УДК 343.533
DOI: 10.28995/2073-6304-2018-3-134-141

Проблемы реализации уголовной политики по противодействию преступлениям в сфере высоких технологий

Евгений С. Смольянинов

Российский государственный гуманитарный университет, Москва, Россия; Академия управления МВД России, Москва, Россия, kimowez@mail.ru

Михаил Ю. Воронин

Академия управления МВД России, Москва, Россия, m.voronin@mail.ru

Аннотация. В статье рассматривается содержание высокотехнологичной преступности, ее характеристика, оценка общественной опасности преступности высоких технологий, проблемы противодействия киберпреступности.

Предпринята попытка анализа основных криминологических признаков, характеризующих эту сферу преступной деятельности. Дана классификация преступлений в сфере высоких технологий.

Обозначены основные проблемы реализации уголовной политики в сфере высоких технологий, предложены пути их разрешения.

Ключевые слова: высокотехнологичная преступность, киберпреступность, информационные и коммуникационные технологии, уголовная политика России

Для цитирования: Смольянинов Е.С., Воронин М.Ю. Проблемы реализации уголовной политики по противодействию преступлениям в сфере высоких технологий // Вестник РГГУ. Серия «Экономика. Управление. Право». 2018. № 3 (13). С. 134–141. DOI: 10.28995/2073-6304-2018-3-134-141

Problems of implementation of the criminal policy on combating high-tech offenses

Evgeny S. Smolyaninov

Russian State University for the Humanities, Moscow, Russia; Academy of Management of the Ministry of Internal Affairs of Russia, Moscow, Russia; kimowez@mail.ru

Mikhail Yu. Voronin

Academy of Management of the Ministry of Internal Affairs of Russia, Moscow, Russia, m.voronin@mail.ru

Abstract. The article deals with the content of high-technology crime, its characteristics, the assessment of the public danger of high-tech crime, the problem of countering cybercrime.

An attempt was made to analyze the main criminological characteristics that characterize this sphere of criminal activity. There is a classification of crimes in the field of high technology.

The key issues for the implementation of the criminal policy in the field of high technologies are indicated, ways of their resolution are proposed.

Keywords: high-tech crime, cybercrime, information and communication technologies, criminal policy of Russia

For citation: Smolyaninov ES., Voronin MYu. Problems of implementation of the criminal policy on combating high-tech offenses. *RSUH/RGGU Bulletin. "Economics. Management. Law" Series.* 2018;3(13):134-41. DOI: 10.28995/2073-6304-2018-3-134-141

Введение

Согласно данным исследования «Лаборатории Касперского» с участием более 350 представителей индустриальных организаций по всему миру, включая Россию, за 2017 г. каждая вторая промышленная компания в мире пережила от одного до пяти инцидентов в сфере высоких технологий – они затронули критически важные инфраструктуры или автоматизированные системы управления технологическими процессами. На устранение последствий этих инцидентов, случившихся в течение года, каждая компания потратила в среднем 497 тысяч долларов[1].

Опрос, проведенный «Лабораторией Касперского», также показал, что столкновение с угрозами не стало неожиданностью для промышленных предприятий – три четверти компаний допускают вероятность пострадать от компьютерных атак. Более того, 83% респондентов считают себя хорошо подготовленными к тому, что в их промышленных инфраструктурах может произойти какой-либо инцидент.

Больше всего на сегодняшний день компании опасаются возможности заражения вредоносным программным обеспечением. И реальность показывает, что это не напрасно – 53% пострадавших от инцидентов предприятий подтвердили случаи столкновения с различным вредоносным программным обеспечением.

---

[1] Киберпреступность в мире: Состояние киберпреступности в различных регионах мира [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/ (дата обращения 15 сент. 2018).

Криминологическая характеристика преступлений в сфере высоких технологий

Большинство преступлений в сфере высоких технологий носит скрытый характер. Мировой и российский опыт свидетельствует, что компании-провайдеры услуг связи и интернета порой скрывают недостатки программных и аппаратных комплексов, факты клонирования средств связи, хищения информации и услуг по соображениям престижа и сохранения клиентов, что является обманом клиентов и способствует безнаказанности преступников. Да и пользователи Интернета далеко не все готовы соблюдать правовые нормы.

При этом постоянно расширяющиеся возможности таких программ способствовали трансформации деятельности преступников в один из профессиональных подвидов корыстной преступности, позволяющей осуществлять атаки на различные сферы.

Необходимо отметить и тот факт, что преступность в информационной и телекоммуникационной сфере не коррелируется с общей динамикой преступности в России, показывающей снижение ее уровня. И если в 2013 г. было зарегистрировано 11 104 подобных преступления, то уже в 2016 г. зарегистрировано 65 949 преступлений. Произошедший в 2015–2016 гг. шестикратный рост зарегистрированных и находящихся в производстве преступлений в информационной и телекоммуникационной сфере обусловлен не только несовершенством статистического учета, связанного с необходимостью разграничения преступлений, совершенных с использованием информационных и телекоммуникационных технологий, от преступлений, совершенных непосредственно в информационной и телекоммуникационной среде, но и доступностью программных средств, позволяющих совершать киберпреступления даже слабо подготовленным пользователям.

Необходимо обратить внимание на то, что к числу преступлений, совершаемых непосредственно в информационных и телекоммуникационных сферах, относятся:

– неправомерный доступ к компьютерной информации, статья 272 УК РФ;
– создание, использование и распространение вредоносных компьютерных программ, статья 273 УК РФ;
– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, статья 274 УК РФ.

Существуют процессы, обусловленные качественными преобразованиями, которые не отражаются в статистических данных. Например, анализ нотифицированных вредоносных компьютерных программ, используемых для осуществления DDoS-атак, указывает на то, что в последнее время они все чаще ориентированы не на заражение отдельных компьютеров, а на заражение серверов, что делает атаку более мощной при использовании меньшего количества зараженных объектов. В связи с этим необходимо сделать вывод о постоянном и системном совершенствовании механизмов преступлений в информационной и телекоммуникационной среде. Указанное, в свою очередь, позволяет злоумышленникам совершенствовать механизм преступлений, совершаемых уже с использованием информационных и телекоммуникационных технологий.

Таким образом, мы говорим о существовании двух категорий преступлений. Первая категория включает в себя общеуголовные преступления, совершаемые с использованием компьютерных устройств и программ как средств совершения преступления, например в качестве хранилища либо устройства связи или распространения информации. Она включает в себя любые преступления, совершаемые при помощи компьютерных устройств, такие как распространение порнографии, сбыт или приобретение наркотиков, отмывание денег, незаконные азартные игры, пропаганда ненависти, совершение интернет-мошенничеств и использование этих технологий для хранения, укрытия или общения в уголовной или террористической деятельности. Также к этой категории можно отнести преступления, где компьютерное устройство может использоваться как орудие совершения преступления, например для изготовления поддельных денег, ценных бумаг или документов.

Вторая категория охватывает преступления, где компьютерные устройства или компьютерная сеть выступают в качестве предмета посягательства, например для совершения атак на информацию, компьютерные устройства и их системы. Это и является высокотехнологичной преступностью в сфере информационных и телекоммуникационных технологий и включает такие общественно-опасные деяния как несанкционированное использование компьютерной системы, взлом компьютера или любое несанкционированное использование или распространение данных, отказ в обслуживании и распространение компьютерных вирусов.

Необходимо отметить, что МВД России закрепило единый подход к разделению преступлений на деликты, совершенные с использованием информационно-телекоммуникационных технологий, и на преступления, совершаемые непосредственно в сфере телекоммуникаций и компьютерной информации. Данное разделение определило

порядок взаимодействия между подразделениями МВД России, разграничило зоны ответственности между ними и создало условия по оптимальному реагированию на вызовы и угрозы в данной сфере.

Таким образом, преступления, совершаемые с использованием современных технологий, не относятся к категории совершаемых непосредственно в информационно-телекоммуникационной среде. При этом используемые злоумышленниками интернет-технологии и средства подвижной радиотелефонной связи выступают исключительно в качестве современного удобного инструмента (способа) для поиска и общения с потенциальными жертвами в целях последующего совершения в отношении них противоправных действий экономической или общеуголовной направленности.

Другими словами, существует два глобальных вектора использования информационных и телекоммуникационных технологий в противоправных целях.

Во-первых, передовые технические разработки выступают в качестве новых инструментов, используемых при совершении преступлений. Злоумышленники активно внедряют их для совершенствования существующих преступных схем и поиска новых способов обогащения. Они помогают облегчить координацию деятельности организованных преступных групп и решить целый комплекс сопутствующих задач: от поиска жертв до переводов похищенных денежных средств и сокрытия собственного местоположения.

Решение указанных задач, как правило, не требует от преступников высокой квалификации и глубоких познаний в IT-сфере и в то же время позволяет значительно повысить эффективность их действий.

Этот фактор напрямую влияет на миграцию традиционных форм преступной деятельности в сеть Интернет. В первую очередь во всемирную сеть переместились наиболее простые виды мошенничеств: обман покупателей при продаже авиабилетов или создание интернет-магазинов с целью получения предоплаты за товар без последующей его поставки клиенту. Хищение реквизитов платежных карт с помощью поддельных сайтов кредитных организаций. Злоумышленники просят ввести конфиденциальную информацию: номер карты, срок действия, имя держателя, а также ПИН-код и CVC-код, указанный на оборотной стороне карты.

Вторым ключевым вектором являются угрозы со стороны киберпреступности, которые характеризуются тем, что информационные технологии выступают уже не только в качестве инструмента, но и являют собой среду, в которой совершаются преступления.

Именно в этой среде появляются совершенно новые виды угроз, которые ставят под сомнение не только финансовую безопасность

каждого конкретного гражданина, но и безопасность функционирования ключевых элементов инфраструктуры государства.

Противодействие преступлениям в данной сфере является основной задачей для БСТМ МВД России по линии «К», а именно: выявление, предупреждение, пресечение и раскрытие преступлений, совершенных непосредственно в информационно-телекоммуникационной сфере, в том числе совершаемых путем вмешательства в функционирование электронных платежных систем дистанционного банковского обслуживания посредством несанкционированного доступа к охраняемой законом компьютерной информации, изготовления или сбыта поддельных банковских карт с использованием специального оборудования (устройств) и (или) вредоносного программного обеспечения.

В информационной и телекоммуникационной сферах меняется качественный состав преступлений. Так, с каждым годом возрастает миграция традиционных форм преступной деятельности в киберпространстве. Все больше краж и мошенничеств совершается с использованием информационных технологий. В 2017 г. они составили 71% от общего числа зарегистрированных преступлений в информационной и телекоммуникационной сфере.

Представляет интерес структура преступлений в информационной и телекоммуникационной сферах.

За этот период не изменились показатели в абсолютных цифрах таких видов преступлений, совершенных с использованием названных технологий, как незаконный оборот специальных технических средств, распространение вредоносных программ, компьютерное пиратство. В то же время уменьшился их удельный вес в общем числе киберпреступлений за счет общего роста числа зарегистрированных преступлений, в основном квалифицированных мошенничеств.

Проблемы противодействия преступлениям в сфере высоких технологий

Практика свидетельствует о том, что одним из основных факторов, негативно влияющих на эффективность раскрытия таких преступлений, выступает межрегиональный характер преступной деятельности, направленной в отношении жителей других регионов, что затрудняет проведение следственных и оперативно-розыскных мероприятий. В частности, период ожидания ответов на все запросы, отправленные для установления цепочки ряда транзакций денежных средств, похищенных в результате мошенничества, превышает разумные сроки проведения предварительного следствия.

Это позволяет преступникам уничтожить следы и легализовать похищенные денежные средства.

Есть проблемы и при квалификации преступлений. Ярким примером может быть хищение денежных средств граждан с их расчетных счетов с использованием вредоносного программного обеспечения, которое квалифицируются в одних случаях как кража по статье 158 УК РФ, а в других – как мошенничество по статье 159.6 УК РФ.

Отмечаются и другие проблемы, лежащие в сфере квалификации. На сегодняшний день в деятельности территориальных органов МВД России сложилась практика, когда местом окончания мошенничества, совершенного с использованием информационных и телекоммуникационных технологий, устанавливается место нахождения потерпевшего, а в других территориальных органах МВД России местом окончания такого мошенничества признается место выполнения виновным объективной стороны преступления. Это приводит к тому, что поступившее заявление без проверки и закрепления доказательств пересылается из органа внутренних дел, принявшего заявление, в орган внутренних дел, где обнаружены технические следы преступления и нахождения преступника. Подобные факты приводят к затягиванию сроков рассмотрения заявления, что в свою очередь влечет утрату следов преступления.

На решения имеющихся процессуальных вопросов повлияло подготовленное Следственным департаментом МВД России и направленное в территориальные органы предварительного следствия указание об исключении фактов неоднократного перенаправления материалов доследственной проверки в порядке статьи 152 УПК РФ и необходимости принятия процессуальных решений о возбуждении уголовных дел по месту поступления заявления о совершенном преступлении.

В качестве главных барьеров на пути реализации успешного судебного преследования выступают следующие факторы:

– значительный объем доказательств;
– короткий период времени, в течение которого поставщики услуг хранят информацию, требующуюся для целей расследования;
– необходимость обеспечения целостности электронных доказательств с момента выемки до момента завершения дела;
– неспособность организовать систему охраны доказательств при их передаче в отсутствие помещений с надлежащими условиями для хранения доказательств;
– возможность предоставления доказательств в суде;
– необеспечение целостности доказательств в результате неправильного обращения с ними сотрудниками правоохранительных органов.

Заключение

Подводя итоги, необходимо сказать, что киберпреступность – это вызов современному обществу, и его надо учитывать в качестве ключевого момента обеспечения безопасности граждан, общества и государства. Вопросы информационной безопасности необходимо рассматривать как ключевые направления не просто развития, они должны найти свое место в рамках любых управленческих процессов в сфере бизнеса, национальной безопасности и государственной службы.

Для обеспечения информационной безопасности требуется системная подготовка сотрудников правоохранительных органов. Необходимо, чтобы каждый сотрудник владел базовыми знаниями в области информационной безопасности, – в этом случае можно будет противодействовать хотя бы самым простым уловкам, которые часто используются злоумышленниками, таким, например, как рассылка вредоносных программ в приложениях к электронным письмам. Одних лишь информационных технологий еще недостаточно. Их роль заключается только в том, чтобы помогать людям в принятии правильных решений и совершении правильных действий.

Информация об авторах

Евгений С. Смольянинов, кандидат юридических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125993, Россия, Москва, Миусская пл., д. 6; Академия управления МВД России, Москва, Россия; 125993, Россия, Москва, ул. Зои и Александра Космодемьянских, д. 8; kimowez@mail.ru

Михаил Ю. Воронин, доктор юридических наук, доцент, Академия управления МВД России, Москва, Россия; 125993, Россия, Москва, ул. Зои и Александра Космодемьянских, д. 8; m.voronin@mail.ru

Information about the authors

Evgeny S. Smolyaninov, LLM, associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Square, Moscow, Russia, 125993; Academy of Management of the Ministry of Internal Affairs of Russia, Moscow, Russia; bld. 8, Zoya i Aleksandr Kosmodem'yanskie Street, Moscow, Russia, 125993; kimowez@mail.ru

Mikhail Yu. Voronin, JD, associate professor, Academy of Management of the Ministry of Internal Affairs of Russia, Moscow, Russia; bld. 8, Zoya i Aleksandr Kosmodem'yanskie Street, Moscow, Russia, 125993; m.voronin@mail.ru