит Казахстана»): постановление Правительства Республики Казахстан от 30 июня 2017 г. № 407. URL: http://adilet.zan.kz/rus/docs/P1700000407

В Соглашении о сотрудничестве между правительствами государств – членов Шанхайской организации сотрудничества в борьбе с преступностью (Ташкент, 11 июня 2010 г.) в числе основных направлений сотрудничества в области предупреждения, пресечения, выявления и раскрытия преступлений помимо прочего были указаны террористическая, сепаратистская и экстремистская деятельность; преступления против собственности; коррупция; преступления в сфере экономики, в том числе легализация доходов, полученных от преступной деятельности, и финансирование терроризма; преступления, связанные с нарушением прав интеллектуальной собственности; преступления, связанные с торговлей людьми, особенно женщинами и детьми; незаконное производство и оборот оружия, боеприпасов, взрывных устройств, взрывчатых, ядовитых и радиоактивных веществ, ядерных материалов; незаконное производство и оборот наркотических средств, психотропных веществ и их прекурсоров; контрабанда; преступления на транспорте; преступления в сфере информационных технологий. Отметим, что на сегодняшний день все перечисленные виды преступлений совершаются с активным использованием IT-технологий.

Вопросы уголовно-правового регулирования отношений в IT-сфере были затронуты в Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.)[1]. В указанном Соглашении стороны обязались признавать в соответствии с национальным законодательством в качестве уголовно-наказуемых следующие деяния, если они совершены умышленно:

«а) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред или тяжкие последствия;

[1] Бюллетень международных договоров. 2009. № 6.

г) незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб»[1].

Данные нормы нашли свое отражение в законодательстве ряда государств – участников СНГ. Например, в уголовных кодексах Российской Федерации – в гл. 28 (ст. 272–274.1) раздела IX «Преступления против общественной безопасности и общественного порядка»; Армении – в гл. 24 «Преступления против безопасности компьютерной информации» раздела 9 «Преступления против общественной безопасности, безопасности компьютерной информации, общественного порядка, общественной нравственности и здоровья населения»; Азербайджана – в гл. 30 «Киберпреступления» раздела X «Преступления против общественной безопасности и общественного порядка»[2]; Молдовы – в гл. XI «Информационные преступления и преступления в области электросвязи»[3]; Туркменистана – в гл. 33 раздела XIII «Преступления в сфере компьютерной информации»[4]; Кыргызстана – в гл. 28 раздела IX «Преступления против общественной безопасности и общественного порядка»[5].

Как уже было отмечено ранее, необходимость адекватного реагирования на угрозы в сфере цифровизации экономики в регионе осознается только Казахстаном, поэтому остановимся на законодательстве указанной страны подробнее. В Концепции кибербезопасности Казахстана отмечается, что «высокая латентность и зачастую международный характер таких преступлений повышают их общественную опасность. Ситуация усугубляется укоренившимися в обществе стереотипами о безнаказанности киберпреступности, ненужности принимаемых государством мер по укреплению сферы безопасного использования ИКТ, ограниченными возможностями органов правопорядка по привлечению к ответственности виновных в совершении высокотехнологичных преступлений»[6].

Различные взаимоувязанные аспекты обеспечения информационной безопасности в области информатизации и связи нашли свое отражение и развитие в Уголовном кодексе Республики Казахстан (УК РК),

---

[1] Там же.

[2] Уголовный кодекс Азербайджанской Республики. СПб.: Юридический центр Пресс, 2001.

[3] Уголовный кодекс Республики Молдова. СПб.: Юридический центр Пресс, 2003.

[4] Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации Туркменистаном подписано не было.

[5] Уголовный кодекс Кыргызской Республики. СПб.: Юридический центр Пресс, 2002.

[6] Об утверждении Концепции кибербезопасности («Киберщит Казахстана»): постановление Правительства Республики Казахстан от 30 июня 2017 г. № 407. URL: http://adilet.zan.kz/rus/docs/P1700000407

Кодексе «Об административных правонарушениях», законах «О государственных секретах», «О персональных данных и их защите», «Об электронном документе и электронной цифровой подписи», «О связи» и целом ряде подзаконных актов, разработанных в реализацию новой редакции Закона «Об информатизации».

Переживший существенные реформы УК Республики Казахстан, вступивший в силу 1 января 2015 г., предусматривает отдельную главу, посвященную преступлениям, совершаемым в сфере информатизации и связи (гл. 7), в которой с учетом квалифицирующих обстоятельств содержится 38 составов преступлений против электронных информационных ресурсов и систем или сетей телекоммуникаций. Стоит подчеркнуть, что в новый УК РК были инкорпорированы положения семи статей гл. 30 «Преступления против информационной безопасности» Модельного Уголовного кодекса для государств – участников СНГ[1].

Так, в УК РК предусмотрена ответственность за неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций, повлекший существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства (ч. 1 ст. 205). Частью 2 указанной нормы предусмотрена ответственность за аналогичные деяния, совершенные в отношении критически важных объектов информационно-коммуникационной инфраструктуры. Преступлением признаются также вышеописанные деяния, повлекшие по неосторожности тяжкие последствия. Аналогичные нормы содержатся в положениях ст. 272, 274.1 УК РФ. Однако отметим, что в УК РФ, в отличие от УК РК, не предусмотрена ответственность за неосторожное причинение вреда объектам критической инфраструктуры. Статьей 206 УК РК предусмотрена ответственность за умышленное неправомерное уничтожение или модификацию охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций. Ответственность за умышленные действия (бездействие), направленные на нарушение работы информационной системы или сетей телекоммуникаций, предусмотрены ст. 207 УК РК. Стоит отметить, что в законодательстве Казахстана отдельно криминализированы неправомерное завладение информацией, выражающееся в умышленном неправомерном копировании или ином неправомерном завладении охраняемой законом информацией, хранящейся на электронном носителе (ст. 208 УК РК); при-

[1] Принят постановлением Межпарламентской Ассамблеи государств – участников СНГ в Санкт-Петербурге 17 февраля 1996 г.

нуждение к передаче информации (ст. 209 УК РК); создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210 УК РК). Наличие в УК РК отдельной нормы, предусматривающей ответственность за принуждение к передаче информации под угрозой применения насилия либо уничтожения или повреждения имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, оглашение которых может причинить существенный вред интересам потерпевшего или его близких, представляется нам интересным решением.

Законодателем введены и иные составы, в частности, ст. 211 «Неправомерное распространение электронных информационных ресурсов ограниченного доступа»; ст. 212 «Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели»; ст. 213 «Неправомерное изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства». Отметим, что указанные нормы (за исключением ст. 213) содержат единый квалифицирующий признак: «совершение преступных действий в отношении критически важных объектов информационно-коммуникационной инфраструктуры», что подчеркивает озабоченность государства возможностью нанесения ущерба противоправным использованием IT-технологий критически важным объектам, таким как энергоснабжение, водоснабжение и т. д.

Интересным представляется и отказ законодателей Казахстана от термина «компьютерные преступления», который используется и в Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации, и в гл. 28 УК РФ.

Термин «компьютер» в узком понимании, учитывая современные реалии и темпы развития информационно-телекоммуникационных технологий, является лишь частью аппаратно-программного комплекса и не исчерпывает всего разнообразия техники и отношений, связанных с обращением информации. Использование понятия «сфера информатизации и связи», под которым понимается совокупность методов, производственных процессов и программно-технических средств, объединенных в технологический комплекс, обеспечивающий сбор, создание, хранение, накопление, обработку, поиск, вывод, копирование, передачу и распространение информации, является, на наш взгляд, более оправданным и уместным.

Особенно следует отметить, что в новом УК РК нашли отражение случаи совершения преступлений против различных объектов уголовно-правовой охраны с использованием информационно-телекоммуникационных технологий, например, ст. 212 «Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели». Введение указанной нормы представляется весьма прогрессивным, однако не совсем ясен механизм привлечения интернет-провайдеров (а именно ими оказывается данная услуга) к ответственности. Так, возникает вопрос, каким образом интернет-провайдер должен узнать о целях лица, обращающегося за услугой по размещению материалов сомнительного содержания. Цель злоумышленника будет реализована только тогда, когда указанные ресурсы будут непосредственно размещены, ввиду чего привлечение интернет-провайдеров к ответственности за предоставление услуги представляется не совсем оправданным. Как видно, данная норма направлена на противодействие преступлениям, совершаемым в сети Интернет. Однако, на наш взгляд, более удачным представляется подход, реализованный в отечественном законодательстве. В частности, реализация ст. 10 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информатизации и информационных технологиях». Согласно данной норме «запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность». По данной норме сайты, посредством которых распространяется запрещенная информация, могут быть заблокированы. Реализация мер, указанных в Законе, стала возможной после вступления в силу приказа Роскомнадзора, МВД России, Роспотребнадзора и ФНС России[1],

[1] Об утверждении критериев оценки материалов и (или) информации, необходимых для принятия решений Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Министерством внутренних дел Российской Федерации, Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека, Федеральной налоговой службой о включении доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет», а также сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие запрещенную информацию, в единую автоматизированную информационную систему «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено: приказ Роскомнадзора № 84, МВД России № 292, Роспотребнадзора № 351, ФНС России ММВ-7-2/461@ от 18 мая 2017 г. Доступ из справочной правовой системы «КонсультантПлюс».

которым утверждены критерии оценки материалов, позволяющие отнести ту или иную информацию к запрещенной.

Говоря об иных странах рассматриваемого региона, стоит отметить, что уголовное законодательство этих стран во многом тождественно отечественному и на сегодняшний день не содержит принципиально удачных решений в вопросе регулирования ответственности за посягательства в IT-сфере. Полагаем, что сегодня среди стран СНГ и ЕАЭС Российская Федерация занимает передовые позиции в вопросе уголовно-правового противодействия IT-преступлениям. Однако темпы развития IT-технологий и введение их в преступный оборот диктуют необходимость постоянного совершенствования норм об ответственности за преступные посягательства в рассматриваемой сфере. Особую озабоченность вызывает и отсутствие регулирования в сфере обращения технологии «блокчейн» и криптовалют. Эксперты ЕАЭС понимают, что запрет криптовалют затормозит развитие цифровой экономики в целом. Тормозит процесс формирования единого рынка ЕАЭС в данной сфере и отсутствие позиции национальных регуляторов государств-членов по данному вопросу. В указанных обстоятельствах поиск эффективной модели взаимодействия и единого подхода к регулированию новых информационно-телекоммуникационных технологий представляется как никогда необходимым и востребованным. Ввиду транснационального характера рассматриваемой преступности единая политика необходима и в сфере уголовно-правового противодействия. Длительная неурегулированность правоотношений в рассматриваемой сфере ведет ко все большей привлекательности региона в качестве площадки для развития теневого Интернета со всеми вытекающими последствиями. «Оперативная и согласованная регуляторная политика позволит максимально эффективно использовать стимулы новых технологических явлений в обеспечении устойчивого экономического роста и повышении конкурентоспособности государств – членов ЕАЭС»[1].

[1] Рябцев Н.В. Вызовы устойчивого экономического развития ЕАЭС в эпоху цифровизации национальных экономик (на примере криптовалют и блокчейн) 28 марта 2018 г. URL: https://www.ictsd.org/bridges-news

Заключение

Цифровая экономика и преступные проявления в ней – это глобальные явления, развивающиеся большей частью на наднациональном уровне. Указанное обстоятельство предопределяет необходимость гармонизации подходов к нормативному регулированию, способных предупредить и предотвратить возникающие угрозы в IT-сфере. Необходимость разработки нового универсального документа сегодня очевидна для всего мирового сообщества. Однако на сегодняшний день единого документа пока не принято.

Проанализировав и обобщив зарубежный опыт противодействия уголовно-правовыми средствами преступлениям, совершаемым в цифровой экономике, мы пришли к выводу, что в мире на сегодняшний день наблюдается два подхода к такому противодействию: евроатлантический и евразийский.

Первый подход, являющийся наиболее популярным, основан на положениях Конвенции Совета Европы о преступности в сфере компьютерной информации, принятой в Будапеште 23 ноября 2001 г.

Второй подход (евразийский) реализуется на основе инициатив, предпринимаемых в рамках ШОС и ЕАЭС.

Национальные подходы к криминализации IT-преступлений имеют существенные различия. Преступления, связанные с незаконным доступом к компьютерным системам и данным, различаются в зависимости от объекта преступления (данные, система или информация). В отдельных странах криминализирован доступ как таковой и наличие умысла на причинение ущерба необязательно, в других странах ситуация складывается противоположным образом. Различаются подходы к наличию умысла в составе преступления при криминализации вмешательства в функционирование компьютерных систем или данные. В большинстве стран вмешательство должно быть преднамеренным, в то время как в других странах предусматривается и вмешательство по неосторожности. Деяния, характеризуемые как вмешательство, охватывают деяния от повреждения или удаления до изменения, блокировки, ввода или передачи данных. Криминализация незаконного перехвата данных различается в зависимости от того, ограничивается ли правонарушение перехватом не предназначенных для общего пользования данных или не ограничивается им, а также в зависимости от того, ограничивается ли преступление перехватом при помощи технических средств.

Наиболее развитым законодательством в рассматриваемой сфере на сегодняшний день обладают страны Европейского континента, Северной Америки и Тихоокеанского региона. Во многом это объясняется тем, что государства указанных регионов являются лидерами цифрового развития. Отличительной особенностью этих стран считается принятие национальных планов и стратегий в сфере обеспечения кибербезопасности. В отдельных странах приняты стратегии противодействия киберпреступности, предполагающие комплексные меры – от повышения эффективности международного сотрудничества и совершенствования законодательной базы до создания отдельной системы подготовки кадров по борьбе с IT-преступностью, в том числе и основным ее направлением – блокчейн-преступностью.

Уголовное законодательство европейских стран в области противодействия IT-преступности достаточно унифицировано ввиду имплементации всеми странами положений Конвенции Совета Европы о преступности в сфере компьютерной информации. Кроме того, в некоторых директивах и решениях предусмотрена дополнительная уголовная ответственность за преступления, совершенные в отдельных сегментах цифровой экономики. Особенностью европейского законотворчества в рассматриваемой сфере является детальная интерпретация и толкование используемых понятий, что в значительной степени упрощает их применение. Отличительными признаками следует считать также универсальность принимаемых норм, которые имеют свой определенный «срок годности», достаточный в условиях быстрого изменения и внедрения новых IT-технологий, и их постоянный пересмотр в целях соответствия возникающим угрозам. Особое внимание в европейских странах уделяется противодействию преступлениям в криптоиндустрии. Главная направленность этого законодательства – блокировка возможностей для высокотехнологичных преступников развернуть в Европе блокчейн-преступность или использовать криптовалюты в операциях кибепреступников или террористов.

В уголовном законодательстве США криминализирован широкий спектр деяний. Конструкция юридических норм американского законодательства позволяет привлекать к ответственности за противоправные деяния в финансовой сфере с использованием новых, еще не получивших широкого распространения информационно-телекоммуникационных технологий.

Не во всех странах криминализированы средства неправомерного использования компьютеров. В тех странах, где они криминализиро-

ваны, имеются различия в зависимости от того, связано ли преступление с хранением, распространением или использованием программного обеспечения (такого, как вредоносные программы) и (или) компьютерных кодов доступа (например, паролей потерпевшей стороны). С точки зрения международного сотрудничества такие различия могут влиять на двойную уголовную ответственность.

В ряде стран приняты специальные положения в отношении компьютерного мошенничества, подлога и использования персональных данных. В других странах используются общие положения в отношении мошенничества или хищения либо за основу берутся преступления, отражающие составные элементы деяния, такие как незаконный доступ, вмешательство в данные и подлог. Весьма широкое распространение получила криминализация правонарушений, связанных с содержанием данных, особенно преступлений, касающихся детской порнографии.

В большинстве стран наблюдается тенденция к ужесточению ответственности за противоправные посягательства в IT-сфере и непрерывная реформация норм уголовного законодательства как реагирование на возникающие угрозы. Ужесточение ответственности за посягательства с использованием информационно-телекоммуникационных технологий, учитывая неограниченность круга потенциальных жертв преступных действий и размеры причиняемого ущерба, на наш взгляд, должно быть реализовано и в отечественном законодательстве.

Литература

Нормативные правовые акты

1. Салвадорская декларация о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире: принята резолюцией Генеральной Ассамблеи 65/230 от 21 дек. 2010 г. URL: http://www.un.org/ru/documents/decl_conv/declarations/salvador_declaration

2. Борьба с преступным использованием информационных технологий: резолюция Генеральной Ассамблеи ООН 55/63 от 22 янв. 2001 г. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/563/19/PDF

3. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности: резолюция Генеральной Ассамблеи ООН A/RES/53/70 от 4 янв. 1999 г. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lan

4. Право на неприкосновенность личной жизни в цифровой век: резолюция Генеральной Ассамблеи ООН A/RES/68/167 от 18 дек. 2013 г. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/49/PDF/N1344949.pdf?OpenElement

5. Расширение сотрудничества в борьбе с кибертерроризмом и другими широкомасштабными агрессивными действиями в Интернете: резолюция ПАСЭ 2070 (2015). URL: https://nxtp://assembly.coe.int

6. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 нояб. 2001 г.). Доступ из справочно-правовой системы «Гарант».

7. Об обеспечении прав на интеллектуальную собственность: директива Европейского парламента и Совета ЕС 2004/48/ЕС от 29 апр. 2004 г. // Официальный журнал Евросоюза. NL 157. 30.04.2004. С. 45–86.

8. Об атаках на информационные системы и о замене Рамочного Решения 2005/222/ПВД Совета ЕС: директива Европейского парламента и Совета ЕС 2013/40/ЕС от 12 авг. 2013 г. URL: https://www.coe.int/ru/web/conventions

9. О предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма, об изменении Регламента (ЕС) 648/2012 Европейского парламента и Совета ЕС и об отмене Директивы 2005/60/ЕС Европейского парламента и Совета ЕС и Директивы 2006/70/ЕС Европейской Комиссии: директива Европейского парламента и Совета ЕС 2015/849 от 20 мая 2015 г. // Официальный журнал Евросоюза. NL 141. 05.06.2015. С. 73.

10. О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза: директива Европейского парламента и Совета ЕС № 2016/1148 от 6 июля 2016 г. // Официальный журнал Евросоюза. NL 194. 19.07.2016. С. 1.

11. Об учреждении и деятельности организаций, эмитирующих электронные деньги, о пруденциальном надзоре за их деятельностью, а также об изменении директив 2005/60/ЕС и 2006/48/ЕС и об отмене Директивы 2000/46/ЕС: директива Совета ЕС № 2009/110/ЕС от 16 сент. 2009 г. // Официальный журнал Евросоюза. NL 267. 10.10.2009 С. 7.

12. Последующая деятельность по итогам тринадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию и подготовка к четырнадцатому Конгрессу Организации Объединенных Наций по предупреждению преступности и уголовному правосудию: доклад Генерального секретаря ООН (Вена, 14–18 мая 2018 г.). URL: http://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_27/ECN152018_11_r_V1801147.pdf

13. Документ A/65/201. Доклад правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. URL: https://www.un.org/disarmament/ru

14. Об инкриминировании расистских актов и совершенного ксенофоба при помощи информационных систем: дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации № 189 от 1 марта 2006 г. URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/ treaty/189

15. О сотрудничестве в области обеспечения международной информационной безопасности: межправительственное соглашение государств – членов Шанхайской организации сотрудничества от 16 июня 2009 г. URL: http://rus.sectsco.org/documents/20090616/203974.html

16. Об утверждении Концепции кибербезопасности («Киберщит Казахстана»): постановление Правительства Республики Казахстан от 30 июня 2017 г. № 407. URL: http://adilet.zan.kz/rus/docs/P1700000407

17. Об утверждении государственной программы Российской Федерации «Информационное общество (2011–2020 годы)»: постановление Правительства РФ от 15 апр. 2014 г. № 313. Доступ из справочной правовой системы «КонсультантПлюс».

18. О внесении изменений в государственную программу Российской Федерации «Информационное общество (2011–2020 годы)»: постановление Правительства РФ от 30 марта 2018 г. № 369-16. Там же.

19. О мерах по развитию цифровой экономики в Республике Узбекистан: постановление Президента Республики Узбекистан от 3 июля 2018 г. № ПП-3832. URL: http://www.lex.uz/ru/pdfs/3806048

20. Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года: приказ Генеральной прокуратуры РФ от 14 сент. 2017 г. № 627. Доступ из справочной правовой системы «КонсультантПлюс».

21. О Рабочей группе Министерства здравоохранения Российской Федерации по созданию и развитию национального сегмента Российской Федерации международных информационных систем развития цифровой экономики: приказ Министерства здравоохранения РФ от 26 июня 2015 г. № 382. Там же.

22. Об утверждении Указаний о порядке применения бюджетной классификации Российской Федерации: приказ Минфина России от 1 июля 2013 г. № 65н. Там же.

23. О внесении изменений в состав Рабочей группы по адаптации ведомственных информационных систем к национальному сегменту международных информационных систем развития цифровой экономики: приказ Федеральной службы по интеллектуальной собственности от 15 сент. 2015 г. № 132. Там же.

24. Об утверждении программы «Цифровая экономика Российской Федерации»: распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р. Там же.

25. О решениях по итогам заседания президиума Совета при Президенте России по стратегическому развитию и приоритетным проектам: поручение Правительства РФ от 26 июля 2017 г. № 8. Там же.

26. О внесении изменений в состав межведомственной рабочей группы по взаимному признанию электронной цифровой подписи, изготовленной в соответствии с законодательством одного государства – члена Евразийского экономического союза, другим государством-членом в целях исполнения раздела XXII Договора о Евразийском экономическом союзе от 29 мая 2014 года: распоряжение Коллегии Евразийской экономической комиссии от 19 дек. 2017 г. № 193. Там же.

27. О проекте распоряжения Совета Евразийской экономической комиссии «О перечне мероприятий по реализации основных ориентиров макроэкономической политики государств – членов Евразийского экономического союза на 2017–2018 годы»: распоряжение Коллегии Евразийской экономической комиссии от 29 авг. 2017 г. № 107. Там же.

28. Об утверждении состава рабочей группы по выработке предложений по формированию цифрового пространства Евразийского экономического союза: распоряжение Коллегии Евразийской экономической комиссии от 29 июня 2016 г. № 89. Там же.

29. О Концепции федеральной целевой программы «Развитие внутреннего и въездного туризма в Российской Федерации (2019–2025 годы)»: распоряжение Правительства РФ от 5 мая 2018 г. № 872-р. Доступ из справочной правовой системы «КонсультантПлюс».

30. О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных): регламент Европейского парламента и Совета ЕС 2016/679 от 27 апр. 2016 г. // Официальный журнал Евросоюза. NL 119. 04.05.2016. С. 1–88.

31. Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года: решение Высшего Евразийского экономического совета от 11 окт. 2017 г. № 12. Доступ из справочной правовой системы «КонсультантПлюс».

32. Об Основных направлениях промышленного сотрудничества в рамках Евразийского экономического союза: решение Евразийского межправительственного совета от 8 сент. 2015 г. № 9. Там же.

33. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г.: ратифицировано Федер. законом РФ от 1 окт. 2008 года № 164-ФЗ // Собр. законодательства РФ. 2009. № 13. Ст. 1460.

34. Соглашение о сотрудничестве между правительствами государств – членов Шанхайской организации сотрудничества в борьбе с преступностью (Ташкент, 11 июня 2010 г.). Доступ из справочной правовой системы «КонсультантПлюс».

35. О Стратегии научно-технологического развития Российской Федерации: указ Президента РФ от 1 дек. 2016 г. № 642. Там же.

36. О Стратегии экономической безопасности Российской Федерации на период до 2030 года: указ Президента РФ от 13 мая 2017 г. № 208. Там же.

37. Об Экономическом совете при Президенте Российской Федерации: указ Президента РФ от 16 июля 2012 г. № 1001. Там же.

38. Об основных направлениях государственной политики по развитию конкуренции: указ Президента РФ от 21 дек. 2017 г. № 618. Там же.

39. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: указ Президента РФ от 7 мая 2018 г. № 204. Там же.

40. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента РФ от 9 мая 2017 г. № 203. Там же.

41. О внесении изменений в Уголовный кодекс Российской Федерации: федер. закон от 23 апр. 2018 г. № 111-ФЗ. Там же.

42. Уголовный кодекс Азербайджанской Республики. СПб.: Юридический центр Пресс, 2001.

43. Уголовный кодекс Кыргызской Республики. СПб.: Юридический центр Пресс, 2002.

44. Уголовный кодекс Республики Казахстан. Алматы: ЮРИСТ, 2014.

45. Уголовный кодекс Республики Молдова. СПб.: Юридический центр Пресс, 2003.

46. Уголовный кодекс Швейцарии от 21 дек. 1937 г. (по сост. на 11 июля 2017 г.). URL: http://www.wipo.int/wipolex/ru/profile.jsp?code=CH

47. Проект Национальной стратегии развития Кыргызской Республики на 2018–2040 годы. URL: http://www.president.kg/ru/sobytiya/novosti/6015_proekt_nacionalnoy_strategii_razvitiya_

48. Council Document 5842/2/2010. Internal Security Strategy for the European Union: Towards a European Security Model. Brussels, 2010. P. 7–31.

49. Internet Governance – Council of Europe Strategy 2016–2019 Democracy, human rights and the rule of law in the digital world // Documents and Publications Production Department (SPDP), Council of Europe, September 2016.

50. Cyber Security Strategy for Norway. URL: https://www.regjeringen.no/globalassets/upload/fad/vedlegg/iktpolitikk/cyber_security_strategy_norway.pdf

51. International cyber strategy for Norway 2017. Published by: Norwegian Ministry of Foreign Affairs.

52. National strategy for Switzerland's protection against cyber risks. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Switzerlands_Cyber_Security_strategy.pdf

53. Public Law 104-294, National Information infrastructure protection act, October 11, 1996. URL: http://www.gpo.gov

54. Public Law 107-305, Cybersecurity Research and development Act, November, 27, 2002. URL: http://www.gpo.gov

55. Public Law 107-347, Homeland security Act, November, 25, 2002. URL: http://www.gpo.gov

56. Public Law 113-246, Cybersecurity workforce assessment Act, December, 18, 2014. URL: http://www.gpo.gov

57. Public Law 113-282, National cybersecurity Act, December, 18, 2014. URL: http://www.gpo.gov

58. Public Law 113-283, Federal information security modernization Act, 18, 2014. URL: http://www.gpo.gov

59. Public Law 114-113, Cybersecurity Act of 2015, December, 18, 2015. URL: http://www.gpo.gov

60. Public Law 98-473, Counterfeit access device and computer fraud and abuse act 1984, October 12, 1984. URL: http://www.gpo.gov

61. Public Law 99-474, Computer Fraud and Abuse Act, October 16, 1986. URL: http://www.gpo.gov

62. The serious Crime Act 2015. URL: http://www.nationalcrimeagency.gov.uk

63. Digital Economy Act 2017. URL: https://http://www.wipo.int/wipolex/ru/text.jsp?file_id=474843

Отчеты и аналитические обзоры

1. Доклад о мировых инвестициях 2017. Инвестиции и цифровая экономика. Основные тенденции и общий обзор // ООН ЮНКТАД. С. 4.
2. Антонян Ю.М., Бражников Д.А., Гончарова М.В. и др. Комплексный анализ состояния преступности в Российской Федерации и расчетные варианты ее развития: аналит. обзор. М.: ВНИИ МВД России, 2018. С. 32–37.
3. Всестороннее исследование проблемы киберпреступности: проект, февраль 2013 года. URL: http://www.unodc.org
4. IT-рынок Сингапура и прогнозы рынка Азии в 2017 г. URL: https://saleslabel.com/it-rynok-singapura-i-prognozy-rynka-azii-v-2017-godu
5. Global Cybersecurity Index 2017 of International Telecommunication Union. URL: http://itu.int
6. Alan Davidson Commerce Department Digital Economy Agenda 2016. May 2016.
7. Alan Charles Raul. Touring the World of Cybersecurity Law // RSAConference 2016, February 29 – March 4.
8. Anwer Yusoff. Cybersecurity Standards: a Case Study on Malaysian Banking Sector // Cybersecurity Malaysia. 2013.
9. Bhaskar Chakravorti and Ravi Shankar Chaturvedi. Digital planet 2017. How competitiveness and trust in digital economies vary across the world. The Fletcher School, Tufts University. July 2017.
10. Symantec Norton Cybercrime report, 2016. URL: www.symantec.com
11. The United Nations Economic and Social Commission for Western Asia (ESWA) Cyber Legislation Digest, 25–27 March, 2015.
12. Report of the United Nations Economic and Social Commission for Western Asia (ESWA) Cyber Legislation project. URL: http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/enUS/Default.aspx
13. Review of e-commerce legislation harmonization in ASEAN. UNCTAD/DTL/STICT/2013/1

Монографии, учебники и иная учебная литература

1. Бауэр В.П. Проблемы на пути создания унифицированной цифровой платформы цифровой экономики. М., 2017.
2. Бычков А.И. Проведение расчетных операций: способы, специфика и риски. М., 2016.
3. Вайпан В.А. Теория справедливости: право и экономика. М., 2017.

4. Петровский А.В. Мусульманское уголовное право и особенности уголовного законодательства мусульманских государств. Краснодар: КубГУ, 2013.

5. Пузыня Т.А. Понятие цифровых технологий в экономике // Взаимодействие науки и общества: проблемы и перспективы: сб. ст. по итогам Междунар. науч.-практ. конф. (Стерлитамак, 21 октября 2017 г.). Стерлитамак: АМИ, 2017.

6. Эмм Д. Киберпреступность и закон. URL: http://cripo.com.ua

Статьи

1. Агеев А.И., Логинов Е.Л. Битва за будущее: кто первым в мире освоит ноомониторинг и когнитивное программирование субъективной реальности? // Экон. стратегии. 2017. Т. 19. № 2. С. 124–139.

2. Ахромеева Т.С., Малинецкий Г.Г., Посашков С.А. Смыслы и ценности цифровой реальности. Будущее. Войны. Синергетика // Филос. науки. 2017. № 6. С. 104–120.

3. Бакулина А.А., Топчий П.П. Управление и финансы в оборонно-промышленном комплексе: преобразования в рамках цифровой экономики // Банковское право. 2017. № 4.

4. Бауэр В.П., Сильвестров С.Н., Барышников П.Ю. Блокчейн как основа формирования дополненной реальности в цифровой экономике // Информационное общество. 2017. № 3. С. 30–40.

5. Белоус А.П. Вектор развития банков в потоке цифровой революции // Банковское дело. 2017. № 10. С. 16–19.

6. Бестужева О.Ю., Вершинская О.Н. Некоторые особенности развития цифровой экономики // Энергетическая политика. 2017. № 5. С. 49–57.

7. Бетелин В.Б. Цифровая экономика: навязанные приоритеты и реальные вызовы // Государственный аудит. Право. Экономика. 2017. № 3–4. С. 22–25.

8. Бианкина А.О. Цифровые технологии и их роль в современной экономике // Экономика и социум: современные модели развития. 2017. № 16. С. 15–25.

9. Боженок С.А. Зарубежный опыт уголовно-правовой борьбы с преступлениями, совершаемыми с использованием банковских карт // Гражданин и право. 2006. № 4. С. 72–76.

10. Бондарик В.Н., Кудрявцев А.В., Лощинин А.А. Некоторые информационно-технологические аспекты цифровой экономики // Микроэкономика. 2017. № 4. С. 67–71.

11. Вайпан В. Основы правового регулирования цифровой экономики // Право и экономика. 2017. № 11. С. 5–18.

12. Ведута Е.Н. Цифровая экономика приведет к экономической киберсистеме // Междунар. жизнь. 2017. № 10. С. 87–102.

13. Ведута Е.Н., Джакубова Т.Н., Асанова Е.А. Стратегия цифровой экономики как инструмент глобализации // Менеджмент и бизнес-администрирование. 2017. № 3. С. 4–17.

14. Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. 2007. № 2. С. 23.

15. Грамматчиков А., Гурова Т. Золотой век «цифры» наступает // Эксперт. 2017. № 30–33. С. 10–15.

16. Громов Е.В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) // Вестн. Томского гос. пед. ун-та. 2006. № 11. С. 30–35.

17. Дегтярев А.В. Работа в «облаке» как способ сохранения уровня производительности труда в условиях демографической ямы // Экономический анализ: теория и практика. 2017. Т. 16. Вып. 2. С. 299–314.

18. Дубко М. Международное сотрудничество в сфере уголовно-правовой борьбы с неправомерным завладением компьютерной информацией. URL: http://www.Crime-research.ru

19. Дыжин А. Цифровая экономика майнит // Эксперт-Сибирь. 2017. № 41–42. С. 24–26.

20. Звечаровский И.Э. Новый УК: проблемы применения // Законность. 1999. № 1. С. 10.

21. Иванов В.В., Малинецкий Г.В. Цифровая экономика: от теории к практике // Инновации. 2017. № 12. С. 3–12.

22. Иванов В.В., Малинецкий Г.В. Стратегические приоритеты цифровой экономики // Стратегические приоритеты. 2017. № 3. С. 54–95.

23. Иванов О.А. На пути к цифровой экономике // Вопросы образования. 2017. № 1. С. 84–85.

24. Калиш Я.В. Информационная политика ЕАЭС – цифровое настоящее и будущее // Власть. 2017. № 10. С. 67–71.

25. Карцхия А. Цифровой императив: новые технологии создают новую реальность // Интеллектуальная собственность. Авторское право и смежные права. 2017. № 8. С. 17–26.

26. Кешелава А.В., Самарин А.В., Амзараков М.Б. Инфраструктура цифровой экономики // Экон. стратегии. 2017. Т. 19. № 8. С. 120–131.

27. Краснушкина Н. «Цифровая экономика» обрастает регуляторами. Власти задумались о координации нормотворчества // Коммерсант. 2018. 10 янв. С. 2.

28. Кунцман А.А. Специфика адаптации современных компаний в условиях цифровой экономики // Инновации. 2017. № 9. С. 14–21.

29. Левин Л.Л. Цифровая революция ожидает Россию в 2018 году. Переход российских компаний на отечественное программное обеспечение неизбежен // Парламентская газета. 27 дек. 2017 г. URL: https://www.pnp.ru

30. Медведев Ю. Шифр в абсолюте // Рос. газ. 2018. 21 февр. С. 11.

31. Нурмухаметов Р.К., Степанов П.Д., Новикова Т.Р. Технология блокчейн: сущность, виды, использование в российской практике // Деньги и кредит. 2017. № 12. С. 101–103.

32. Овчинский В., Ларина Е. Криптовалюта, блокчейн и преступность. URL: http://zavtra.ru/blogs/kriptovalyuta_blokchejn_i_prestupnost_

33. Паньшин Б. Цифровая экономика: особенности и тенденции развития // Наука и инновации. 2016. № 3 (157). С. 17–20.

34. Попов Е., Семячков Е. Анализ трендов развития цифровой экономики // Проблемы теории и практики управления. 2017. № 10. С. 82–91.

35. Розенберг Е.Н., Уманский В.И., Дзюба Ю.В. Цифровая экономика и цифровая железная дорога // Транспорт Российской Федерации. 2017. № 5. С. 45–49.

36. Рябцев Н.В. Вызовы устойчивого экономического развития ЕАЭС в эпоху цифровизации национальных экономик (на примере криптовалют и блокчейн), 28 марта 2018 г. URL: https://www.ictsd.org/bridges-news

37. Саркисянц А. Цифровой банкинг: мировой опыт и российская специфика // Бухгалтерия и банки. 2018. № 6.

38. Свириденко Д. Принять вызов цифровой экономики // Эксперт-Сибирь. 2017. № 48–49. С. 40–41.

39. Сидоренко Э.Л. Криминологические риски оборота криптовалюты // Экономика. Налоги. Право. 2017. № 6. С. 147–154.

40. Смирнов Ф.А. Блокчейн и «умные контракты» как ключевые факторы развития «цифровой экономики» // Валютное регулирование. Валютный контроль. 2017. № 4. С. 54–58.

41. Соколов И.А. Инновационные технологии цифровой экономики как важное условие достижения бюджетных гарантий для организации обороны и обеспечения безопасности страны // Вестн. Акад. воен. наук. 2017. № 2. С. 37–40.

42. Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал рос. права. 2018. № 2.

43. Устинович Е.С. Цифровая экономика и новая социальная доктрина // Социальная политика и социальное партнерство. 2017. № 7. С. 33–41.

44. Устюжанина Е.В., Сигарев А.В., Шеин Р.А. Цифровая экономика как новая парадигма экономического развития // Национальные интересы: приоритеты и безопасность. 2017. Т. 13. Вып. 10. С. 1788–1804.

45. Федорков А.А., Бирюков О.А. Цифровая экономика: особенности управления и тенденции развития // Петербургский экономический журнал. 2017. № 3. С. 60–66.

46. Хохлова М.Н. Новая архитектура цифровой экономики // Экономические стратегии. 2017. № 4. С. 132–144.

47. Черновалов А.В., Солодуха П.В. Институциональное измерение цифровой экономики // Социальная политика и социология. 2017. Т. 16. № 2. С. 104–112.

48. Bushra Mohamed Elamin Elnain. Cybercrime in Kingdom of Saudi Arabia: The threat today and expected future // Information and knowledge management. 2013. Vol. 3. № 12. P. 14–18.

49. Hee Jhee Jiow. Cybercrime in Singapore: An analysis of regulation based on lessig's four modalities of constraint // International journal of cyber criminology (IJCC). January – June 2013. Vol. 7 (1): 18–27.

50. Stein Schjolberg. The history of cybercrime 1976–2014. Oslou.

51. Sulaiman Al Amro Cybercrime in Saudi Arabia: fact or fiction // International Journal of Computer Science Issues. 2017. Vol. 14. Iss. 2. P. 36–42.

Диссертации, авторефераты диссертаций

1. Данг Хай Дан. Развитие информационных технологий в АСЕАН: автореф. дис. … канд. экон. наук. М., 2008.

2. Ефремова М.А. Уголовно-правовая охрана информационной безопасности: дис. ... д-ра юрид. наук. М., 2017.

3. Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ: автореф. дис. … канд. юрид. наук. М., 2005.

4. Томилин О.О. Административная ответственность юридических лиц за правонарушения в финансовой сфере: автореф. дис. … канд. юрид. наук. Саратов, 2003.

5. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. … канд. юрид. наук. Владивосток, 2005.

6. Чеботарева А.А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе: дис. ... д-ра юрид. наук. М., 2017.

7. Чупрова А.Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. ... д-ра юрид. наук. М., 2015.

Интернет-ресурсы

1. Армения создаст свободную экономическую зону для развития блокчейн-проектов. URL: https://forklog.com/armeniya-sozdast-svobodnuyu-ekonomicheskuyu-zonu-dlya-razvitiya-blokchejn-proektov

2. В США арестовали «повелителя» темной стороны интернета. URL: https://www.rbc.ru/society/02/10/2013/570410869a794761c0ce255e

3. В Тайланде вступил в силу закон о регулировании криптовалют. URL: https://cryptolot.ru/post_v-tailande-vstupil-v-silu-zakon-o-regulirovanii-kriptovalyut_399

4. В Филиппинах ужесточат наказания за криптовалютные преступления. URL: https://yandex.ru/turbo?text=https%3A%2F%2Fwww.rbc.ru%2Fcrypto%2Fnews%2F5ad763919a794719b73b96ec&fallback=1

5. В Швейцарии воруют в киберпространстве. URL: http://nashagazeta.ch/news/12610

6. Всемирная встреча на высшем уровне по вопросам информационного общества. URL: http://www.un.org/ru/events/pastevents/wsis.shtml

7. Государственная программа «Цифровой Казахстан». URL: https://primeminister.kz/rupage/view/gosudarstvennaya_programma_digital_kazahstan

8. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. URL: https://www.un.org/disarmament/ru

9. Европарламент ужесточил контроль за криптовалютами. URL: https://ru.slovoidilo.ua/2018/04/20/novost/mir/evroparlament-uzhestochil-kontrol kriptovalyutami

10. Законодательство о киберпреступлениях в зарубежных странах // РИА. URL: http://www.ligainternet.ru/publications/publication.php?ID=2065

11. Заявление глав государств – членов ШОС по международной информационной безопасности (г. Шанхай, 15 июня 2006 г.). URL: http://rus.sectsco.org/load/44842

12. Информация Управления ООН по наркотикам и преступности. URL: http://cybrepo.unodc.org

13. Комиссия Организации Объединенных Наций по торговле и развитию. URL: http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

14. Конференция по киберпреступности: доказательства в киберпространстве, данные WHOIS, кибернасилие, общемировое состояние законодательства. URL: https://www.coe.int/ru/web/portal/-/conference-on-cybercrime-evidence-in-cyberspace-whois-data-cyberviolence-global-state-of-legislation

15. Официальный сайт Правительства Великобритании. URL: http://www.gov.uk

16. Предложения по участию АРБ в мероприятиях по направлению «Нормативное регулирование цифровой экономики». URL: http://regulation.gov.ru/projects#npa=75671

17. Путин выступил на Международном конгрессе по кибербезопасности. URL: https://www.gazeta.ru/tech/2018/07/06/11827759/putin_cybercongress.shtml

18. Путин призвал выработать единые международные правила игры в цифровой сфере. URL: http://tass.ru/ekonomika/5352758

19. Российская ассоциация электронных коммуникаций. URL: http://raec.ru

20. Россия онлайн? Догнать нельзя отстать. URL: http://image-src.bcg.com/Images/BCG-Russia-Online_tcm27-152058.pdf

21. Самые цифровые страны мира. URL: https://hbr-russia.ru

22. Совещание по вопросу использования цифровых технологий в финансовой сфере. URL: http://www.kremlin.ru/events/president/news/55813

23. Цифровая трансформация европейской промышленности затронет каждого. URL: http://group- global.org/en/node/121984

24. Швейцария заняла 18-е место в рейтинге стран по кибербезопасности. URL: http://nashagazeta.ch/news/politique/shveycariya-zanyala-18-oe-mesto-v-reytinge-stran-po-kiberbezopasnosti

25. Швейцария меняет закон о защите данных. URL: http://www.towave.ru/pub/shveitsariya-menyaet-zakon-o-zashchite-dannykh.html

26. Швейцария постоянно подвергается кибератакам. URL: http://https://www.swissinfo.ch

27. California Computer Crime Laws. URL: https://state-laws.findlaw.com/california-law/california-computer-crimes-laws.html

28. Commerce Department Digital Economy Agenda. URL: https://www.ntia.doc.gov

29. Common Criteria for Information Technology Security Evaluation Security. URL: http://www.ipa.go.jp/security/jisec/cc/documents/CCPART1V3.1R4.pdf

30. Cybercrimelaw. URL: http://www.cybercrimelaw.net/Norway.html

31. Cybersecurity: Protecting the digital economy. URL: https://www.euractiv.com/section/digital/linksdossier/cybersecurity-protecting-the-digital-economy

32. Electronic Frontier Foundation. URL: https://www.eff.org

33. Federal Information Technology Security Assessment Framework. URL: http://csrc.nist.gov/drivers/documents/Federal-IT-Security-Assessment-Framework.pdf

34. Federal Office for Information Security. URL: http://www.bsi.bund.de/EN/Home/home_node.html

35. Gartner Analysts. URL: https://www.gartner.com/technology/analysts.jsp

36. Illegal network used cryptocurrencies and credit cards to launder more than EUR 8 million from drug trafficking. URL: https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking

37. Michael Isler, Hugh Reeves and Jürg Schneider. Cybersecurity. Switzerland. URL: https://gettingthedealthrough.com/area/72/jurisdiction/29/cybersecurity-switzerland

38. The Crown Prosecution Service. URL:https://www.cps.gov.uk/legal-guidance/computer-misuse-act-1990

39. Will cybercrime and other cybersecurity issues undermine the digital economy? URL: https://www.welivesecurity.com/2017/04/26/will-cybercrime-and-other-cybersecurity-issues-undermine-the-digital-economy

40. WIPO Lex. URL: http://www.wipo.int/wipolex/ru/profile.jsp?code=CH

Оглавление

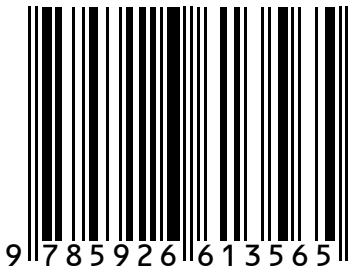
Научное издание

Хисамова Зарина Илдузовна

МЕЖДУНАРОДНЫЙ ОПЫТ УГОЛОВНО-ПРАВОВОГО ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ЦИФРОВОЙ ЭКОНОМИКИ

Редактор *М. В. Краснобаева*
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-1356-5



Подписано в печать 15.08.2018. Формат 60х84 1/16.
Усл. печ. л. 6,7. Тираж 500 экз. Заказ 704.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.