УДК 343.23:004.056

Пучков Д. В.
Puchkov D. V.

ПРАВОВЫЕ АСПЕКТЫ СОТРУДНИЧЕСТВА ПО ПРОТИВОДЕЙСТВИЮ И БОРЬБЕ С ПРЕСТУПНОСТЬЮ В СФЕРЕ РЕАЛИЗАЦИИ КИБЕРНЕТИЧЕСКИХ ТЕХНОЛОГИЙ

LEGAL ASPECTS OF COOPERATION ON COUNTERACTION AND FIGHT CRIME IN THE SPHERE OF IMPLEMENTATION OF CYBERNETIC TECHNOLOGIES

Установлено, что за счет реализации интересов государства в области кибербезопасности, идентификации государственного сегмента критической инфраструктуры электросвязи и концентрации ресурсов государства на обеспечении его кибербезопасности актуальной становится выработка альтернативной модели регулирования для частной отрасли, определяющей рамочные нормы, меры и требования в части кибербезопасности. При этом правоохранительные органы должны сосредоточить усилия на преследовании киберпреступников, где бы они ни находились, что предполагает сотрудничество российского государства с международными партнерами. Помимо этого, следует продолжить работу по повышению уровня осведомленности и стандартов кибербезопасности.

It is determined that due to the implementation of the state interests in the field of cybersecurity, identification of the state segment in critical telecommunication infrastructure and concentration of state resources on ensuring cybersecurity of this state segment, the development of an alternative model of regulation for the private sector, which determines the framework norms, measures and requirements in terms of cybersecurity, becomes relevant. At the same time, law enforcement agencies should focus on the prosecution of cybercriminals, wherever they are, which implies the cooperation of the Russian state with international partners. In addition, awareness-raising and cybersecurity standards should continue to be promoted.

Ключевые слова: уголовное право, международное сотрудничество, киберпреступность, кибербезопасность, меры противодействия преступности, кибертехнологии.

Keywords: criminal law, international cooperation, cybercrime, cybersecurity, measures against crime, cyber technologies.

Первоочередной задачей правоохранительных органов РФ является координация работы с международными партнерскими агентствами по определению, предупреждению и пресечению враждебной деятельности со стороны иностранных субъектов, киберпреступников и террористов для усовершенствования методов сбора и использования информации в целях получения упреждающих разведывательных данных относительно намерений и возможностей киберпреступников.

Сотрудничество государств по борьбе с преступностью в сфере кибертехнологий во многом определяется деятельностью Международной организации уголовной полиции – Интерполом. Эта организация была учреждена в 1923 г. на Международном полицейском конгрессе в качестве Международной комиссии уголовной полиции, которая уже в качестве Интерпола, начиная с 1956 г., с момента утверждения Устава организации на 25-й сессии Генеральной Ассамблеи ООН, обрела статус универсальной международной организации специальной компетенции. К настоящему моменту Генеральной Ассамблеей Интерпола уже приняты резолюции, регламентирующие меры противодействия отдельным видам преступлений в сфере кибертехнологий.

Генеральная Ассамблея Интерпола приняла резолюции, направленные на противодействие торговле детской порнографией с использованием интернета, в частности, в резолюции № AGN/65/RES/9 «Международная торговля детской порнографией» представлены рекомендации по декриминализации производства, распространения, ввоза или владения детской порнографией, в том числе подстрекательству и пособничеству в совершении подобных деяний, а также указаны направления совершенствования нормативного регулирования, в рамках которого предусмотрена конфискация имущества, полученного в результате совершения подобных преступлений. Также в резолюции установлено требование придания максимальной важности расследованию фактов распространения детской порнографии с использованием кибертехнологий.

В резолюции № AG-2005-RES-09 «К вопросу о веб-сайтах, продающих детскую порнографию и торгующих детьми» установлены требования по совершенствованию процессуального законодательства в части сотрудничества и взаимодействия правоохранительных органов по расследованиям деятельности веб-сайтов, продающих детскую порнографию, повышению уровня обмена информацией по подобным деяниям, а также отмечена необходимость информирования Генерального Секретариата обо всех идентифицированных преступниках и детях, чтобы избежать дублирования оперативной и процессуальной деятельности.

К следующему виду относятся резолюции по вопросам противодействия мерам поощрения терроризма в интернете, таковой, в частности, является резолюция № AG-2005-RES-10 «К вопросу о деятельности, ведущейся в интернете, по поощрению терроризма». В данной резолюции заявлено о необходимости принятия законодательных мер по совершенствованию международных расследований и судебного преследования информационной деятельности веб-сайтов, оказывающих поддержку террористам, и создания национальных контактных пунктов в системе правоохранительных органов для быстрого обмена информацией о деятельности подобного рода сайтов.

К третьему виду следует отнести резолюции по вопросам противодействия совершению преступления в сфере незаконного оборота наркотиков с использованием интернета. К таковым следует отнести, например, резолюцию № AG-2006-RES-12 «Преступления, связанные с наркотиками и интернетом», в которой для государств-членов Интерпола представлены рекомендации о мерах противодействия совершению преступления в этой сфере.

Говоря о резолюциях Генеральной Ассамблеи Интерпола по вопросам правоохранительной деятельности, следует указать, что их правовой статус не является обязывающим, однако сам факт инициирования этих вопросов такой авторитетной организацией, как Интерпол, способствует повышению качества борьбы с киберпреступностью, а отсутствие их обязательности позволяет использовать различные, более гибкие подходы к решению проблем борьбы с киберпреступностью на национальном уровне.

Широкие масштабы и постоянный характер деятельности, связанной с киберпреступностью, включая рассылку спама и функционирование ботнетов, указывают на важность и необходимость принятия соответствующих мер, поскольку отдельные преступления совершаются в отношении новых потерпевших нередко при помощи автоматически действующих устройств. В качестве важной меры как в области предупреждения преступности, так и в области оперативного расследования была названа способность отслеживать и устранять вредоносные программы. Среди актуальных мер можно отметить создание полномочий и возможности блокирования либо «удаления» веб-сайтов, используемых для совершения преступлений или распространения незаконного контента и вредоносных программ.

Например, правительством Китая для борьбы с киберпреступностью 1 июля 2015 г. был принят «Закон о национальной безопасности КНР», 6 июля 2015 г. опубликован проект закона «О безопасности в интернете». В декабре того же года по результатам исследований, в том числе и западных коллег из США, Германии, Великобритании и др. [1] был разработан проект

«Закона о борьбе с терроризмом», введенный в действие в 2016 г., согласно которому правительство обеспечивает выявление различных видов террористической информации в интернете с помощью интернет-операторов, которые являются поставщиками услуг, и предприятий, специализирующихся на отслеживании информации в потенциально опасных зонах.

В КНР создан национальный центр информации по борьбе с терроризмом, обеспечивающий сбор информации, координацию работы всех структур и исследований в этой области для своевременного выявления, оперативного вмешательства и предотвращения терроризма.

Разработанная в Китае система «Золотой щит» осуществляет постоянный мониторинг как внешних, так и внутренних сайтов и блокировку доступа, которую довольно сложно обойти. Согласно описанным выше законодательным актам китайские интернет-ресурсы несут ответственность за легитимность информации, более того, все новости они должны цитировать только со специальных медиа-ресурсов, включенных в своеобразный «белый список». Китайский файрвол пока опережает российский блокировщик и с технической, и с юридической точки зрения, однако российские законодатели делают все, чтобы его улучшить.

Так, например, в июле 2016 г. был принят так называемый «закон Яровой – Озерова» [2], призванный решить сразу несколько задач в борьбе с терроризмом, экстремизмом, кибертерроризмом и распространением незаконной информации. Несмотря на сильнейшую критику экспертами и населением возможных серьезных негативных последствий принятых мер и предстоящих колоссальных финансовых затрат на техническое обеспечение, оцениваемых вплоть до 33 млрд долларов США, его реализация уже началась, поскольку безопасность интернета декларируется сегодня как один из приоритетов внутренней политики России.

В дальнейшем Китай планирует развивать сотрудничество с правоохранительными службами других стран для активной борьбы с интернет-преступностью и кибертерроризмом в целом. Так, в опубликованной «Международной стратегии по сотрудничеству в киберпространстве» указано: «Китай усилит политический обмен и сотрудничество с правоохранительными органами других стран по киберпреступности и кибертерроризму» [3]. КНР планирует реализовывать двустороннее сотрудничество с полициями других государств, содействовать обмену опытом по борьбе с киберпреступностью и развивать технологии, вести активное обсуждение конвенций для достижения согласия в данной сфере. Для этих целей Китай планирует усиление сотрудничества со странами-участниками БРИКС, ШОС и АСЕАН [4].

Стратегической целью сотрудничества КНР в сфере кибербезопасности признается получение доступа к лицензиям на приоритетные в рамках импортозамещения технологии и решения, прежде всего аппаратные. Другим способом решения проблемы, не подпадающим под политические риски отношений с Западом, выступают доступные на рынке проекты на основе открытого кода. Добавляя эти источники технологий к своей технологической базе, государство во взаимодействии с отраслью запускает ряд долгосрочных проектов по импортозамещению в сфере кибертехнологий. Приоритетом является разработка собственных конкурентных технологий микропроцессоров и обеспечение для них базы в отрасли микроэлектроники.

Как видно, Россия – не единственное государство, движущееся к регулированию своего сегмента сети и его обособлению. Подобные меры считаются большинством стран необходимыми в связи со все более нарастающей угрозой кибертерроризма.

В настоящее время в краткосрочной перспективе основной целью является повышение защищенности систем, обеспечивающих функционирование критической инфраструктуры и инфраструктур государственных органов, ответственных за обработку конфиденциальных сведений и сведений, содержащих государственную тайну. Главным риском является зависимость операторов таких систем от западных технологий, доступ к которым может быть перекрыт в рамках санкций либо иных последствий ухудшения отношений. В отношении таких систем вырабатывается и принимается дорожная карта их приоритетного импортозамещения.

При этом в соответствии с концепцией разведения рисков и повестки дня в области обеспечения кибербезопасности между государством и частным сектором агентами этих изменений выступают по большей части игроки частного сектора телекоммуникаций и кибертехнологий. Такой подход позволяет учитывать интересы частного сектора отрасли как

в плане безопасности, так и с точки зрения оптимизации и конкурентного развития их трансграничных бизнес-процессов. При этом за счет реализации интересов государства в области кибербезопасности, идентификации государственного сегмента критической инфраструктуры электросвязи и концентрации ресурсов государства на обеспечении его кибербезопасности актуальной становится выработка альтернативной модели регулирования, определяющей рамочные нормы, меры и требования в части кибербезопасности и предоставляющей частным игрокам коридор возможностей для определения своей роли, политики и интересов в этой сфере с учетом самостоятельного несения ими основного бремени рисков.

Сегодня в отношении цифровой трансформации ведущих стран важный посыл в управлении рисками кибербезопасности состоит в консервативном подходе к внедрению новых решений и легализации новых технологий и основанных на них сервисов (финансовые и иные сервисы на распределенных реестрах, беспилотный интеллектуальный транспорт, промышленные применения «интернета вещей», «умные» энергосети и энергосистемы (Smart Grid) и пр.). Консервативный подход к регулированию предполагает практическую реализацию концепции «обеспечение ИБ перед внедрением ИТ», которая позволяет снизить риски, связанные с не продуманным в части безопасности внедрением технологии (например, массовое внедрение незащищенных устройств «интернета вещей», используемых для организации масштабных DDoS-атак).

Также, выступая с позиций консервативного регулятора в нише кибербезопасности, РФ получает возможность «фильтровать» непрерывный поток ИТ-инноваций, достигающих регионального рынка, давая «зеленый свет» прежде всего тем из них, которые уже охвачены регулированием на ее национальном рынке, и тем, внедрение которых в масштабах региона может быть выполнено с опорой на уже имеющиеся и сертифицированные решения в российской отрасли. Следовательно, применительно, например, к ЕАЭС Россия может стать источником модели регулирования в нише кибербезопасности и одновременно закрепить свою позицию ключевого инфраструктурного и технологического провайдера в отрасли для реализации проектов цифровой трансформации, прошедших регуляторный фильтр.

С этой целью государство должно обеспечить максимальное увеличение потенциала поистине инновационного сектора кибербезопасности за счет оказания поддержки стартапам и инвестиций в инновации. Также следует стремиться к выявлению в системе образования перспективных студентов на ранних стадиях обучения и создавать условия для развития их таланта, чтобы сформировать каналы карьерного роста в этой профессии, которая требует более четкого определения. Одновременно государство должно использовать все имеющиеся в его распоряжении рычаги для повышения стандартов кибербезопасности в масштабах национальной экономики, включая, если это необходимо, регулятивные меры. К ним можно отнести разработку и развертывание технологий, в том числе мер активной киберзащиты в партнерстве с отраслевыми предприятиями в целях укрепления безопасности систем и сетей государственного и частного сектора, а также пресечения вредоносной деятельности.

В этой связи значительным шагом в борьбе с киберпреступностью могут стать мероприятия, связанные с совершенствованием систем технической киберзащиты на основе внедрения адекватных этим задачам стандартов. Например, в системах «виртуального банка» переход от стандарта TAN к ITAN сможет обеспечить устранение большей части угроз опасностей, возникающих при совершении фишинг-атак. При этом с точки зрения материально-технического фактора более простым и не менее эффективным решением может стать приоритет защиты основной инфраструктуры и ее элементов: магистральной сети, маршрутизаторов, базовых услуг, а также множества персональных компьютеров, связанных по всему миру.

Для защиты пользователей интернета можно определить две потенциальных целевых группы: конечные пользователи и предприятия (прямой подход), а также поставщики услуг и компании, занятые разработкой программного обеспечения, выступающие значимыми субъектами в стратегии борьбы с киберпреступностью. Наличие у них прямых контактов с клиентами позволяет таким компаниям выступать в качестве гаранта кибербезопасности предприя-

тий, например, передавая им средства защиты и информацию об актуальных угрозах киберпреступлений. В отношении операторов и провайдеров трансграничного доступа в интернет государство должно настаивать на создании ими представительств в юрисдикции РФ.

Реализация механизмов защиты возможна путем продвижения модели государственно-частных партнерств, ориентированных прежде всего на обеспечение беспроводного доступа для жителей российских регионов, где отсутствует широкополосный доступ, а современная высокоскоростная инфраструктура не развита либо ее нет.

В этой связи на основе дублирования баз данных о ресурсах нумерации и пропуске трафика, описанных выше, возможно также создание единой системы мониторинга маршрутизации трафика в пределах российского сегмента интернета. Такая технологическая система может быть создана крупнейшими операторами связи и добровольно пополняться всеми участниками рынка пропуска интернет-трафика для предоставления каждому ее участнику максимально полной информации о доступных альтернативных маршрутах. Доступ к полной картине маршрутизации интернет-трафика в Рунете поможет выявить участки сети со слабой связностью и более эффективно реагировать на DDoS-атаки и аномальные нагрузки, а также идентифицировать критические точки (bottlenecks) российского сегмента сети.

Это предполагает наращивание «вертикальной» связности в пределах национального сегмента интернета, а также ключевых интеграционных объединений с участием РФ за счет инвестирования ресурсов в развитие инфраструктуры крупнейших национальных операторов связи. Параллельной вспомогательной стратегией является укрепление регионального инфраструктурного присутствия российских игроков, в том числе опосредованно контролируемых государством. Оптимальный результат такой работы – трансформация региональной топологии и карты связности в рамках магистральных каналов с целью повышения ее зависимости от высокоскоростной инфраструктуры российских операторов связи в части трансграничного пропуска трафика с одновременным ужесточением государственного контроля над пограничными переходами, используемыми операторами связи в РФ. Должен проводиться курс на максимально возможное сокращение объема интернет-трафика, маршрутизация которого осуществляется между автономными системами, принадлежащими российским субъектам, но через промежуточные узлы за рубежом.

Криптографические возможности имеют фундаментальное значение для защиты секретной информации и решений по использованию потенциала национальной безопасности. Для сохранения этой способности необходимы знания, умения и технологии частного сектора, проверенные спецслужбами. Эта деятельность, очевидно, должна осуществляться на территории России с привлечением граждан, имеющих необходимый допуск и работающих в компаниях, готовых открыто и подробно обсуждать со спецслужбами вопросы проектирования и внедрения решений. Уполномоченные органы должны работать над тем, чтобы оценить резонный объем долгосрочных издержек, связанных с сохранением суверенных криптографических средств, ориентируясь на превалирующие рыночные условия и сотрудничая с компаниями, которые уже способны представить такие решения.

С развитием подобных технологий в России появится возможность существенно понизить киберпреступную деятельность за счет продуктов и услуг, «безопасных по умолчанию». Это означает, что настройки безопасности, встроенные в используемое в России программное и аппаратное обеспечение, должны активироваться производителем по умолчанию, обеспечивая пользователям максимальный уровень безопасности. Сложность заключается в том, чтобы совершить этот трансформационный переворот таким способом, чтобы обеспечить поддержку конечного пользователя и поставку коммерчески жизнеспособных продуктов и услуг и одновременно сохранить свободную и открытую природу среды интернета.

Необходимо решить системные проблемы, лежащие в основе дефицита специалистов в кибернетической области: недостаточное количество молодых людей, выбирающих эту профессию; недостаток имеющихся специалистов по кибербезопасности; недостаточное освещение концепций кибернетической и информационной безопасности в программах компьютерных курсов; нехватка квалифицированных преподавателей; отсутствие канала карьерного роста и подготовки для этой профессии. Следует изучать возможности стимулирования рынка

путем использования рейтингов безопасности новых продуктов для потребителей, определить возможности увязывания таких рейтингов безопасности продуктов с существующими регламентами и способы предупреждения потребителей о том, что действия, которые они собираются совершить в сети, грозят нарушению их безопасности. С другой стороны, кибербезопасность определенных российских организаций имеет особое значение, так как, в случае успеха кибератаки на них, последствия для национальной безопасности страны могут быть чрезвычайно серьезными. Они могут сказаться на жизнедеятельности российских граждан, стабильности и прочности российской экономики, международном авторитете и репутации Российской Федерации. В элитную группу этих компаний и организаций государственного и частного сектора входят предприятия критической национальной инфраструктуры, обеспечение безопасности и устойчивости которых должно стать приоритетом для государства. В эту элитную группу должны также войти компании и организации, требующие более высокого уровня государственной поддержки в этой сфере.

На фоне укрепления защиты от кибератак и уменьшения количества уязвимостей необходимо обеспечить постоянное преследование правоохранительными органами преступников, которые продолжают атаковать российское киберпространство, где бы они ни находились, что предполагает сотрудничество государства с отечественными и международными партнерами в разрушении инфраструктуры и сетей поддержки киберпреступников, а также повышение уровня осведомленности правоохранительных органов и совершенствования стандартов кибербезопасности.

Литература

1. Контртерроризм в Китае необходим. URL: http://www.Legaldaily.com/.

2. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : федер. закон от 06.07.2016 № 374-ФЗ. URL: http://kremlin.ru/.

3. Цзан Ц. Обзор уголовного законодательства о борьбе с терроризмом и «Закона о борьбе с терроризмом» Китая // Евразийск. науч. журн. 2016. № 5. С. 313–318.

4. Китай усилит сотрудничество с другими странами в борьбе с кибертерроризмом. URL: https://ria.ru/.