Константин Евдокимов
(Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ)

Основные причины компьютерной преступности в современной России

Резюме

В наш век технического прогресса, новых технологий и инновационной экономики уже ни у кого не вызывает сомнений необходимость использования электронно-вычислительных машин, компьютерных систем, глобальных информационных сетей в различных сферах политической, социально-экономической, духовно-культурной жизни общества, и в повседневной жизни обычного человека.

Между тем, продолжающее развитие прикладных технических наук, совершенствование компьютерных технологий, глобальных информационных сетей в условиях рыночной экономики обусловили появление нового вида общественно опасного поведения – «компьютерной» преступлений.

В свою очередь, организованный и профессиональный характер современной «компьютерной» преступности, ее мобильный и высоколатентный характер, невозможность вести успешную борьбу с ней в рамках границ отдельного государства обусловливают необходимость осуществления международно-правового сотрудничества и взаимодействия правоохранительных органов разных стран в данной сфере.

Кроме того, общественная опасность компьютерных преступлений в значительной степени возрастает в связи с использованием компьютерных технологий для совершения множества других умышленных преступлений, относящихся к категории тяжких и особо тяжких.

Для решения задач обеспечения информационной безопасности российского общества и государства требуется повышение эффективности уголовного закона, а также практики его применения за преступления в сфере компьютерной информации.

Огромные масштабы причиняемого ущерба и крайне низкие показатели его возмещения свидетельствуют о том, что действующая в России нормативно-правовая база, регламентирующая борьбу с такими преступлениями, требует дальнейшего совершенствования, в том числе на региональном уровне.

В судебно-следственной практике возникают сложности при уголовно-правовой квалификации преступлений, предусмотренных статьями 272, 273, 274 УК РФ, т.к. установление объективных признаков составов преступлений в сфере компьютерной информации предполагает не только уяснение технических особенностей деятельности в сфере высоких технологий и компьютерной информации, но и использование специальных знаний в области устройства компьютера и носителей компьютерной информации. Кроме того, нуждаются в дополнительном уточнении и отдельные субъективные признаки данных составов преступлений.

Поэтому, безусловно, необходима активизация научных разработок уголовно-правовых средств борьбы и комплекса современных криминологических мер предупреждения преступлений рассматриваемого вида.

Данная научная статья посвящена основным причинам компьютерной преступности в Российской Федерации. Автор проводит классификацию и анализ наиболее актуальных причин совершения преступлений в сфере компьютерной информации, предлагает меры по их устранению и делает обобщающие выводы о дальнейшем развитии компьютерной преступности в России.

Ключевые слова: Компьютерная преступность, киберпреступность, преступления в сфере компьютерной информации, причины преступности, вредоносные компьютерные программы

I. Введение

Современный мир характеризуется стремительным развитием информационных отношений, информационно-коммуникационных технологий, киберпространства, компьютерных социальных сетей, тотальной компьютеризацией общества и появлением новых технических средств создания, использования, обработки и распространения цифровой информации.

Век научно-технического прогресса, наукоемких технологий и инноваций доказывает необходимость и эффективность использования компьютеров, информационно-коммуникационных систем, глобальных информационных сетей в различных сферах политической, социально-экономической, духовно-культурной жизни, как всего общества, так и в повседневной жизни обычного человека. Это объективно обусловлено тем, что применение компьютерных и информационно-коммуникационных технологий позволяет органам власти, организациям, учреждениям, предприятиям, общественным объединениям и отдельным гражданам получить доступ к практически неограниченным информационным ресурсам, которые можно использовать в служебной, трудовой, образовательной, научной, культурной и повседневной деятельности, хранить и передавать большие объемы полезной информации.

В соответствии с принятой «Стратегией развития информационного общества в Российской Федерации», утвержденной Президентом РФ 7 февраля 2008 года, в результате реализации ее основных направлений и мероприятий к 2015 году должны быть достигнуты следующие контрольные значения показателей:

- место Российской Федерации в международных рейтингах в области развития информационного общества – в числе двадцати ведущих стран мира;
- место Российской Федерации в международных рейтингах по уровню доступности национальной информационной и телекоммуникационной инфраструктуры для субъектов информационной сферы – не ниже десятого;
- уровень доступности для населения базовых услуг в сфере информационных и телекоммуникационных технологий – 100%;
- доля отечественных товаров и услуг в объеме внутреннего рынка информационных и телекоммуникационных технологий – более 50%;
- рост объема инвестиций в использование информационных и телекоммуникационных технологий в национальной экономике по сравнению с 2007 годом – не менее чем в 2.5 раза;
- сокращение различий между субъектами Российской Федерации по интегральным показателям информационного развития – до 2 раз;
- уровень использования линий широкополосного доступа на 100 человек населения за счет всех технологий: к 2010 году – 15 линий и к 2015 году – 35 линий;
- наличие персональных компьютеров, в том числе подключенных к сети Интернет – не менее чем в 75% домашних хозяйств;
- доля исследований и разработок в сфере информационных и телекоммуникационных технологий в общем объеме научно-исследовательских и опытно-конструкторских работ, осуществляемых за счет всех источников финансирования: к 2010 году – не менее 15% и к 2015 году – 30%;
- рост доли патентов, выданных в сфере информационных и телекоммуникационных технологий, в общем числе патентов: к 2010

году – не менее чем в 1.5 раза и к 2015 году – в 2 раза;

- доля государственных услуг, которые население может получить с использованием информационных и телекоммуникационных технологий, в общем объеме государственных услуг в Российской Федерации – 100%;

- доля электронного документооборота между органами государственной власти в общем объеме документооборота – 70%;

- доля размещенных заказов на поставки товаров, выполнение работ и оказание услуг для государственных и муниципальных нужд самоуправления с использованием электронных торговых площадок в общем объеме размещаемых заказов – 100%;

- доля архивных фондов, включая фонды аудио- и видеоархивов, переведенных в электронную форму – не менее 20%;

- доля библиотечных фондов, переведенных в электронную форму, в общем объеме фондов общедоступных библиотек – не менее 50%, в том числе библиотечных каталогов – 100%;

- доля электронных каталогов в общем объеме каталогов Музейного фонда Российской Федерации – 100%».[1)]

Поэтому персональные компьютеры, ноутбуки, нетбуки, айфоны, айпады и другие информационные устройства прочно вошли в нашу жизнь наряду с телевизором, музыкальным центром, холодильником, автомобилем и другими достижениями научно-технического прогресса.

Однако информационно-коммуникационные технологии – это

1) «Стратегия развития информационного общества в Российской Федерации»(утв. Президентом РФ 07.02.2008 N Пр-212), Российская газета, № 34, 16.02.2008.

своеобразный «ящик Пандоры», который несет обществу не только блага, но и различные проблемы. Расплатой за «технологические блага» является изменение самой социальной культуры людей, мы реже ходим в театры, филармонии, консерватории, библиотеки, музеи, т.к. можем посмотреть, послушать, изучить музыкальные, изобразительные, литературные шедевры через интернет, потратив на это меньше времени и средств. Общение в «социальных сетях», часто заменяет молодежи «живое» общение со сверстниками. Мы становимся все более «интернет»-зависимыми, т.к. не можем спокойно лечь спать, не просмотрев последние новости, новый фильм, саундтрек или электронную почту.

Таким образом, наша социальная культура последние годы трансформируется из «человеческой» культуры в некую «интернеткультуру» или «киберкультуру», которая, по мнению автора, является упрощенным суррогатом человеческой культуры и достижений цивилизации, насчитывающей десятки тысяч лет, давая человеку в основном поверхностное восприятие и знания об окружающем мире, истории, науке, образовании и т.д.

Тем не менее, общество становится «технократичным», а это требует от людей более глубокой специализации, знаний и навыков в области информационных технологий, компьютерной техники, программного обеспечения.

Между тем большинство населения, используя компьютер в личных или служебных целях, имеют слабое представление о программировании и программном обеспечении, средствах антивирусной защиты и ее возможностях.

В связи с чем, все более актуальным становится вопрос о защите компьютерной информации наших граждан, муниципальных и государственных учреждений, предприятий, органов власти от несанкционированного доступа к

компьютерной информации, вредоносных компьютерных программ.

На современном этапе развития российского общества важное значение приобретают проблемы обеспечения его безопасности в целом, и информационной безопасности в частности. Активное и динамичное развитие информационных технологий, особенно компьютерной техники, в управленческой, производственной, коммерческой, банковской и иных сферах объективно требует повышения уровня обеспечения информационной безопасности.

В «Доктрине информационной безопасности Российской Федерации» определены угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, которыми могут являться:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;

утечка информации по техническим каналам;

- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.[2)]

В свою очередь, «Стратегия национальной безопасности Российской Федерации до 2020 года» предусматривает, что угрозы информационной безопасности будут предотвращаться за счет совершенствования безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повы-

2) См.: «Доктрина информационной безопасности Российской Федерации» (утв. Президентом РФ 09.09.2000 N Пр-1895), Российская газета, N 187, 28.09.2000.

шенной опасности в Российской Федерации, повышения уровня защищенности корпоративных и индивидуальных информационных систем, создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности.[3)]

Продолжающее развитие и совершенствование прикладных технических наук, компьютерных технологий, глобальных информационных сетей в условиях рыночной экономики обусловили и совершение большого количества общественно опасных деяний - «компьютерных» преступлений, посредством которых преступники осуществляют несанкционированный доступ к компьютерной информации, незаконное копирование, блокирование, модификацию и уничтожение компьютерной информации.

Общественная опасность киберпреступлений выражается в их умышленном и организованном характере, в том, что данные деяния с технической точки зрения являются высоколатентными и транснациональными, что не позволяет вести успешную борьбу с ними в рамках границ отдельного государства. Тем самым, создавая обществу дополнительные трудности в борьбе с этим преступным явлением, обусловленные достаточно сложным механизмом международно-правового сотрудничества и взаимодействия правоохранительных органов зарубежных стран в данной уголовно-правовой сфере.

Кроме того, общественная опасность компьютерных преступлений заключается в том, что они становятся способом для совершения многих других умышленных преступлений (например, кражи или мошенничества), облегчения их совершения и уничтожения следов преступной деятельности.

Ущерб, причиняемый киберпреступниками, колоссален по своим масштабам и не подается точной оценке, что объясняется высокой латентностью компьютерных преступлений, а также отсутствием единой методики расчета причиненного вреда.

Так, по оценкам аналитиков компании Group-IB объем рынка киберпреступности в РФ в 2012 году составил 1.93 миллиарда долларов.[4)]

В свою очередь, американская корпорация Symantec оценила ущерб от киберпреступности в России за 2013 год в 1 миллиард долларов, а в 2012 году в 1.48 миллиарда долларов. При этом общий ущерб от киберпреступности в мире в 2013 году составил 113 миллиардов долларов, против 110 миллиардов долларов в 2012 году.[5)]

По данным «Лаборатории Касперского», ежедневно появляется до 70 тыс. вредоносных программ. Зачастую они используют новые методы «заражения», скрывая свое присутствие в системе, стремясь действовать в обход защиты. За последний год в 96% российских компаний фиксировались инциденты в области П-безопасности. Больше половины опрошенных специалистов признали факт потери данных в результате заражения вредоносным программным обеспечением (ПО). Наиболее часто IT-специалисты сталкиваются с вирусами. В список актуальных угроз также входят спам, фишинг, сетевые атаки на инфраструктуру компаний (включая целевые и DDos-атаки), а также потенциально опасные уязвимости в программном обеспечении. 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%).[6)]

3) См.: Указ Президента РФ от 12.05.2009 N 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года», Российская газета, N 88, 19.05.2009.

4) http://digit.ru/business/20130910/405335397.html#ixzz2r1xUjpbf (дата обращения: 07.06. 2014).
5) http://go.symantec.com/norton-report-2013/ (дата обращения: 07.06. 2014).
6) http:// www.kaspersky.ru/downloads/pdf/kaspersky_security_network.pdf (дата обращения: 07.06. 2014).

Российское законодательство устанавливает уголовную ответственность за «неправомерный доступ к компьютерной информации» – ст.272 Уголовного кодекса Российской Федерации (далее УК РФ), «создание, использование и распространение вредоносных компьютерных программ» – ст.273 УК РФ, «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» – ст.274 УК РФ. Уголовно-правовые нормы, описывающие преступное деяние и наказание за их совершение, объединены в главу №28 УК РФ «Преступления в сфере компьютерной информации».

Согласно официальным данным Главного Информационного Аналитического Центра Министерства Внутренних Дел Российской Федерации (ГИАЦ МВД России), было зарегистрировано преступлений, предусмотренных статьями 272, 273, 274 УК РФ, в 2010 г. – 6132 (ст.272 УК РФ), 1010 (ст.273 УК РФ), 0 (ст.274 УК РФ),[7] в 2011 г. – 2005 (ст.272 УК РФ), 693 (ст.273 УК РФ), 0 (ст.274 УК РФ),[8] в 2012 г. – 1930 (ст.272 УК РФ), 889 (ст.273 УК РФ), 1 (ст.274 УК РФ),[9] в 2013 г. – 1799 (ст.272 УК РФ), 764 (ст.273 УК РФ), 0 (ст.274 УК РФ).[10]

7) См.: Ф-615 кн.1 *Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации.* Сводный и сборник по России за январь-декабрь 2010 г. http://www.mvd.ru/ (дата обращения: 07.06. 2014).

8) См.: Ф-615 кн.1 *Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации.* Сводный и сборник по России за январь-декабрь 2011 г. http://www.mvd.ru/ (дата обращения: 07.06. 2014).

9) См.: Ф-615 кн.1 *Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации.* Сводный и сборник по России за январь-декабрь 2012 г. http://www.mvd.ru/ (дата обращения: 07.06. 2014).

10) См.: «О направлении статистических сведений»: письмо ФКУ «ГИАЦ МВД России» от 5.03.2014 г. исх.№ 34/4 – 158.

II. Причины компьютерной преступности: онтологические и гносеологические аспекты

Как мы видим, официальная статистика и аналитические отчеты специалистов указывают на снижение уровня компьютерной преступности в России. Однако полагаем, что есть необходимость определиться с причинами компьютерной преступности и тем самым ответить на вопрос - насколько приведенные цифры соответствуют российской действительности.

Анализ научной литературы по данной проблематике позволяет привести следующие точки зрения.

По мнению профессора Ю. Гульбина одной из основных причин возникновения компьютерной преступности вообще явилось информационно-технологическое перевооружение предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных. Другой – реальная возможность получения значительной экономической выгоды за противоправные деяния с использованием ЭВМ (электронно-вычислительных машин). Появилась заманчивая возможность как бы обменивать продукт своего неправомерного труда на иные материальные ценности.[11]

В свою очередь профессор Вехов В.Б. считает, что в качестве основных причин и условий, способствующих совершению компьютерных преступлений, в большинстве случаев стали:

- неконтролируемый доступ сотрудников к пульту управления (клавиа-

11) Гульбин Ю, «Преступления в сфере компьютерной информации», Российская юстиция, (10)1997, с.24.

туре) компьютера, используемого как автономно, так и в качестве рабочей станции автоматизированной сети для дистанционной передачи данных первичных бухгалтерских документов в процессе финансовых операций;

- бесконтрольность за действиями обслуживающего персонала, что позволяет преступнику свободно использовать указанную в п.1 ЭВМ в качестве орудия совершения преступления;
- низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;
- несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;
- отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации и ее безопасности в части защиты средств компьютерной техники от несанкционированного доступа;
- отсутствие категорирования (разграничения) допуска сотрудников к документации строгой финансовой отчетности, в т.ч. находящейся в форме машинной информации;
- отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации.[12)]

12) Вехов В.Б. *Компьютерные преступления: способы совершения и раскрытия,* под ред. Смагоринского Б.П. (М.: Право и Закон, 1996), с.114.

С точки зрения Е.А. Маслаковой: «Преступность, связанная с незаконным оборотом вредоносных компьютерных программ, в любых своих проявлениях представляет собой прежде всего преступный бизнес, в основе которого лежат главным образом экономические причины, т.е. среди различных деформаций общественного сознания, детерминирующих такую преступность как свое следствие, одно из основных мест занимают дефекты, сформированные в его экономической сфере».[13)]

Между тем У.В. Зинина считает, что «Системы защиты информационных систем и сетей связи не успевают совершенствоваться вслед за все более совершенными методами и способами совершения преступлений в сфере компьютерной информации. Сюда же можно отнести и не всегда серьезный подход руководителей предприятий к вопросу обеспечения информационной безопасности и защите информации, а нередко даже и сокрытие от правоохранительных органов фактов компьютерного преступления в организации».[14)]

Таким образом, У.В. Зинина выделяет технические и организационные причины совершения преступлений в сфере компьютерной информации, к которым также относится создание, использование и распространение вредоносных компьютерных программ.

М.М. Малыковцев полагает, что «Преступления, связанные с созданием, использованием и распространением вредоносных программ, и их последствия, зачастую могут являться следствием нескольких различных причин. Как правило, это результат сложного причинно-следственного

13) Маслакова Е.А.. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты. Дис. ... канд. юрид. наук: 12.00.08 (Орел: РГБ, 2008), с.106.

14) Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. Автореферат дис. ... канд. юрид. наук: 12.00.08 (М.: РГБ, 2007), с.18.

взаимодействия, в котором наряду с техническими, организационными и иными обстоятельствами, наличествуют такие элементы как сформировавшееся с годами неверное представление о вредоносных программах, устаревшие взгляды на проблему преступлений в сфере компьютерной информации в целом, непонимание общественной опасности последних».[15)]

Примерно такой же позиции придерживается А.Н. Копырюлин указывая, что «Специфические факторы, способствующие совершению преступлений в сфере компьютерной информации, относятся к социально-экономической, правовой и организационнно-управленческим сферам».[16)]

Интересной на наш взгляд является позиция В.А. Бессонова, который считает, что «компьютерные технологии непроизвольно формируют, возбуждают – вызывают к жизни в преступнике «чувство уязвимости любой защиты», в свою очередь у человека-жертвы всегда присутствует особое антропологическое свойство – криминальная уязвимость, а, следовательно, у компьютера хранящего в себе массу ценной информации, присутствует также особое свойство – «компьютерная» уязвимость. Таким образом, «компьютерная» уязвимость подразумевает собой способность персонального компьютера в силу своих технических, потребительских свойств быть виктимным; виктимологические факторы, влияющие на совершение компьютерных преступлений, делятся по содержанию на социальные, поведенческие и нравственно-психологические».[17)]

15) Малыковцев М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ. Дис. ... канд. юрид. наук: 12.00.08 (М.: РГБ, 2007), сс.145-146.

16) Копырюлин А.Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты. Автореферат дис. ... канд. юрид. наук: 12.00.08 (Тамбов: РГБ, 2007), с.19.

17) Бессонов В.А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации. Дис. ... канд. юрид. наук: 12.00.08 (Н.Новгород: РГБ, 2000), с.211.

Не отрицая вышеуказанные позиции ученых, и в тоже время, не признавая абсолютную бесспорность некоторых из них, автор считает, что причин для существования компьютерной преступности в России значительно больше, чем принято считать, и они носят разнообразный, многогранный характер.

III. Социальные и экономические причины компьютерной преступности в России

С методологической точки зрения, по мнению автора, причины компьютерной преступности представляется возможным классифицировать по сферам общественной жизни и на основании этого критерия выделить следующие виды причин совершения компьютерных преступлений: социальные, экономические, юридические, кадровые, технические, организационные, политические.

К социальным причинам компьютерной преступности в современной России следует отнести:

(1) Всеобщую компьютеризацию российского общества (активное развитие компьютерных технологий, информационно-телекоммуникационных сетей, информационных услуг, электронного документооборота и т.п.), что создает необходимую среду для деятельности киберпреступников.

Как сообщил средствам массовой информации глава Министерства связи и массовых коммуникаций Российской Федерации Игорь Щеголев: «Число пользователей интернета в России в 2011 году, по предварительным данным, выросло на 5.4% - до 70 миллионов человек. Таким образом, количество интернет-пользователей в стране составило 49% от 142 миллионов 857 тысяч

человек, проживающих в России (по данным Росстата). В 2011 году Россия вышла на первое место по количеству интернет-пользователей в Европе, обогнав Германию. По данным Минкомсвязи, наиболее популярным среди россиян интернет-сайтом в 2011 году был «Яндекс», а крупнейшая российская соцсеть «Вконтакте» – лидер по количеству времени, проводимому европейцами на сайте (в среднем около 7.1 часа за месяц). По прогнозу Минкомсвязи, в 2013 году россиян, пользующихся сетью, станет значительно больше – порядка 90 миллионов человек. Щеголев также отметил, что в уходящем году Россия вошла в первую десятку стран мира по развитию широкополосного доступа в интернет. Россия признана наиболее быстро растущей страной по темпам прироста пользователей: ежегодный прирост оценивается более чем в 2 миллиона человек – это более чем 20-процентное увеличение по сравнению с 12-процентным приростом в мире. Министр также сообщил, что в 2011 году общее количество персональных компьютеров составит 74.4 миллиона штук, что на 20.2% больше, чем в 2010 году. Еще в прошлом году мы предполагали, что к 2013 году оснащенность ПК должна составить 62.4 штуки на 100 человек (всего порядка 89 миллионов штук), но уже сейчас скорректировали прогноз, увеличив эту цифру до 62.9 штуки».[18)]

Мы согласны с проф. Т.М. Лопатиной, что компьютеризация, будучи в целом позитивным явлением, тесно связана с феноменом преступности, совершаемой с использованием возможностей высоких технологий и компьютерной техники, что неизбежно приводит к исследованию возникающих здесь криминологических проблем и рассмотрению её как криминологического процесса Развитие информационного обмена, компьютерных технологий стимулирует «изобретательность» преступников, повсеместная компьютеризация предоставляет преступным группировкам возможность доступа к новым техническим средствам, которые позволяют им незаконно присваивать огромные суммы денег, уклоняться от налогообложения, отмывать доходы, полученные преступным путем и т. д. Быстрый рост технических достижений в области хранения и передачи информации, фрагментированность компьютерной сети (вследствие перехода от центральных к файловым процессорам), отставание мер безопасности от уровня развития компьютерных технологий являются криминогенными факторами, порождающими возникновение и рост компьютерных преступлений. Эти явления тесно взаимосвязаны: без компьютеризации не было бы таких оснований для постановки вопросов о «технизации» преступности.[19)]

(2) Противоречия между реальными потребностями населения в информационных услугах, программной продукции и возможностью их удовлетворения легальными способами, в силу низкого уровня жизни.

С 01.01.2014 г. минимальный размер оплаты труда в РФ составляет 5554 рубля в месяц,[20)] т.е. около 170 долларов, что в 3 раза ниже общепринятого международного уровня. При этом минимальный размер оплаты труда составляет: в Швейцарии – 2400 долларов, во Франции – 1720 долларов, в Великобритания – 1540 долларов, в США – 1320 долларов, в Израиле – 1030 долларов, в Испании – 810 долларов, в Польше – 450 долларов, в Турции –

18) http://www.gazeta.ru/news/lenta/2011/12/26/n_2148486.shtml (дата обращения: 07.06. 2014).

19) Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности. Дис. ... докт. юрид. наук: 12.00.08 (М.: РГБ, 2007), сс.106-107.

20) См.: «О минимальном размере оплаты труда»: федеральный закон от 19.06.2000 N 82-ФЗ, Собрание законодательства РФ, 26.06.2000, N 26, ст. 2729.

420 долларов, в Чехии – 410 долларов, в Латвии – 330 долларов.[21)]

Поэтому Россия по-прежнему уступает по качеству жизни своих граждан странам Северной Америки, Европы, некоторым странам Азии (Япония, Южная Корея, Тайвань), Ближнего Востока (Объединенные Арабские Эмираты, Саудовская Аравия, Катар, Кувейт).

Однако для справедливости, необходимо отметить, что в последние годы отмечается рост зарплат в государственном секторе и в целом улучшение уровня жизни населения, но достаточно медленными темпами, т.к. проводимые правительством социальные реформы тормозятся неэффективным управлением на региональном и муниципальном уровне (в силу бюрократизма и коррупции), высоким уровнем инфляции и нестабильной мировой конъюнктурой на российские энергоносители и сырье.

По мнению специалистов, нужда является причиной 20-30% всех корыстных преступлений,[22)] что, по мнению автора, в полной мере относится и к преступлениям в сфере компьютерной информации, которые массово совершаются студентами и учащимися, т.е. категорией населения с низким уровнем доходов.

Для подтверждения данного тезиса, в качестве примера можно рассмотреть приговор Мурашинского районного суда Кировской области от 25.04.2012 года, которым к 1 году ограничения свободы был осужден гр. Пинаев за совершение преступлений, предусмотренных ст. ст. 146 ч.2, 272 ч.2, 273 ч.2 УК РФ. Пинаев 18 декабря 2011 года в период времени с 13 часов до 15 часов 47 минут в помещении ОАО «Железнодорожная торговая компания» по адресу: <адрес> за денежное вознаграждение в размере 4000 рублей, незаконно установил на жесткий диск компьютера программы для ЭВМ: «Microsoft Windows XP Professional SP 3 RUS», в количестве одного экземпляра стоимостью 9276 рублей 87 копеек и «Microsoft Office 2007 Professional Rus» в количестве одного экземпляра стоимостью 14233 рубля 00 копеек, правообладателем которых на территории Российской Федерации является корпорация «Майкрософт»; программы «1С:Предприятие 7.70.027 SQL (Конфигурация: Бухгалтерский учет; Оперативный учет; Расчет Управление распределенными ИБ)» в количестве одного экземпляра стоимостью 171000 рублей, правообладателем которой является компания ООО «1С»; «CorelDRAW Graphics Suite X3» в количестве одного экземпляра стоимостью 11405 рублей 46 копеек, правообладателем которой на территории Российской Федерации является корпорация «Корел». Тем самым, гр. Пинаев причинил материальный ущерб правообладателям корпорации «Майкрософт», компании «Корел», ООО «1С», на сумму 205915 рублей 33 копейки, что является крупным размером.[23)]

Как видно из приведенного примера, стоимость лицензионных компьютерных программ достаточно высока, поэтому, учитывая уровень доходов, для граждан или организаций доступней за несколько сотен рублей установить их пиратские копии, которые по функциональным признакам аналогичны оригиналу.

(3) Несерьезное отношение российского общества к компьютерной преступности.

Произошедшие в нашей стране за последние 20 лет события (развал СССР, переход к многопартийной политической системе и рыночной экономике,

21) http://www. bs-life.ru/rabota/zarplata/mrot2013.html (дата обращения: 07.06. 2014).
22) См.: Кудрявцев В.Н. *Генезис преступления* (М.: Инфра-М, 1998), сс.49-50.
23) См.: Уголовное дело № 1-21 (66502), Архив Мурашинского районного суда Кировской области за 2012 год.

смена политического режима, спад промышленного производства и сельского хозяйства, финансовый дефолт 1998 года, контртеррористические операции на Северном Кавказе) привели к затянувшемуся в российском обществе социальному кризису и резкому снижению уровня жизни наших граждан. Тем самым, отодвинув вопрос противодействия компьютерной преступности в разряд второстепенных, незначительных проблем, что, безусловно, повлияло на рост компьютерных преступлений.

Экономические причины компьютерной преступности в России представляются следующими:

(4) Недобросовестная конкуренция (шпионаж) между производителями программного обеспечения и антивирусной защиты.

Переход России к рыночной экономике с гарантированной свободой предпринимательской деятельности обеспечил естественную конкуренцию между отечественными и зарубежными производителями программной продукции в области компьютерных технологий, тем самым на рынке должен присутствовать как бы отлаженный механизм регулирования спроса и предложения на такую продукцию. Однако на практике существует недобросовестная конкуренция в виде нарушения авторских и патентных прав производителя с целью получения недобросовестными конкурентами сверхприбылей от продажи, так называемой «пиратской» продукции. При этом потребитель либо не в состоянии обнаружить подделку недоброкачественного товара, либо сознательно приобретает нелицензированную продукцию в силу ее дешевизны. Поэтому система саморегулирования рынка в данной ситуации не обеспечивает защиту законных правообладателей программного обеспечения и государство обязано вмешиваться в регулирование этих правоотношений.

В данном случае мы можем говорить об использовании вредоносных компьютерных программ производителями программного обеспечения для «технологического» или промышленного шпионажа в отношении конкурирующих компаний по производству программного продукта.

Например, еще в 1997 году тайваньский разработчик антивирусного ПО Trend Micro обвинил сразу две ведущие антивирусные компании – McAfee и Symantec – в нарушении его патента на технологию сканирования данных, передаваемых по интернету и электронной почте. Позднее компания Symantec предъявила иск McAfee по обвинению в использовании кодов из Norton AntiVirus Symantec в продуктах McAfee.[24)]

(5) Быстрое и относительное безопасное обогащение преступников. Экономическая причина, при которой компьютерное преступление рассматривается преступниками как способ незаконного обогащения.

Так, 4 июня 2012 года сотрудниками Центрального аппарата МВД РФ и ГУ МВД по Москве была пресечена деятельность организованной преступной группы, похищавшей денежные средства вкладчиков банков из восьми регионов России, шпионские программы были внедрены более чем в 1.5 млн. компьютеров. Потерпевшими по уголовному делу признаны компании и организации, расположенные как в Москве и Подмосковье, так и в Санкт-Петербурге, Сургуте, Калининграде, Перми, Омске, Астрахани. Общее количество зараженных компьютеров по предварительным подсчетам Следственного департамента МВД РФ составляет около 1.6 миллионов. Ежемесячный «доход» каждого участника преступной группы составлял около двух миллионов рублей.[25)]

(6) Использование преступниками ресурсов персональных компьютеров и корпоративных сетей в корыстных целях путем создания «ботнетов», т.е.

24) Касперский Е. Компьютерное зловредство (+CD) (СПб.: Питер, 2009), сс.112-113.
25) http://www.interfax.ru/society/news.asp?id=248821 (дата обращения: 07.06. 2014).

сетей «зомби-компьютеров».

Ботнет – это сеть компьютеров, зараженных вредоносной программой, позволяющей киберпреступникам удаленно управлять зараженными машинами без ведома пользователя, с целью рассылки спама, кибершантажа, анонимного доступа в Интернет, фишинга, использования ресурсов зараженных компьютеров и т.д.

Ярким примером может послужить предъявленное в ноябре 2011 года в США прокуратурой г. Нью-Йорка обвинение шести гражданам Эстонии (Владимиру TSASTSIN, 31 год; Тимуру Герасименко, 31год; Дмитрию Егорову, 33года; Валерию Алексееву, 31год; Константину Полтеву, 28 лет и Антону Иванову, 26 лет – все арестованы эстонской полицией и находятся под стражей на территории Эстонской республики) и одному гражданину России (Андрей ТААМЕ, 31 год – находится на свободе), которые занимались распространением вируса-троянца DNS Changer, известного также под именами TDSS, Alureon, TDL4. По данным ФБР, за последние четыре года члены преступной группы инфицировали и создали ботнет из более 4 миллионов компьютеров в 100 странах, получив почти $14 миллионов прибыли.[26)]

В криминальном мире «ботнеты» могут продаваться, обмениваться или передаваться организованными преступными группировками, либо отдельными хакерами. Однако практически всегда здесь присутствуют корыстные мотивы.

26) http://www.fbi.gov/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business (дата обращения: 07.06. 2014).

IV. Правовые, кадровые и организационно-технические причины компьютерной преступности в России

Безусловно, социально-экономические причины компьютерной преступности в современной России носят значимый характер, но к сожалению, причинный комплекс совершения компьютерных преступлений носит более многогранный и разносторонний характер, включая юридические, кадровые, технические и организационные детерминанты данного вида преступности.

В частности, юридические причины компьютерной преступности в России включают:

(1) Несовершенство российского уголовного законодательства в сфере борьбы с компьютерной преступностью.

В уголовном, гражданском и административном законодательстве окончательно не урегулирован вопрос оценки ущерба, причиненного компьютерными правонарушениями и какими критериями должен руководствоваться суд при определении размера этого ущерба и его возмещения виновными.

Кроме того, по мнению автора, целесообразно было бы ввести уголовную ответственность за умышленное приобретение вредоносных программ с целью несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Это связано с тем, что большинство компьютерных преступников не являются специалистами по созданию компьютерных вирусов или вредоносных программ, поэтому для совершения преступлений приобретают вредоносное программное обеспечение на различных хакерских страницах, сайтах, форумах, т.е. используют уже

готовый продукт.

В тоже время, УК РФ регламентирует в ч.ч.1,2 ст.146 ответственность при причинении крупного ущерба авторским или смежным правам, если стоимость экземпляров произведений или фонограмм либо стоимость прав на использование объектов авторского права и смежных прав превышают сто тысяч рублей; в ч.1 ст.165 УК РФ за причинение имущественного ущерба путем обмана или злоупотребления доверием при отсутствии признаков хищения, совершенное в крупном размере, т.е. в размере превышающим двести пятьдесят тысяч рублей; в ч.2 ст. ст. 272, 273, ч.1 ст.274 УК РФ за причинение крупного ущерба, сумма которого превышает один миллион рублей.

Это приводит к тому, что большинство компьютерных преступников избегает уголовной ответственности в силу того, что причиненный ими вред ниже установленного законодателем размера нанесенного ущерба.

Как результат, количество уголовных дел, возбужденных по ст.ст.272-274 УК РФ, сократилось в разы, а по ст.274 УК РФ в 2010-2013 годах уголовные дела вообще не возбуждались, за исключением 2012 года – 1 уголовное дело. При этом административная ответственность за соответствующие правонарушения, причинившие меньший вред в КоАП РФ не установлены.

Также, по мнению автора, пробелом отечественного законодательства является отсутствие нормы об уголовной ответственности юридических лиц за совершение компьютерных преступлений.

(2) Несовершенство судебной практики.

До сих пор отсутствуют разъяснения пленума Верховного суда РФ по квалификации и определению наказаний за компьютерные преступления, что негативно сказывается на следственно-судебной практике и единообразии понимания и применения уголовно-правовых норм органами внутренних дел РФ. Кроме того, в подавляющем большинстве случаев суды при рассмотрении дел о компьютерных преступлениях, назначают «хакерам» и «вирусмейкерам» наказание не связанное с лишением свободы (штраф, условное наказание с испытательным сроком), обосновывая свое решение тем, что данные преступления относятся к деяниям небольшой и средней тяжести. Недостаточная жесткость наказания к лицам, создающим, использующим и распространяющим вредоносные компьютерные программы, по нашему мнению способствует рецидиву со стороны данной категории преступников.

Кадровые причины в деятельности правоохранительных органов:

(3) Недостатки в деятельности органов предварительного следствия.

Проведенный автором анализ официальной статистики показывает, что значительное количество уголовных дел прекращаются на стадии предварительного следствия. Так, например, по данным ГИАЦ при МВД РФ по реабилитирующим основаниям прекращены уголовные дела за создание, использование и распространение вредоносных компьютерных программ: в 2010 г. – 35 из 1010, в 2011 г. – 78 из 693, в 2012г. – 163 из 889; приостановлены уголовные дела за нерозыском лица либо в случае неустановления лица, совершившего преступление: в 2010 г. – 58,[27)] в 2011 г. – 75,[28)] в 2012 г. – 108,[29)] в 2013 г. – 106.[30)]

Из зарегистрированных в 2010 году 1010 уголовных дел направлено в суд 914,[31)] в 2011 году из возбужденных 693 уголовных дел в суд направлено 558,[32)] в 2012 году соответственно 889 уголовных дел и направлено в суд

27) См.: Ф-615 кн.1 (2010).
28) См.: Ф-615 кн.1 (2011).
29) См.: Ф-615 кн.1 (2012).
30) См.: «О направлении статистических сведений»: письмо ФКУ «ГИАЦ МВД России» от 5.03.2014 г. исх.№ 34/4 – 158.
31) См.: Ф-615 кн.1 (2010).
32) См.: Ф-615 кн.1 (2011).

только 664,[33] в 2013 году из зарегистрированных 764 уголовных дел в суд направлено с обвинительным заключением 575 уголовных дел.[34]

Таким образом, официальная статистика показывает, что от 10 до 25 % зарегистрированных уголовных дел прекращается либо приостанавливается на стадии предварительного следствия, что подтверждает тезис о недостатках проводимого расследования преступлений данного вида и качестве подготовки следователей.

(4) Недостатки в деятельности органов и должностных лиц, осуществляющих оперативно-розыскную деятельность.

В органах полиции при УВД по субъектам Российской Федерации созданы отделы по борьбе с преступлениями в сфере высоких технологий (Отделы «К»), которые практически на 100% укомплектованы личным составом, но проблема высококвалифицированных специалистов в сфере информационных технологий (программирования, сетевого администрирования, защиты информации) остается по прежнему острой, т.к. подготовка сотрудников к выполнению поставленных задач остается недостаточной, что выражается в отсутствии специального образования, необходимой квалификации и навыков в области компьютерных технологий.

Указанные подразделения полиции по большей части укомплектованы сотрудниками, имеющими богатый оперативный опыт по линии борьбы с экономическими преступлениями, например с выявлением преступлений в сфере нарушения авторских и смежных прав (ст.146 УК РФ), и изъятием контрафактной продукции (нелицензионных компьютерных программ в области менеджмента, бухгалтерии, экономики; фильмов-новинок, компьютерных игр и иной пиратской компьютерной информации). Однако они не обладают навыками компьютерного программирования, сетевого администрирования, защиты компьютерной информации, что делает проблематичным выявление и раскрытие ими сложных преступлений в сфере компьютерной информации (например в области интернет-банкинга, Ddos-атак, botnet).

В подтверждение данной позиции, можно привести следующую статистику. Так, по данным специалистов «Лаборатории Касперский», в 2012 году в России было зарегистрировано 317697806 вирусных атак (2-е место в мире после США),[35] но при этом, как уже указывалось выше, по факту создания, использования и распространения вредоносных компьютерных программ (ст.273 УК РФ) в 2012 году было возбуждено всего 889 уголовных дел. Это говорит о существенной проблеме выявления и раскрытия полицией компьютерных преступлений.

Данная проблема вполне разрешима за счет привлечения на высокооплачиваемую службу в полицию выпускников кибернетических факультетов технических вузов, а также опытных программистов, специалистов в области информационной безопасности и защиты информации.

Технические причины компьютерной преступности, к которым можно отнести:

(5) Высокую латентность преступлений в сфере компьютерной информации, формирующая у большинства киберпреступников чувство

33) См.: Ф-615 кн.1 (2012).

34) См.: «О направлении статистических сведений»: письмо ФКУ "ГИАЦ МВД России" от 5.03.2014 г. исх.№ 34/4 – 158.

35) Kaspersky Security Bulletin 2012. Основная статистика за 2012 год, http://www.securelist.com/ru/analysis/208050778/Kaspersky_Security_Bulletin_2012_Osnovnaya_statistika_za_2012_god#6 (дата обращения: 07.06. 2014).

собственного превосходства и неуязвимости.

Компьютерные преступления в силу их виртуальности и высокотехнологичности, остаются незамеченными большинством граждан, непосвящённых в вопросы программирования и информационной безопасности.

В свою очередь банки, крупные компании и предприятия став жертвой преступления редко обращаются в правоохранительные органы в целях сохранения своей деловой репутации, банковской или коммерческой тайны.

Таким образом, данную причину вполне можно отнести к разряду экономических.

В частности, бывший начальник бюро специальных технических мероприятий МВД РФ генерал-полковник Борис Мирошников отмечал: «говоря о компьютерных преступлениях, мы часто повторяем, что в этой зоне наблюдается самая высокая латентность – до 80%».[36)]

Однако, по мнению автора, латентность преступлений в сфере компьютерной информации значительно выше и по отдельным видам может составлять 200% (ст.272 УК РФ), и даже тысячи процентов (ст.273 УК РФ).

Организационные (корпоративные) причины компьютерной преступности в России:

(6) Организованный и профессиональный характер компьютерной преступности, позволяющий киберпреступникам считать себя «хакерским» сообществом, частью социальной элиты, научно-техническим андеграундом. В свою очередь, это предполагает, для поддержания своего неординарного статуса и подтверждения принадлежности к криминальному миру, совершение преступлений.

36) http://www.zakon.kz/82167-v-rossii-v-2006-godu-vpervye-ostanovlen.html (дата обращения: 07.06.2014).

В данном случае мы имеем в наличии все признаки «хакеров» и «вирусмейкеров» как профессиональных преступников: устойчивый вид преступного занятия (специализация); получение преступного дохода (прибыли) в результате преступной деятельности; наличие у преступника необходимой квалификации (сетевого администратора, программиста и т.п.) для совершения преступления; наличие у компьютерных преступников определенных правил, «законов» и терминологии,[37)] позволяющих им общаться, обмениваться опытом и находить единомышленников; наличие преступных связей с др. преступными элементами (многие «хакеры» работают по «найму») и др.

V. Политические причины компьютерной преступности в России

В последние пять лет причины компьютерной преступности претерпели определенную трансформацию и кроме традиционных факторов, определяющих совершение преступлений в сфере компьютерной информации, мы отмечаем появление причин, носящих политический характер, затрагивающие сферу национальной безопасности и обороны, международных отношений, функционирования государственной власти и местного самоуправления.

По мнению автора, к политическим причинам компьютерной

37) См.: Словарь жаргонных слов и выражений крэкеров, фрикеров, кардеров. Вехов В.Б. и В.А. Голубев, *Расследование компьютерных преступлений в странах СНГ*, под ред. Смагоринского Б.П. (Волгоград: ВА МВД России, 2004), сс.256-272.

преступности в России можно отнести следующие:

(1) Отсутствие эффективного государственного контроля над киберпространством и средствами массовой информации.

Деятельность СМИ не только не активизирует борьбу общества с компьютерной преступностью, а иногда даже наоборот пытается оправдать киберпреступников, выставляя их в свете «борцов за информационные права», делая акцент на их технической одаренности, смелости, любознательности, предприимчивости.

Книги, газеты, журналы пестрят ссылками на «полезные» сайты (например, www. хакер.ru, www.hackzone.ru, www.sdteam.com, www.oszone.net и др.).[38] В сети «Интернет» любой пользователь может зайти на огромное количество хакерских сайтов и форумов: hacksongs.ru, best-hacker.ru, forumhackerov.ru, truehackers.ru, iso27000.ru, progmnogo.ucoz.ru, ihaker.ru и др.

Поэтому, по мнению автора, государство в лице правоохранительных органов должно занять более жесткую позицию к интернет-провайдерам, электронным СМИ, книжным издательствам, редакциям газет и журналов размещающим информацию преступного характера, вплоть до лишения лицензии и юридической ликвидации.

Определенные шаги в этом направлении уже сделаны. В частности, с 2012 года российским законодательством Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) предоставлено полномочие по ведению «Единый реестра доменных имён, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено», т.е. автоматизированной информационной системы ведения и использования базы данных о сайтах, содержащих запрещённую к распространению в России информацию.

В свою очередь, это позволяет Роскомнадзору через операторов связи и хостинг-провайдеров в течение 6 суток в досудебном порядке удалять контент и блокировать web-страницы при наличии на них детской порнографии или объявлений о привлечении несовершеннолетних в качестве исполнителей в мероприятиях порнографического характера; информации об изготовлении или получении наркотиков, психотропных веществ и их прекурсоров; информации о способах совершения суицида, а также призывов к его совершению; информации о несовершеннолетних, пострадавших в результате преступлений.[39] Аналогичная процедура выполняется Роскомнадзором на основании решения суда о признании информации, распространяемой посредством сети «Интернет», информацией, распространение которой в Российской Федерации запрещено.

В связи с вышесказанным, автором предлагается дополнить п. 1) ч.5 ст.15.1 ФЗ «Об информации, информационных технологиях и о защите информации» о включении в данный реестр сайтов, распространяющих вредоносные компьютерные программы; информацию о способах совершения и сокрытия компьютерных преступлений, а также иную вредоносную компьютерную информацию.

(2) Хактивистское движение как политическая причина компьютерной преступности.

38) Глушаков С.В., М.И. Бабенко, Н.С. Тесленко, *Секреты хакера: защита и атака* (М.: АСТ, Хранитель, 2008), с.533.

39) «Об информации, информационных технологиях и о защите информации»: федеральный закон от 27.07.2006 № 149-ФЗ, Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

Хактивизм (Hacktivism от англ. «Hack» - рубить и «acktivism» - активизм), предусматривает борьбу за права и свободы личности, посредством использования компьютерных технологий и информационно-телекоммуникационных сетей, включая сеть «Интернет». Наиболее известными международными хактивистскими движениями являются «WikiLeaks» и «Anonymous».

Протестными формами хактивистского движения является гражданское неповиновение в виде: блокирования правительственных веб-сайтов, перенаправления URL, Ddos-атаки, кража компьютерной информации и демпинг, веб-сайт пародии и т.д.

Так, например, российские хакеры из группы Anonymous в марте-мае 2012 года предприняли Ddos-атаки против сайтов СМИ: «Дождь», «НТВ», «Коммерсантъ», «Slon.ru», «Эхо Москвы», а также сайтов президента и правительства РФ, заблокировав их на достаточно продолжительное время.

Как результат, в январе 2013 года ФСБ РФ направило в суд уголовные дела в отношении двух жителей г.Красноярска (20-летнего Никиты Спасского и 30-летнего Виктора Хребтова), которые 6, 7 и 9 мая 2012 года при помощи вредоносных компьютерных программ осуществили DDoS-атаки и временно блокировали сайты президента, премьер-министра и правительства РФ.[40)]

(3) Использование кибероружия между враждующими (соперничающими) государствами как геополитическая причина компьютерной преступности.

Так называемое «кибероружие» может быть использовано в политических целях для оказания информационного давления или пропаганды, путем получения контроля над электронными и цифровыми средствами массовой информации, компьютерного шпионажа, вывода из строя средств связи и

40) http://ria.ru/incidents/20130117/918552526.html (дата обращения: 07.06.2014).

массовых коммуникаций противника, блокирования объектов энергоснабжения и транспортной инфраструктуры, иного причинения вреда противоборствующей стороне.

Эксперты «Лаборатории Касперского» считают, что вредоносные программы Stuxnet, Wiper, Flame и Gauss, обнаруженные на Ближнем Востоке в 2010-2012 г.г., являются несомненно кибероружием, разработанными при государственной поддержке.[41)]

Журналистское расследование, проведенное в 2011 году газетой New York Times, подтвердило предположение «Лаборатории Касперского», что вредоносная программа Stuxnet была создана спецслужбами Израиля и США для саботажа ядерной программы Ирана.[42)]

В свою очередь, в августе 2013 года экс-сотрудник ЦРУ Эдвард Сноуден сообщил, что разведывательные службы США в 2011 год провели 231 кибератаку, направленную против электронных сетей иностранных государств, в том числе России, Китая, Ирана и КНДР (Северной Кореи).[43)]

Незадолго до этого, в январе 2013 года, «Лаборатория Касперского» опубликовала отчет, в котором было объявлено об обнаружении вируса-трояна «Backdoor.Win32.Sputnik» (условное название Red October - «Красный Октябрь», по названию шпионской советской подводной лодки в одноименном американском фильме «Охота за Красным Октябрем») и раскрытии глобальной шпионской сети, включавшей зараженные компьютеры более чем 300 различных организаций из ряда стран Восточной Европы,

41) http://www.securelist.com/ru/analysis/208050777/Kaspersky_Security_Bulletin_2012_Razvitie_ugroz_v_2012_godu (дата обращения: 07.06. 2014).

42) http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2& (дата обращения: 07.06. 2014).

43) http://digit.ru/internet/20130902/405019726.html#ixzz2r20AikwZ (дата обращения: 07.06. 2014).

Азии, Африки, и Северной Америки, в т.ч 38 российских организаций.

Вредоносная программа на протяжении пяти лет собирала информацию со всех подключенных к сети компьютеров, флеш-носителей и даже мобильных телефонов, похищая секретную информацию, в основном геополитического и дипломатического характера.[44)]

В настоящее время, «кибервойсками» обладают только два государства – США и Китай, при этом какая-либо информация об их структуре и деятельности носит строго засекреченный характер. С учетом того, что кибератаки со стороны враждебных государств, хактивистских движений, кибертеррористов и обычных киберпреступников могут нанести значительный вред национальной безопасности России, то в Министерстве Обороны и Федеральной Службе Безопасности Российской Федерации должны быть созданы специальные подразделения по обеспечению информационной безопасности страны.

VI. Заключение

С учетом приведенного научного, нормативного, аналитического, статистического и иного исследовательского материала, по мнению автора, можно сделать следующие выводы теоретического и практического характера.

Автором была представлена классификация причин компьютерной

44) http://www.securelist.com/ru/blog/207764382/Operatsiya_Red_October_obshirnaya_set_kibershpionazha_protiv_diplomaticheskikh_i_gosudarstvennykh_struktur (дата обращения: 07.06.2014).

преступности в России по сферам общественной жизни. Однако, несмотря на значимость данного основания классификации, он не является единственным в силу многогранности и динамики развития причинного комплекса преступности. Так, в частности, по действию в пространстве можно выделить международные, национальные и региональные причины компьютерной преступности. Например, жажда обогащения у компьютерных преступников и профессиональный характер компьютерной преступности, безусловно, относятся к международным причинам. В свою очередь, уровень жизни граждан или отношение средств массовой информации, общества к компьютерным преступникам являются причинами национальными. Наконец, компьютеризация общества, уровень развития информационных технологий, финансово-банковских институтов с точки зрения причин компьютерной преступности носят региональный характер. Так количество компьютерных преступлений в Москве, Санкт-Петербурге значительно выше, чем в регионах Сибири и Дальнего Востока (Иркутская область, республика Бурятия, Забайкальский край, Приморский край и др.), что связано с более высоким уровнем развития информационной и банковско-финансовой инфраструктуры в столичных регионах.

Кроме того, причины компьютерной преступности по действию во времени могут быть постоянными и временными (например, жажда обогащения и профессионализм компьютерной преступности – это постоянные причины данного вида преступности, а несовершенство уголовного законодательства, судебной практики, деятельности правоохранительных органов, несомненно, носят временный характер.).

Также причины компьютерной преступности по характеру возникновения могут быть объективными (например, всеобщая компьютеризация и информатизация человеческой цивилизации) и субъективными (суще-

ствующее национальное законодательство, сложившаяся судебная практика, деятельность правоохранительных органов зависит от вполне конкретных лиц: депутатов парламента, судей, прокуроров, следователей, а также непосредственно компьютерных преступников, которые выражают свое личное, т.е. субъективное отношение к процессу совершения преступлений в сфере компьютерной информации и наказания за данные противоправные деяния).

Перечень оснований для классификации причин компьютерной преступности в России можно продолжать, но это тема отдельного научного исследования. Однако можно с полной достоверностью утверждать, что все причины совершения преступлений в сфере компьютерной информации действуют комплексно и взаимосвязано. Поэтому неправильно и антинаучно придавать какому-либо виду причин (например, экономическим) главный и основополагающий характер, а другим наоборот второстепенный и несущественный характер (например, деятельность средств массовой информации или несерьезное отношение общества к компьютерным преступникам).

Официальная статистика, в силу латентности компьютерных преступлений, недостатков в законодательстве РФ и деятельности правоохранительных органов, не отражает реальное состояние компьютерной преступности в России.

Причины компьютерной преступности в современной России носят разносторонний характер и с развитием информационных технологий, их количество будет только увеличиваться.

Устранение вышеуказанных причин компьютерной преступности должно быть симметричным и адекватным со стороны общества, предполагая устранение всех обстоятельств и условий их порождающих (политических, юридических, социальных, экономических, кадровых и иных) как силами государства, так и негосударственных организаций. Тем самым, предупреждение и противодействие компьютерной преступности в современной России должно носить всеохватывающий и комплексный характер.

Библиография

1. Законодательные и правовые акты

- «Об информации, информационных технологиях и о защите информации»: федеральный закон от 27.07.2006 № 149-ФЗ, Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.
- «О минимальном размере оплаты труда»: федеральный закон от 19.06.2000 N 82-ФЗ, Собрание законодательства РФ, 26.06.2000, N 26, ст. 2729.
- «Стратегия развития информационного общества в Российской Федерации»
- (утв. Президентом РФ 07.02.2008 N Пр-212), Российская газета, № 34, 16.02.2008.
- «Доктрина информационной безопасности Российской Федерации» (утв. Президентом РФ 09.09.2000 N Пр-1895), Российская газета, N 187, 28.09.2000.
- «О Стратегии национальной безопасности Российской Федерации до 2020 года»: указ Президента РФ от 12.05.2009 N 537, Российская газета, N 88, 19.05.2009.

2. Диссертации, монографии и научные статьи

- Бессонов В.А., «Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации», Дис. ... канд. юрид. наук: 12.00.08 (Н.Новгород: РГБ, 2000).
- Вехов В.Б., *Компьютерные преступления: способы совершения и раскрытия,* под ред. Смагоринского Б.П. (М.: Право и Закон, 1996).
- Вехов В.Б., Голубев В.А., *Расследование компьютерных преступлений в странах СНГ*, под ред. Смагоринского Б.П. (Волгоград: ВА МВД России, 2004).
- Глушаков С.В., М.И. Бабенко, Н.С. Тесленко, *Секреты хакера: защита и атака* (М.: АСТ, Хранитель, 2008).
- Гульбин Ю., «Преступления в сфере компьютерной информации», *Российская юстиция,* 10(1997).
- Зинина У.В., «Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве», Автореферат дис. ... канд. юрид. наук: 12.00.08. (М.: РГБ, 2007).
- Касперский Е., *Компьютерное зловредство* (+CD) (СПб.: Питер, 2009).
- Копырюлин А.Н., «Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты», Автореферат дис. ... канд. юрид. наук: 12.00.08 (Тамбов: РГБ, 2007).
- Кудрявцев В.Н., *Генезис преступления* (М.: Инфра-М, 1998).
- Лопатина Т.М. «Криминологические и уголовно-правовые основы противодействия компьютерной преступности», Дис. ... докт. юрид. наук: 12.00.08 (М.: РГБ, 2007).
- Малыковцев М.М., «Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ. Дис. ... канд. юрид. наук: 12.00.08 (М.: РГБ, 2007).
- Маслакова Е.А., «Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты», Дис. ... канд. юрид. наук: 12.00.08 (Орел: РГБ, 2008).

3. Статистика и судебная практика

- Ф-615 кн.1 *Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации.* Сводный и сборник по России за январь-декабрь 2010 г. http://www.mvd.ru/ (дата обращения: 07.06.2014).
- Ф-615 кн.1 *Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации.* Сводный и сборник по России за январь-декабрь 2011 г. http://www.mvd.ru/ (дата обращения: 07.06.2014).
- Ф-615 кн.1 *Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации.* Сводный и сборник по России за январь-декабрь 2012 г. http://www.mvd.ru/ (дата обращения: 07.06.2014).
- «О направлении статистических сведений»: письмо ФКУ «ГИАЦ МВД России» от 5.03.2014 г. исх.№ 34/4 – 158.
- Уголовное дело № 1-21 (66502), Архив Мурашинского районного суда Кировской области за за 2012 год.

4. Электронные (интернет) ресурсы:

- http://digit.ru/business/20130910/405335397.html#ixzz2r1xUjpbf (дата обращения: 07.06.2014).

- http://go.symantec.com/norton-report-2013/ (дата обращения: 07.06.2014).
- http:// www.kaspersky.ru/downloads/pdf/kaspersky_security_network.pdf (дата обращения: 07.06.2014).
- http://www.gazeta.ru/news/lenta/2011/12/26/n_2148486.shtml (дата обращения: 07.06.2014).
- http://www. bs-life.ru/rabota/zarplata/mrot2013.html (дата обращения: 07.06.2014).
- http://www.interfax.ru/society/news.asp?id=248821 (дата обращения: 07.06.2014).
- http://www.fbi.gov/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business (дата обращения: 07.06.2014).
- http://www.securelist.com/ru/analysis/208050778/Kaspersky_Security_Bulletin_2012_Osnovnaya_statistika_za_2012_god#6 (дата обращения: 07.06.2014).
- http://www.zakon.kz/82167-v-rossii-v-2006-godu-vpervye-ostanovlen.html (дата обращения: 07.06.2014).
- http://ria.ru/incidents/20130117/918552526.html (дата обращения: 07.06.2014).
- http://www.securelist.com/ru/analysis/208050777/Kaspersky_Security_Bulletin_2012_Razvitie_ugroz_v_2012_godu (дата обращения: 07.06.2014).
- http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2& (дата обращения: 07.06.2014).
- http://digit.ru/internet/20130902/405019726.html#ixzz2r20AikwZ (дата обращения: 07.06. 2014).
- http://www.securelist.com/ru/blog/207764382/Operatsiya_Red_October_obshirnaya_set_kibershpionazha_protiv_diplomaticheskikh_i_gosudarstvennykh_struktur (дата обращения: 07.06.2014).

The Main Causes of Computer Crime in Contemporary Russia*

Konstantin N. Evdokimov
(Irkutsk Law Institute (branch) of the Academy of the General Prosecutor's office of RF)

Abstract

In our age of technological progress, new technologies and the innovation economy has no one doubts the need for the use of electronic computers, computer systems, global information networks in various spheres of political, socio-economic, spiritual and cultural life of society, and in the everyday life of ordinary people. Meanwhile, continuing development of applied technical Sciences, improvement of computer technologies of global information networks in the conditions of market economy led to the emergence of a new kind of socially dangerous behavior - "computer" crimes. In turn, organized and professional character of modern computer crime, its mobile and vysokochastotnyi character, the inability to effectively deal with it within the borders of individual States determine the need to implement international legal cooperation and interaction of law enforcement bodies of different countries in this sphere. In addition, public danger of computer crime increases considerably in connection with the use of computer technology for making many other intentional crime belonging to the category of grave and particularly grave.

* This article was submitted on April 30, 2014 and screened until June 1. Its publication was approved on June 3.

For the decision of problems of information security of the Russian society and state need to increase the efficiency of the criminal law, as well as practice of its application for crimes in the sphere of computer information. The huge scale of the damage being done and extremely low level of compensation indicate that the acting Russian normative-legal base, regulating the fight against such crimes, requires further improvement, including at the regional level.

In judiciary practice has difficulty criminal-legal qualification of the crimes provided in articles 272, 273, 274 of the criminal code, since the establishment of objective evidence of crimes in the sphere of computer information implies not only an understanding of the technical features of the activity in the sphere of high technologies and computer information, but also the use of special knowledge in the field of computer devices and storage media. In addition, need further clarification and individual subjective characteristics of these crimes. So, of course, need to intensify scientific developments criminal-legal means of challenging and complex modern criminological measures of prevention of offences of this type.

This scientific article is devoted to the main causes of computer crime in the Russian Federation. The author carries out the classification and analysis of the most important causes of crime in the sphere of computer information, proposes measures for their elimination and making General conclusions on the further development of computer crime in Russia.

Keywords: Computer crime, cyber crime, crime in the sphere of computer information, causes of crime, malicious computer programs