Parhomenko S.V., Evdokimov, K.N.♦

Prevention of cybercrime in the Russian Federation: an integrative and comprehensive approaches

Abstract: The relevance of this research due to the fact that cybercrime is detrimental to the political, economic, social and information relations in the Russian Federation, causing enormous material damage. The purpose of a scientific article is the analysis of modern scientific approaches to the prevention of cybercrime in the Russian Federation and the production of an effective set of preventive measures to counter cybercrime. According to the authors, the purpose of the prevention of cybercrime acts as security in the Russian Federation, the necessary conditions for secure creation, processing and dissemination of computer information, as well as the normal functioning of computer devices and information and telecommunication networks. Subject to the methodological approach of criminological science, the authors highlighted the measures of General prevention and special preventive measures of cybercrime. To special measures to prevent cybercrimes proposed include: improvement of the existing criminal law, criminal procedure and information legislation; improvement of the judicial practice; training in educational establishments of the required number of specialists in the sphere of information security; the establishment in Universities and research institutes research laboratories on the development of hardware and software systems computer security; consolidation in the employment contracts (contracts) provisions on the criminal liability of persons for the disclosure of sensitive information about the system of protection of proprietary information; continuous monitoring of managers for the installation and upgrading of computer security in state and municipal organizations; the creation in Russia of a national operating system for computing devices and systems for fixation, identification of crimes in the sphere of computer information and computer criminals; the creation of new and improvement of existing methods of detecting cybercrimes involving experts in the field of information security. The list of measures for the prevention of cybercrime can be extended, but, no doubt, only an integrative and comprehensive approaches in the application of law

♦ **Parhomenko Svetlana V.** - Doctor of Law, Professor, Professor of the Chair of Criminal and Law Disciplines of the Irkutsk Institute of Law (branch) of Academy of the Prosecutor General's Office of the Russian Federation, Irkutsk, Russian Federation; e-mail: psvet@mail.ru.

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

enforcement preventive measures to improve the level of information security of Russia and the efficiency of prevention of cybercrimes.

Keywords: computer crime; cybercrime; Internet crime; crimes in the sphere of computer information; cybercrimes.

Одной из социальных проблем в современном российском обществе является возникновение и активное развитие компьютерной преступности, причиняющей колоссальный вред экономической, политической, культурной, научной, образовательной и информационной сферам Российской Федерации.

Все более актуальным становится вопрос о защите граждан, муниципальных и государственных учреждений, предприятий, органов власти от несанкционированного доступа к компьютерной информации, вредоносных компьютерных программ и иных компьютерных угроз.

Масштабы ущерба, причиняемого компьютерными преступлениями, впечатляют. Так, по оценкам аналитиков компании Group-IB, объем рынка киберпреступности в РФ в 2012 г. составил 1,93 млрд. дол. [26], а с середины 2013 по середину 2014 г. в России и СНГ русскоговорящие хакеры «заработали» 2,5 млрд. дол., что составляет 2 % от глобального рынка [28].

В свою очередь, американская корпорация Symantec оценила ущерб от киберпреступности в России в 2013 г. в 1 млрд. дол., в 2012 г. — в 1,48 млрд. дол. При этом общий ущерб от киберпреступности в мире в 2013 г. составил 113 млрд. дол. [27].

По данным исследования 2014 Cost of Cyber Crime Study, проведенного компанией Ponemon Institute при поддержке HP Enterprise Security, среднегодовой ущерб российских организаций от киберпреступлений в 2014 г. достигает 3,3 млн. дол. [30]. По данным «Лаборатории Касперского», в мире ежедневно появляется до 70 тыс. вредоносных программ. При этом за последний год в 96 % российских компаний фиксировались инциденты в области IT-безопасности. Больше половины опрошенных специалистов признали факт потери данных в результате заражения компьютеров вредоносным программным обеспечением. При этом чаще всего инциденты в области IT-безопасности приводят к потере данных о платежах (13 %), интеллектуальной собственности (13 %), клиентских баз (12 %) и информации о сотрудниках (12 %) [29].

Поэтому в настоящее время профилактика компьютерных преступлений является одним из главных направлений деятельности правоохранительных органов по обеспечению информационной безопасности российского общества.

Проведенный анализ специальной и научной литературы показывает, что вопросам уголовно-правовой защиты компьютерной информации и противодействия компьютерным преступлениям в Российской Федерации уделяется пристальное внимание как со стороны государства, так и со стороны научного сообщества [6; 14; 15].

По мнению авторов, целью предупреждения компьютерной преступности выступает обеспечение в Российской Федерации необходимых условий для безопасного создания, обработки и распространения компьютерной информации, а также нормального функционирования компьютерных устройств и информационно-телекоммуникационных сетей. В свою очередь, мы полагаем, что к основным задачам превенции данного вида преступности относится выработка и реализация комплекса мер, направленных на предотвращение:

– преступных посягательств на основы конституционного строя, общественную безопасность и общественный порядок в РФ;

– угроз информационной безопасности личности, общества, государства, т.е. обеспечение возможности безопасного создания, хранения, обработки и передачи вышеуказанными субъектами права не запрещенной законом компьютерной информации;

– несанкционированных действий, направленных на уничтожение, блокирование, модификацию, копирование компьютерной информации или нейтрализацию средств защиты компьютерной информации физических и юридических лиц, либо угрозы причинения указанных последствий;

– противоправных действий, направленных на нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям;

– угроз информационной безопасности коммерческих и некоммерческих организаций, государственных (муниципальных) органов власти, предприятий и учреждений, связанных с обеспечением режима тайны конфиденциальной информации (персональных данных и информации частного характера, сведений, представляющих государственную, служебную, профессиональную, коммерческую и иную тайну);

– несанкционированных действий, направленных на нарушение работы средств защиты, хранения, обработки и передачи компьютерной информации на военных, стратегических и социально значимых объектах (транспортных, промышленных, энергетических, научных, здравоохранительных, образовательных и т.д.);

– нарушения конституционных прав граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом, неприкосновенность частной жизни, личной и семейной тайны, собственности и др. [3].

Содержание указанных задач, по нашему мнению, позволит определить круг мер общего и специального характера, направленных на предупреждение компьютерных преступлений.

Анализ научной литературы позволяет выделить следующие подходы к освещению данной проблематики. Так, В.Б. Вехов и В.Е. Козлов в своих работах указывают три основные группы мер предупреждения компьютерных преступлений, а именно правовые, организационно- технические и криминалистические [1; 8].

Близкой точки зрения придерживается Е.А. Маслакова, по мнению которой можно выделить три группы мер предупреждения указанных преступных деяний, составляющих в своей совокупности целостную систему борьбы с этим социально опасным явлением, а именно правовые, организационные и технические [12, с. 141].

В свою очередь, М.М. Малыковцев называет меры законодательного, технического и правоприменительного характера, направленные на предупреждение компьютерных преступлений [11, с. 157].

С позиции Т.М. Лопатиной, система мер предупреждения компьютерных преступлений должна быть комплексной и включать в себя, с одной стороны, организационно-управленческие, технические (физические) меры, с другой — кадровые (в сочетании с морально-этическими) и правовые [10, с. 316].

Не подвергая сомнению приведенные позиции, можно согласиться с точкой зрения Т.М. Лопатиной, согласно которой система профилактических мер, направленных на предупреждение компьютерных преступлений, должна носить комплексный и многосторонний характер. Между тем, учитывая методологический подход криминологической науки, мы выделяем меры общей превенции (например, политические, экономические, социальные, научно-технические, духовно-культурные) и специальные превентивные меры (правовые, духовно-культурные, организационно-управленческие, технические, криминалистические и др.).

Общепревентивные меры предупреждения компьютерных преступлений носят всеобщий характер и направлены на профилактику как компьютерной преступности в частности, так и преступности в целом. Достаточно ясно и лаконично, на наш взгляд, они сформулированы в указе Президента РФ «О Стратегии национальной безопасности Российской Федерации до 2020 года» от 12 мая 2009 г. № 537 [16].

Например, к общеполитическим мерам предупреждения преступлений в сфере компьютерной информации в России можно отнести: развитие демократии и гражданского общества, обеспечение незыблемости конституционного строя, территориальной целостности и суверенитета Российской Федерации; превращение Российской Федерации в мировую державу, деятельность которой направлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях многополярного мира.

Общеэкономические превентивные меры включают: повышение конкурентоспособности национальной экономики; экономический рост, который достигается прежде всего путем развития национальной инновационной системы и увеличения инвестиций в человеческий капитал; повышение производительности труда и др.

Общие социальные меры предполагают: снижение уровня социального и имущественного неравенства населения, стабилизацию его численности в среднесрочной перспективе, а в долгосрочной перспективе — коренное улучшение демографической ситуации; обеспечение личной безопасности, а также доступности комфортного жилья, высококачественных и безопасных товаров и услуг, достойной оплаты активной трудовой деятельности и т.д.

К научно-техническим общепревентивным мерам относятся: формирование системы целевых фундаментальных и прикладных исследований и ее государственной поддержки в интересах организационно-научного обеспечения достижения стратегических национальных приоритетов; создание сети федеральных университетов, национальных исследовательских университетов, обеспечивающих в рамках кооперационных связей подготовку специалистов для работы в сфере науки и образования, разработки конкурентоспособных технологий и образцов наукоемкой продукции, организации наукоемкого производства и др.

Духовно-культурные меры общей превенции включают: признание первостепенной роли культуры для возрождения и сохранения культурно-нравственных ценностей, укрепления духовного единства многонационального народа Российской Федерации и международного имиджа России в качестве страны с богатейшей традиционной и динамично развивающейся современной культурой, создание системы духовного и патриотического воспитания граждан России [16].

Однако представляется необходимым остановиться именно на специальных мерах предупреждения компьютерной преступности (правовых, духовно-культурных, организационно-управленческих, технических и криминалистических).

К специальным правовым мерам предупреждения компьютерных преступлений можно отнести следующие:

1. Совершенствование действующего уголовного законодательства. Например, необходимо 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.

Следует дополнить гл. 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, так как стоимость вышеуказанных носителей информации не превышает 1 тыс. р. При этом виновное лицо получает доступ к компьютерной информации, которая представляет для ее владельца бóльшую ценность, чем сам материальный носитель информации, тем самым потерпевшему причиняется 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).

Кроме того, для более эффективного противодействия преступлениям в сфере компьютерной информации ряд авторов предлагают дополнить диспозиции ч. 3 ст. 272, ч. 2 ст. 273, ч. 1 ст. 274 УК РФ новыми квалифицирующими признаками:

1. «Те же деяния, совершенные с целью скрыть другое преступление или облегчить его совершение».

2. «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» [11, с. 115-116].

При этом рекомендуется установить санкцию за указанные деяния до десяти лет лишения свободы.

Данная позиция обусловлена тем, что преступления в сфере компьютерной информации часто выступают или могут стать способом совершения множества других тяжких и особо тяжких преступных деяний (убийства, причинения тяжкого вреда здоровью, умышленного уничтожения или повреждения имущества, вымогательства, шпионажа, государственной измены и т.д.).

При этом полагаем возможным внести изменения в ст. 151 УПК РФ в плане отнесения преступлений, предусмотренных ч. 2-4 ст. 272, ч. 2, 3 ст. 273, ч. 1, 2 ст. 274 УК РФ к подследственности органов ФСБ РФ, поскольку вышеуказанные преступные деяния, безусловно, представляют угрозу национальной безопасности Российской Федерации [4, с. 46-47].

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

Например, 29 сентября 2014 г. Октябрьский районный суд г. Уфы Республики Башкортостан рассмотрел уголовное дело по обвинению И. и С. в совершении преступления, предусмотренного ч. 3 ст. 272 УК РФ, т.е. в осуществлении неправомерного доступа к охраняемой законом компьютерной информации, повлекшего копирование этой информации, совершенного из корыстной заинтересованности группой лиц по предварительному сговору.

В ходе судебного рассмотрения дела было установлено, что И. и С. приобрели у не установленного следствием лица два комплекта электронных устройств, имитирующих функциональные детали терминалов дистанционного банковского обслуживания (банкоматов). При этом одно из электронных устройств выполнено в виде панели картоприемника банкомата и предназначено для скрытого получения информации, содержащейся на магнитной полосе банковских карт, а другое электронное устройство выполнено в виде лицевой панели банкомата и предназначено для скрытой видеофиксации ввода PIN-кодов законными держателями банковских карт (скиммеры). После чего преступники установили скиммеры на банкомат, находившийся в одном из башкирских отделений ОАО «Сбербанк России». Через установленные И. и С. скиммеры в виде панели картоприемника банкомата были проведены банковские карты, эмитированные ОАО «Сбербанк России», в результате чего содержащаяся на магнитной полосе банковских карт компьютерная информация, вопреки воле их законных владельцев и ОАО «Сбербанк России», была негласно скопирована в память скиммеров.

В период с 00:28 по 00:45 И. и С. произвели демонтаж установленных ими на банкомат скиммеров, намереваясь расшифровать полученную незаконным способом информацию и использовать ее с целью хищения денежных средств в свою пользу.

В тот же день преступная деятельность И. и С. была пресечена сотрудниками УФСБ России по Республике Башкортостан, а скиммеры с незаконно скопированной компьютерной информацией у них изъяты в ходе оперативно-розыскных мероприятий.

Суд признал И. и С. виновными в совершении преступления, предусмотренного ч. 3 ст. 272 УК РФ, и назначил каждому наказание в виде штрафа в доход государства в размере 25 тыс. р. [21].

Кроме того, суды нередко назначают компьютерным преступникам, ранее судимым за совершение уголовных преступлений, наказание, не связанное с лишением свободы.

Например, 17 февраля 2014 г. Кронштадтский районный суд г. Санкт-Петербурга рассмотрел уголовное дело И., ранее судимого по ч. 1 ст. 322.1 УК РФ, обвиняемого в совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ, а именно в распространении вредоносных компьютерных программ либо иной компьютерной информации, заведомо предназначенной для нейтрализации средств защиты компьютерной информации.

Приговором суда И. было назначено наказание в виде двух лет лишения свободы условно с испытательным сроком в два года со штрафом в доход государства [17].

12 апреля 2011 г. Ленинский районный суд г. Нижнего Тагила приговорил И. к одному году лишения свободы условно с испытательным сроком два года и взысканию с осужденного компенсации за нарушение авторских прав в пользу корпорации «Майкрософт» в размере 38 906 р. 82 к., компании Adobe System - 62 447 р. 62 к. за совершение преступлений, предусмотренных ч. 2 ст. 146, ч. 1 ст. 272, ч. 1 ст. 273 УК РФ. При этом И. был ранее осужден: 9 апреля 2002 г. - по ч. 3 ст. 147, п.п. «а», «б» ч. 3 ст. 159, ч. 3 ст. 69 УК РФ к пяти годам трем месяцам лишения свободы; 13 июня 2002 г. - по ч. 1 ст. 228, ч. 5 ст. 69 УК РФ к пяти годам шести месяцам лишения свободы, постановлением Ленинского районного суда г. Нижнего Тагила от 18 марта 2005 г. освобожден условно-досрочно 29 марта 2005 г. на 2 года 18 дней [18].

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

Кроме того, совершенствование судебной практики требует разъяснений Пленума Верховного Суда РФ по вопросам квалификации деяний, предусмотренных ст. 272-274 УК РФ. Например, будет ли являться уничтожением компьютерной информации деяние, при котором информация была изначально уничтожена, но спустя определенное время частично или полностью восстановлена специалистами? Как квалифицировать уничтожение компьютерной информации сильным электромагнитным или высокочастотным излучением, не повлекшим уничтожение самого носителя информации? Будут ли являться копированием компьютерной информации действия преступника при получении копии документа путем распечатывания информации на принтере, фотографирования или видеосъемки изображения с монитора компьютера?

Наконец, как квалифицировать несанкционированное ознакомление с компьютерной информацией, когда преступник, визуально запомнив конфиденциальные сведения (например, персональные данные лица, информацию о содержании коммерческой сделки и сторонах договора, сведения об усыновлении (удочерении), врачебную тайну и т.д.), впоследствии переносит их на другой материальный носитель информации, создав ее копию (написав на листе бумаги, введя информацию в память своего компьютера или иного компьютерного устройства - айфона, смартфона, планшетного компьютера, коммуникатора и т.п.).

3. Активизация и совершенствование международно-правового сотрудничества в сфере предупреждения компьютерных преступлений и борьбы с ними. Учитывая транснациональный и трансграничный характер

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

Так, 11 ноября 2013 г. Тушинским районным судом г. Москвы за совершение преступлений, предусмотренных ч. 3 ст. 30, п. «б» ч. 4 ст. 158, ч. 3 ст. 272 УК РФ, граждане Республики Молдова Б. и А. были осуждены к наказанию в виде двух лет шести месяцев лишения свободы без штрафа и без ограничения свободы с отбыванием наказания в исправительной колонии общего режима каждый. Преступная группа, состоявшая из граждан Республики Молдова, длительное время занималась скиммингом в Москве, осуществляя хищение денежных средств с банковских карт физических лиц с помощью специального оборудования, устанавливаемого на картоприемник банкомата.

Несколько участников преступной группы скрылись от следствия и суда за пределами Российской Федерации [20].

В 2014 г. Псковским городским судом Псковской области за совершение преступлений, предусмотренных ч. 3 ст. 183, ч. 3 ст. 272, ч. 2 ст. 273 УК РФ, был осужден Б., гражданин Республики Молдова. Приговором суда ему назначено наказание в виде 11 месяцев лишения свободы в колонии-поселении со штрафом в размере 100 тыс. р. без лишения права занимать определенные должности или заниматься определенной деятельностью. Однако остальные три члена преступной группы, граждане Республики Молдова, занимавшиеся скиммингом в Пскове, скрылись от следствия и суда, предположительно на территории Молдовы или Румынии [19].

Между тем Россия до сих пор не ратифицировала Конвенцию Совета Европы о киберпреступности, участниками которой являются 47 государств [9]. Официальная причина - отсутствие в УК РФ правовой нормы, предусматривающей 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 о 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» был отклонен в Совбезе ООН [31].

4. Совершенствование информационного законодательства РФ. Авторы полагают возможным принятие федерального закона о страховании информационных рисков, который бы закреплял страхование 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 следует 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) несанкционированного доступа. Эта мера позволит уменьшить наносимый материальный ущерб и снизить количество несанкционированных проникновений в компьютерные системы, происходящих по вине потерпевших. Данную меру из 150 проанкетированных сотрудников ОВД Иркутской области поддержали 86,7 % опрошенных [5, с. 141–142].

Кроме того, по мнению авторов, следует законодательно закрепить полномочия правоохранительных органов (Прокуратуры РФ, СК РФ, МВД РФ, ФСБ РФ и др.) по контролю появляющихся в информационно-телекоммуникационных сетях материалов противоправного характера, а в необходимых случаях разрешить им проводить соответствующие надзорные, оперативно-розыскные, следственные мероприятия.

Полагаем необходимым для предупреждения совершения компьютерных преступлений в сети Интернет в Федеральном законе «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ закрепить юридическую обязанность пользователей информационно-телекоммуникационных сетей, в том числе сети Интернет, при регистрации сайтов, вебстраниц, получении аккаунтов в социальных сетях указывать свои персональные данные (Ф.И.О., год рождения, данные паспорта) [3].

Опыт Китайской Народной Республики, где официальная персонализация интернет-пользователей была введена в 2010 г., 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 по предупреждению компьютерных преступлений. Например, можно возложить обязанность на специализированные средства массовой информации (печатные издания, такие как «Хакер», «Компьютерленд», «Компьютерра», «Игромания» и др.; каналы телерадиовещания, на которых идут программы об IT-технологиях, новинках программного обеспечения и пр.) доводить до читателей (зрителей) информацию о привлечении компьютерных преступников к уголовной ответственности с разъяснением правовых положений действующего законодательства, предусматривающего наказание за преступления в сфере компьютерной информации. Данный шаг, несомненно, положительно скажется на профилактике компьютерной преступности.

С учетом того что большинство компьютерных специалистов используют Интернет для чтения новостей (около 64 %) и получения деловой информации (около 76 %), в этом случае было бы логичным вести профилактическую работу посредством сети Интернет через электронные мультимедиа [2, с. 213].

2. Обратить внимание на 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, достаточно 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» [7, с. 16].

К специальным организационно-управленческим и техническим мерам предупреждения компьютерных преступлений можно отнести следующее:

1. Подготовка 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 и 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 в НИИ МВД, ФСБ, МО, ФТС РФ научно-исследовательских лабораторий по разработке 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, следует создать курсы обучения и повышения квалификации для сотрудников служб безопасности банков, предприятий, учреждений либо заинтересованных компьютерных пользователей.

4. В трудовых договорах (контрактах) лиц, работающих в корпоративной компьютерной системе или информационно-телекоммуникационной сети либо имеющих доступ к ней, нужно предусмотреть положение о персональной ответственности данных лиц за разглашение конфиденциальных сведений о системе защиты служебной компьютерной сети или передачу 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 необходимо 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. Требуется 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 фиксации, анализа и учета преступлений в сфере компьютерной информации и компьютерных преступников (разработку таких систем можно поручить российским компаниям: «Лаборатория Касперского», Dr. Web, Group-IB).

К криминалистическим мерам предупреждения преступлений в сфере компьютерной ин формации можно отнести:

1. Совершенствование уголовно-процессуального законодательства. Как уже указывалось выше, надо внести изменения в ст. 151 УПК РФ и отнести преступления, предусмотренные ч. 2-4 ст. 272, ч. 2, 3 ст. 273, ч. 1, 2 ст. 274 УК РФ к подследственности органов ФСБ РФ, так как компьютерные преступления все чаще носят политический характер и угрожают национальной безопасности России.

Кроме того, следует 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 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 [13].

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 осуществляется, 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 предупреждению компьютерной преступности может быть продолжен. Однако, вне всякого сомнения, только интегративный и комплексный подходы в применении правоохранительными органами профилактических мер 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.).

Bibliography

1. Vekhov V.B., Smagorinskii B.P. (ed.). Komp'yuternye prestupleniya: Sposoby sovershеniya i raskrytiya [Cybercrimes: ways of commission and investigation]. Moscow, Pravo i Zakon Publ., 1996. 182 p.

2. Dremlyuga R.I. Internet-prestupnost' [Internet crime]. Vladivostok, Far-Eastern Federal University Publ., 2008. 240 p.

3. Evdokimov K.N. Current issues of computer information crimes in Russian Federation. Akademicheskii yuridicheskii zhurnal = Academical law journal, 2015, no. 1 (59), pp. 21–31. (In Russian).

4. Evdokimov K.N. Political factors of cybercrimes in Russia. Informatsionnoe pravo = Information law, 2015, no. 1, pp. 41–47. (In Russian).

5. Evdokimov K.N. Problemy kvalifikatsii i preduprezhdeniya komp'yuternykh prestuplenii [Cybercrimes classification and prevention problems]. Irkutsk Law Institute Affiliated with the Academy of the General Prosecutor's Office of the Russian Federation, 2009. 171 p.

6. Ephremova M.A. Ugolovnaya otvetstvennost' za prestupleniya, sovershaemye s ispol'zovaniem informatsionno-telekommunikatsionnykh tekhnologii [Criminal responsibility for crimes committed using information telecommunication technology]. Moscow, Yurlitinform Publ., 2015. 200 p.

7. Kasperskii E.V. Komp'yuternoe zlovredstvo [Computer harm]. Saint Petersburg, Piter Publ., 2009. 208 p.

8. Kozlov V.E. Teoriya i praktika bor'by s komp'yuternoi prestupnost'yu [Theory and practice of cybercrimes' fighting]. Moscow, Goryachaya liniya — Telekom Publ., 2002. 336 p.

9. Convention on Cybercrime (ETS N 185): (Budapest, 23 Nov. 2001)). Sobranie zakonodatel'stva Rossiiskoi Federatsii = Collection of the legislation of the Russian Federation, 2005, no. 47, art. 4929. (In Russian).

10. Lopatina T.M. Kriminologicheskie i ugolovno-pravovye osnovy protivodeistviya komp'yuternoi prestupnosti. Doct. Diss. [Criminologial and criminal legal fundamentals of cybercrimes counteraction. Doct. Diss.]. Moscow, 2007. 418 p.

11. Malykovtsev M.M. Ugolovnaya otvetstvennost' za sozdanie, ispol'zovanie i rasprostranenie vredonosnykh programm dlya EVM. Kand. Diss. [Criminal responsibility for development, utilization and distribution of malicious software. Cand. Diss.]. Orel, 2007. 186 p.

12. Maslakova E.A. Nezakonnyi oborot vredonosnykh komp'yuternykh programm: ugolovno-pravovye i kriminologicheskie aspekty. Kand. Diss. [Illegal trafficking of malicious software: criminal legal and criminological aspects. Cand. Diss.]. Orel, 2008. 198 p.

13. Best practices of prosecutorial supervision over execution of laws while investigating cybercrimes: adopted by Prosecutor General of Russian Federation. Available at: http://www.consultant.ru/document/cons_doc_LAW_161817/. (In Russian).

14. Rodivilin I.P. Problems of classification of cybercrimes via external control over bank account and their prevention. Prolog = Journal about Law, 2014, no. 2 (6), pp. 61–64. (In Russian).

15. Stepanov-Egiyants V.G. Problems of delimitation of unlawful access to computer information and associated elements. Pravo i kiberbezopasnost' = Law and cyber security, 2014, no. 2, pp. 27–32. (In Russian).

16. Decree of the President of the Russian Federation № 537 Russian Federation national security strategy till 2020 dated 12 May 2009. Rossiiskaya gazeta = Russian newspaper, 2009, May 19. (In Russian).

17. Criminal case No. 1-26/2014. Arkhiv Kronshtadtskogo raionnogo suda g. Sankt-Peterburg, 2014 [Saint-Petersburg, Kronshtadt district court 2014 archive A]. (In Russian).

18. Criminal case No. 1-3/2011. Arkhiv Leninskogo raionnogo suda g. Nizhnii Tagil, 2012 [Nizhni Tagil, Lenin district court 2012 archive]. (In Russian).

19. Criminal case no. 1-382/2014. Arkhiv Pskovskogo gorodskogo suda Pskovskoi oblasti, 2014 [Pskov oblast, Pskov city court 2014 archive]. (In Russian).

20. Criminal case no. 1-520/2013. Arkhiv Tushinskogo raionnogo suda g. Moskva, 2014 [Moscow, Tushino district court 2014 archive]. (In Russian).

21. Criminal case no. 1-521/2014. Arkhiv Oktyabr'skogo raionnogo suda g. Ufa, 2014 [Ufa, Oktyabrsky district court 2014 archive]. (In Russian)..

22. Broadhurst R. Organizations and Cybercrime: An Analysis of the Nature of Groupsengagedin Cyber Crime [Electronic resource] / Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, Steve Chon // International Journal of Cyber Criminology. 2014. Jan. - June. Vol. 8, iss. 1. Mode of access: http://www.cybercrimejournal.com/#aj.

23. O'Connell M. Cyber Security without Cyber War / M. O'Connell // Journal of Conflict & Security Law. 2012. Vol. 17. P. 187-209.

24. Smith R.G. Cyber Criminals on Trial / Russell G. Smith, Peter Grabosky, Gregor Urbas // International Journal of Law and Information Technology. 2012. Vol. 20. P. 242-245.

25. Yar M. The Novelty of «Cybercrime»: An Assessment in Light of Routine Activity Theory // European Journal of Criminology. 2005. Vol. 2. P. 407-427.

26. Режим доступа: http://digit.ru/business/20130910/405335397.html#ixzz2r1xUjpbf.

27. Режим доступа: http://go.symantec.com/norton-report-2013.

28. Режим доступа: http://www.group-ib.ru/index.php/investigation/1063-link-nezavisimye.

29. Режим доступа: http:// www.kaspersky.ru/downloads/pdf/kaspersky_ security_network.pdf.

30. Режим доступа: http://www.octree.co.uk/Documents/2014-Global-Report-on-the-Cost-of-Cybercrime.pdf.

31. Режим доступа: http://www.scrf.gov.ru/documents/6/112.html.