УДК 343.9

К.Н. Евдокимов,
Н.Н. Таскаев

АКТУАЛЬНЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ: УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ

Актуальность данного научного исследования обусловлена тем, что компьютерная преступность наносит колоссальный вред информационной безопасности Российской Федерации, причиняя огромный материальный ущерб российскому обществу.

Целью научной статьи является анализ современных научных подходов по вопросу предупреждения компьютерной преступности в Российской Федерации и выработка эффективного комплекса уголовно-правовых мер для обеспечения информационной безопасности российского государства.

Ключевые слова: информационная безопасность, компьютерная преступность, преступления в сфере компьютерной информации, компьютерные преступления.

Одной из главных проблем современного российского общества и государства является возникновение угрозы их информационной безопасности, а также масштабное распространение компьютерной преступности, причиняющей колоссальный вред существующим экономическим, политическим, культурным, научным, образовательным и иным социальным отношениям в Российской Федерации.

Масштабы ущерба, причиняемого компьютерными преступлениями, впечатляют. Так, по оценкам аналитиков компании Group-IB объем рынка киберпреступности в РФ в 2012 году составил 1,93 млрд дол. [6], а с середины 2013 по середину 2014 года в России и СНГ русскоговорящие хакеры «заработали» 2,5 млрд дол., что составляет 2 % от глобального рынка [4].

В свою очередь, американская корпорация Symantec оценила ущерб от киберпреступности в России за 2013 год в 1 млрд дол., а в 2012 году в 1,48 млрд дол.

При этом общий ущерб от киберпреступности в мире в 2013 году составил 113 млрд дол. [2].

По данным исследования 2014 Cost of Cyber Crime Study, проведенного компанией Ponemon Institute при поддержке HP Enterprise Security, среднегодовой ущерб российской организации от киберпреступлений в 2014 году достигает 3,3 млн дол. [9].

Между тем, эксперты «Лаборатории Касперского» проанализировав в 2015 году ущерб от деятельности киберпреступников на российском рынке, пришли к выводу, что в случае успешной атаки крупные компании теряют около 20 млн р., а предприятия среднего и малого бизнеса в среднем 780 тыс. р. – за счет вынужденного простоя, упущенной прибыли и расходов на дополнительные услуги специалистов. На ликвидацию последствий инцидента и профилактику крупные компании дополнительно тратят около 2,1 млн р., а небольшие – около 300 тыс. р. [3].

В связи с этим все более актуальным становится вопрос о защите физических и юридических лиц от неправомерного доступа к компьютерной информации, вредоносных компьютерных программ, кибершпионажа, DDoS-атак и иных компьютерных угроз.

С учетом вышесказанного, авторы предлагают комплекс мер криминологического, уголовно-правового и криминалистического характера, направленного на совершенствование информационной безопасности Российской Федерации.

К *специальным правовым мерам* следует отнести:

1. Совершенствование действующего уголовного законодательства.

Например, законодательное закрепление ряда юридических понятий, содержащихся в диспозициях ст. 272–274 УК РФ, а именно: «компьютерная программа», «несанкционированное уничтожение, блокирование, модификация, копирование компьютерной информации», «нейтрализация средств защиты компьютерной информации», «средства хранения, обработки или передачи охраняемой компьютерной информации». Поскольку указанные юридические термины законодательно нигде не определены, а разъяснения пленума Верховного Суда РФ на данный счет отсутствуют.

Дополнить главу № 28 УК РФ новыми составами преступлений, например, ст. 272.1: «Незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации».

Данная авторская позиция обусловлена тем, что преступник тайно, открыто или обманным путем завладев, например, флэш-картой или DVD-диском с компьютерной информацией для последующего ее использования, избегает уголовной ответственности по ст. 158, 159, 161 УК РФ в связи с малозначительностью совершенного деяния, т.к. стоимость вышеуказанных носителей информации не превышает тысячи рублей. При этом виновное

лицо получает доступ к компьютерной информации, которая представляет большую ценность для ее владельца, чем сам материальный носитель информации, тем самым причиняя потерпевшему более существенный вред.

Кроме того, представляется целесообразным, введение уголовной ответственности за создание, использование и распространение «ботнетов», т.е. сети компьютеров или компьютерных устройств, зараженных вредоносной программой, позволяющей удаленно управлять инфицированными машинами без ведома их (владельца) пользователя, использовать ресурсы зараженных компьютерных средств в преступных целях (рассылки спама, анонимного доступа в Интернет, совершения Ddos-атак, фишинга, кибершантажа, компьютерного мошенничества, сбыта наркотических средств, распространения детской порнографии и иных преступных деяний, а также сокрытия следов преступной деятельности), дополнив уголовное законодательство ст. 273.1 УК РФ.

Кроме того, для более эффективного противодействия преступлениям в сфере компьютерной информации авторы предлагают дополнить диспозиции ч. 3 ст. 272, ч. 2 ст. 273, ч. 1 ст. 274 УК РФ новым квалифицирующим признаком:

«Те же деяния, совершенные с целью устрашения населения или воздействия на принятие решения органами государственной власти и (или) местного самоуправления, а также воспрепятствования нормальной деятельности средств массовой информации, органов государственной власти и местного самоуправления, государственных и муниципальных учреждений, предприятий».

При этом установив санкцию за указанное деяния до 10 лет лишения свободы.

Полагаем возможным также внести изменения в ст. 151 УПК РФ и отнесения преступлений, предусмотренных ч. 4 ст. 272, ч. 3 ст. 273, ч. 2 ст. 274 УК РФ к подследственности органов ФСБ РФ, поскольку вышеуказанные преступные деяния, безусловно, представляют угрозу национальной безопасности Российской Федерации [7, с. 46–47].

2. Совершенствование судебной практики по уголовным делам о компьютерных преступлениях в Российской Федерации.

В настоящее время, до сих пор отсутствуют разъяснения пленума Верховного суда РФ о практике рассмотрения судами уголовных дел по преступлениям в сфере компьютерной информации, что негативно сказывается на следственно-судебной практике и единообразии применения уголовно-правовых норм правоохранительными органами.

Кроме того, в подавляющем большинстве случаев, суды при вынесении обвинительных приговоров, назначают компьютерным преступникам

наказания не связанные с лишением свободы (штраф, условное наказание, ограничение свободы и др.), обосновывая свое решение тем, что данные преступления относятся к деяниям небольшой и средней тяжести.

По мнению авторов, недостаточная жесткость наказания к лицам, ранее судимым и продолжающим совершать компьютерные преступления, безусловно, будет способствовать рецидиву со стороны данной категории преступников.

Таким образом, совершенствование судебной практики требует разъяснений пленума Верховного Суда РФ по вопросам квалификации деяний, предусмотренных ст. 272–274 УК РФ.

3. Активизация и совершенствование международно-правового сотрудничества в сфере предупреждения и борьбы с компьютерными преступлениями.

Учитывая транснациональный и трансграничный характер рассматриваемых преступлений, большое значение приобретает вопрос взаимодействия правоохранительных органов России и зарубежных стран в сфере противодействия компьютерной преступности.

Между тем, Россия до сих пор не ратифицировала Конвенцию Совета Европы о киберпреступности [1], участниками которой являются 47 государств. Официальная причина – отсутствие в УК РФ правовой нормы, предусматривающих уголовную ответственность юридических лиц за преступления в сфере компьютерной информации.

Данное обстоятельство, несомненно, препятствует эффективной борьбе с международными преступными группами, совершающими компьютерные преступления на территории Российской Федерации и полноценному международному сотрудничеству в сфере информационной безопасности.

Однако следует отметить, что Россия недавно выступила в Организации Объединенных Наций с инициативой принятия специальной Конвенции ООН «Об обеспечении международной информационной безопасности», считая, что назрела потребность в разработке и принятии универсальной международной конвенции по борьбе с киберпреступностью, содержащей принципы поведения государств в мировом информационном пространстве. К сожалению, подготовленный Советом безопасности и МИД РФ проект конвенции ООН «Об обеспечении международной информационной безопасности» [2] был отклонен в Совбезе ООН.

4. Совершенствование информационного законодательства РФ.

Авторы полагают возможным принятие федерального закона о страховании информационных рисков, который бы закреплял страхование охраняемой законом компьютерной информации, а также средств ее хранения, обработки и передачи, информационно-телекоммуникационных

сетей и оконечного оборудования от несанкционированного уничтожения, блокирования, модификации либо копирования.

При этом перед заключением страхового договора, обязать собственника (владельца) компьютерной информации или средств хранения, обработки, передачи охраняемой компьютерной информации, информационно-телекоммуникационных сетей и оконечного оборудования установить необходимое программное обеспечение по антивирусной защите компьютерной информации и фиксации (предупреждении) о несанкционированном доступе. Эта мера позволит уменьшить наносимый материальный ущерб и снизить количество несанкционированных проникновений в компьютерные системы, происходящих по вине потерпевших.

Кроме того, полагаем необходимым, для предупреждения совершения компьютерных преступлений в сети «Интернет», в федеральном законе от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» закрепить юридическую обязанность для пользователей информационно-телекоммуникационных сетей, в том числе сети «Интернет», при регистрации сайтов, веб-страниц, получении аккаунтов в социальных сетях указывать свои персональные данные (Ф. И. О., год рождения, данные паспорта) [5, с. 25–26].

Опыт Китайской Народной Республики, где официальная персонализация интернет-пользователей была введена в 2010 году, показал, что данная мера значительно снизила количество компьютерных преступлений, совершенных в сети «Интернет».

В качестве *специальных духовно-культурных (идеологических) мер* противодействия компьютерным преступлениям предлагается:

1. *Активизировать деятельность средств массовой информации в предупреждении компьютерных преступлений.*

С учетом того, что большинство компьютерных специалистов использует Интернет для чтения новостей (около 64 %) и получения деловой информации (около 76 %), то в этом случае было бы логично вести профилактическую работу посредством сети «Интернет» через электронные мультимедиа [4, с. 213].

2. *Правовое воспитание молодежи.*

По мнению авторов, проводя правовую пропаганду и правовое просвещение среди учащихся и студентов технических образовательных учреждений, будущих программистов, сетевых администраторов и специалистов в области защиты информации, информируя их о действующем уголовном законодательстве и ответственности за указанные противоправные деяния, можно снизить риск появления компьютерных преступников в среде

технических специалистов. Поскольку, как показывает практика, достаточное большое количество «хакеров» появляется в молодежной среде технического «андеграунда».

В качестве аргумента в поддержку эффективности этой меры, можно привести воспоминания Е.В. Касперского, который писал: «Однажды, где-то в конце 1990-х годов, нам удалось узнать домашний адрес одного вирусописателя из Москвы, весьма активного в то время. На этот адрес была отправлена посылка – с книгой о компьютерных вирусах и ксерокопией «компьютерных» статей из Уголовного кодекса РФ. Через несколько дней в Сети появилось его письмо, в котором он сообщил, что прекращает разрабатывать новые компьютерные вирусы» [8, с. 16].

К *специальным организационно-управленческим и техническим мерам* полагаем отнести следующее:

1. *Подготовку специалистов по специальностям «Информационная безопасность», «Защита информации и информационно-телекоммуникационных сетей»* в высших учебных заведениях МВД, ФСБ, МО, ФТС РФ и др., с целью дальнейшего комплектования правоохранительных органов профессиональными и компетентными сотрудниками.

При этом следует также осуществлять повышение квалификации профессорско-преподавательского состава вышеуказанных вузов, включая проведение стажировок, обмена опытом, мастер-классов, семинаров в соответствующих образовательных учреждениях за рубежом, а также в российских и иностранных компаниях занимающихся информационной безопасностью, защитой информации, разработкой антивирусного программного обеспечения и т.п.

2. *Создание в технических ВУЗах, а также НИИ МВД, ФСБ, МО, ФТС РФ научно-исследовательских лабораторий по созданию и модификации программных систем компьютерной защиты*, с правом реализации (продажи) своей продукции заинтересованным физическим и юридическим лицам. Работа в лабораториях должна проводиться как в научных, так и в коммерческих целях на договорной основе, в том числе для государственных и муниципальных нужд.

3. *При технических образовательных учреждениях, специализирующихся на подготовке специалистов по информационной безопасности, создать курсы обучения и повышения квалификации для сотрудников служб безопасности банков, предприятий, учреждений, либо заинтересованных компьютерных пользователей.*

4. *В трудовых договорах (контрактах) лиц, работающих или имеющих доступ к корпоративной компьютерной системе или*

информационнотелекоммуникационной сети предусмотреть положение о персональной ответственности данных лиц за разглашение конфиденциальных сведений о системе защиты служебной компьютерной сети или передачи служебных паролей и логинов третьим лицам (уголовной или иной юридической ответственности, в зависимости от тяжести наступивших последствий или угрозы их наступления).

5. С целью совершенствования систем защиты компьютерной информации в государственных и муниципальных организациях, *возложить на руководителей или иных уполномоченных лиц персональную обязанность – осуществлять контроль за установкой и постоянным обновлением антивирусного программного обеспечения, а также иных систем компьютерной защиты*.

6. *Тесное взаимодействие органов прокуратуры, органов внутренних дел (отделов «К»), органов федеральной службы безопасности со средствами массовой информации при предупреждении и раскрытии преступлений в сфере компьютерной информации*. Анализ правоприменительной практики показывает эффективность такого взаимодействия, тем более, что основные формы сотрудничества правоохранительных органов и средств массовой информации давно уже апробированы, и активно используются.

7. *Создание в Российской Федерации национальной операционной системы для компьютерных устройств, а также общенациональной компьютерной системы по фиксации, анализу и учету преступлений в сфере компьютерной информации и компьютерных преступников* (Разработку таких систем можно поручить российским компаниям: «Лаборатория Касперского», «Dr.Web», «Group-IB»).

К *криминалистическим мерам* обеспечения информационной безопасности отнести:

1. Совершенствование уголовно-процессуального законодательства.

Внести изменения в ст. 176, 177 УПК РФ, определив, что осмотр места происшествия, местности, жилища, иного помещения, предметов и документов в целях обнаружения следов компьютерного преступления, выяснения других обстоятельств, имеющих значение для уголовного дела, обязательно проводится только с участием эксперта.

2. Создание новых и совершенствование существующих методик выявления компьютерных преступлений с привлечением специалистов в области информационной безопасности (например, вышеуказанных специалистов компаний «Лаборатория Касперского», «Dr.Web», «Group-IB»).

3. Обобщение и анализ юридической практики Прокуратурой РФ, СК РФ, МВД РФ, ФСБ РФ, МО РФ для дальнейшей выработки методических

рекомендаций по вопросам раскрытия и расследования компьютерных преступлений.

4. Создание во всех экспертно-криминалистических центрах МВД, ГУВД, ОВД отделов компьютерных экспертиз и технологий, для производства необходимых судебно-компьютерных экспертиз, выдачи заключений и справок заинтересованным лицам.

5. Совершенствование подготовки экспертов-криминалистов, осуществляющих судебно-компьютерные экспертизы, на базе единого учебного центра.

В данное время системная подготовка экспертов-криминалистов и повышение их квалификации при проведении судебно-компьютерных экспертиз в системе МВД России не проводится. Поэтому возникает необходимость создания единого учебного центра на базе ЭКЦ МВД РФ, либо одного из образовательных учреждений МВД России, имеющих необходимый опыт обучения экспертов-криминалистов (например, Волгоградская Академия МВД России или Омская Академия МВД России).

Перечень мер по обеспечению информационной безопасности может быть продолжен. Однако, вне всякого сомнения, только интегративный и комплексный подходы в деятельности правоохранительных органов могут повысить уровень информационной безопасности России и сделать предупреждение компьютерных преступлений более эффективным. При этом не стоит забывать, что предложенные превентивные меры дадут ощутимый результат только в случае совместных действий государства с институтами гражданского общества (органами местного самоуправления, образовательными и научными учреждениями, средствами массовой информации, общественными объединениями и т.д.).

Список использованной литературы

1. Конвенция о преступности в сфере компьютерной информации (ETS № 185) [рус., англ.] : заключена в г. Будапеште 23.11.2001 г. // Собрание законодательства Российской Федерации. – 2005. – № 47. – Ст. 4929.

2. Конвенция об обеспечении международной информационной безопасности (концепция) [Электронный ресурс] // Совет безопасности РФ. – М., 2016. – Режим доступа: http://www.scrf.gov.ru/documents/6/112.html.

3. Газета.ру [Электронный ресурс]. – Режим доступа: http://www.gazeta.ru/ tech/2014/11/05a6289085.shtml.

4. Дремлюга Р.И. Интернет-преступность : монография / Р.И. Дремлюга. – Владивосток : Изд-во Дальневост. ун-та, 2008. – 240 с.

5. Евдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации /

К.Н. Евдокимов // Академический юридический журнал. – 2015. – № 1. – С. 25–26.

6. Евдокимов К.Н. Основные причины компьютерной преступности в современной России [Электронный ресурс] / К.Н. Евдокимов. – Режим доступа: http://digit.ru/business/20130910/405335397.html#ixzz2r1xUjpbf.

7. Евдокимов К.Н. Политические факторы компьютерной преступности в России / К.Н. Евдокимов // Информационное право. – 2015. – № 1. – С. 41–47.

8. Касперский Е.В. Компьютерное зловредство (+CD) / Е.В. Касперский. – СПб. : Питер, 2009. – 207 с.

9. Global Report on the Cost of Cyber Crime 2014 [Электронный ресурс] : Research Report / Ponemon institute. – Режим доступа: http://www.octree.co.uk/ Documents/2014-Global-Report-on-the-Cost-of-Cybercrime.pdf.

10. Group-IB [Электронный ресурс] : междунар компания по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий. – Режим доступа: http://www.group-ib.ru/index.php/investigation/1063-link-nezavisimye.

11. Norton Security Deluxe [Электронный ресурс] (первоклассная антивирусная защита) : офиц. сайт. – М., 2016. – Режим доступа: http://go.symantec.com/ norton-report-2013.

Сведения об авторах

Евдокимов Константин Николаевич – доцент кафедры государственноправовых дисциплин Иркутского юридического института (филиала) Академии Генеральной прокуратуры РФ, кандидат юридических наук, доцент, г. Иркутск, Российская Федерация; e-mail: kons-evdokimov@yandex.ru.

Таскаев Николай Николаевич – доцент кафедры конституционного и административного права Байкальского государственного университета, кандидат юридических наук, доцент, г. Иркутск, Российская Федерация; e-mail: ktig@isea.ru.

Authors

Evdokimov Konstantin Nikolaevich – Associate Professor of the Chair of State and Law Disciplines of the Irkutsk Law Institute Affiliated with the Academy of the General Prosecutor's Office of the Russian Federation, PhD in Law, Associate Professor, Irkutsk, the Russian Federation; e-mail: kons-evdokimov@yandex.ru.

Taskaev Nikolai Nikolayevich – Associate professor of the Chair of Constitutional and Administrative Law, Baikal National University, PhD

in Law, Associate Professor, Irkutsk, the Russian Federation; e-mail: ktig@isea.ru.