Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение высшего образования «Казанский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра криминологии и уголовно-исполнительного права

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему
«Криминологическая характеристика и предупреждение преступлений в сфере компьютерной информации»

Выполнил: слушатель, мл. лейтенант полиции Шайхутдинов Ильнур Ильсунович, 40.05.01 Правовое обеспечение национальной безопасности, год набора – 2013, 132 учебная группа.

Руководитель: преподаватель кафедры криминологии и уголовно–исполнительного права, ст. лейтенант полиции Кормильцева Светлана Олеговна.

Рецензент: начальник отдела СЧ ГСУ МВД по Республике Татарстан, подполковник юстиции Ситдикова Альбина Дамировна.

К защите _____
(допущена, дата)
Начальник кафедры _____

Дата защиты: "___" _____20___г. Оценка _____

Казань 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы. Сфера компьютерной информации является активно развивающимся направлением, охватывающим все сферы общественной жизни, и требующей особого внимания со стороны законодателя, в том числе в вопросах информационной безопасности. В настоящее время очевидна необходимость изучения рассматриваемой сферы, новых способов совершения преступлений и разработки мер предупреждения. Преступления в данной сфере характеризуются транснациональным характером и обладают определенной спецификой – высокой латентностью, сложностью выявления, связанного с местом совершения преступления, а также сбором и оформлением доказательной базы.

Особую актуальность представляют вопросы, связанные с противодействием преступлениям в сфере компьютерной информации, в связи с активным развитием информационных технологий и международных компьютерных сетей, которые в значительной степени способствуют облегчению совершения преступных деяний как внутри государства, так и на международном уровне.

Указом Президента Российской Федерации 5 декабря 2016 года утверждена новая Доктрина информационной безопасности Российской Федерации[1]. Она основана на Стратегии национальной безопасности Российской Федерации от 31 декабря 2015 г. и развивает ее соответствующие положения[2].

Повышение эффективности профилактики преступлений, совершаемых в сфере компьютерной информации, является важной составляющей в обеспечении информационной безопасности. Требование законности в

---

[1] Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 5 дек. 2016 г.№ 646 // Собр. законодательства Рос. Федерации. 2016. № 50, ст. 7074.

[2] Стратегия национальной безопасности Российской Федерации: утв. Указом Президента РФ от 31 дек. 2015 г.№ 683 // Собр. законодательства Рос. Федерации. 2016. № 1 (часть II), ст. 212.

информационной сфере и правовое равенство всех их участников основываются на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом и представляют собой один из принципов деятельности государственных органов по обеспечению ее безопасности.

В Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг. отмечается необходимость обеспечения национальных интересов в области цифровой экономики – один из важнейших приоритетов при развитии информационного общества[3]. Этот вектор развития актуализирует Стратегию научно–технологического развития Российской Федерации, в которой среди иных приоритетных направлений указываются те, которые обеспечивают переход к цифровым, интеллектуальным производственным технологиям, роботизированным системам, новым материалам и способам конструирования, созданию систем обработки больших объемов данных, машинного обучения и искусственного интеллекта, в том числе противодействие киберугрозам для общества, экономики и государства[4].

В настоящее время Уголовный кодекс Российской Федерации (далее – УК РФ)[5], предусматривает серьезные меры ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст.ст. 272 – 274 УК РФ).

Анализ статистических данных о преступлениях против безопасности компьютерной информации (ст.ст. 272 – 274 УК РФ) показывает высокий уровень латентности совершенных преступлений. В Российской Федерации число выявленных лиц за рассматриваемые преступления составляло в 2011 г. – 576, в 2012 г. – 633, в 2013 г. – 634, в 2014 г. – 539, в 2015 г. – 575, в 2016 г. –

---

[3] Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы : утв. Указом Президента РФ от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации. 2017. № 20, ст. 2901.

[4] О научно-технологическом развитии Российской Федерации : утв. Указом Президента РФ от 1 дек. 2016 г. № 642 // Собр. законодательства Рос. Федерации. 2016 г. № 49, ст. 6887.

[5] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собр. законодательства Рос. Федерации. 2017. № 1 (часть II), ст. 2102.

476, в 2017 г. – 357, за январь–апрель 2018 г. – 70. Уровень латентности рассматриваемых преступлений подтверждается статистическими данными в рассматриваемой сфере, однако ежегодно наблюдается рост размера ущерба, причиненного вышеуказанными преступлениями.

Теоретическую основу исследования составляют научные труды по криминологии и уголовному праву таких ученых, как А.И. Алексеев, Ю.М. Антонян, А.В. Бриллиантов, Р.М. Валеев, А.И. Долгова, Н.В. Иванцова, Л.В. Иногамова–Хегай, С.М. Иншаков, А.Р. Каюмова, Т.В. Кленова, Л.Л. Кругликов, В.В. Лунеев, В.П. Малков, А.В. Наумов, В.С. Овчинский, А.И. Рарог, Б.В. Сидоров, Ф.Р. Сундуров, Н.С. Таганцев, А.И. Чучаев, В.А. Якушин и др. Вопросы уголовной ответственности за рассматриваемые преступления, их отдельные виды и криминологические аспекты исследованы в в диссертациях С.И. Ушакова «Преступления в сфере обращения компьютерной информации: теория, законодательство, практика» (2000 г.), В.А. Бессонова «Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации» (2001 г.), М. Ю. Дворецкого «Преступления в сфере компьютерной информации: уголовно–правовое исследование» (2001), С.Г. Спириной «Криминологические и уголовно–правовые проблемы преступлений в сфере компьютерной информации» (2001), С.Д. Бражника «Преступления в сфере компьютерной информации: проблемы законодательной техники» (2002), А.М. Доронина «Уголовная ответственность за неправомерный доступ к компьютерной информации» (2003), Т.Л. Тропиной «Киберпреступность: понятие, состояние, уголовно–правовые меры борьбы» (2005), Д.А. Ястребова «Неправомерный доступ к компьютерной информации. Уголовно–правовые и криминологические аспекты» (2005), Д.В. Добровольского «Актуальные проблемы борьбы с компьютерной преступностью» (2006), Т.М. Лопатиной «Криминологические и уголовно–правовые основы противодействия компьютерной преступности» (2006), В. Н. Щепетельникова «Уголовно–правовая охрана электронной информации» (2006), У. В. Зининой «Преступления в сфере компьютерной информации в

российском и зарубежном уголовном праве» (2007), М.А. Зубовой «Компьютерная информация как объект уголовно–правовой охраны» (2008), А.Н. Ягудина «Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно–телекоммуникационных сетей» (2013), А. В. Мнацаканян «Информационная безопасность в Российской Федерации: уголовно–правовые аспекты» (2016), И. Р. Бегишева «Понятие и виды преступлений в сфере обращения цифровой информации» (2017), Р.Р. Гайфутдинов «Понятие и квалификация преступлений против безопасности компьютерной информации» (2017) и др.

Объектом исследования являются общественные отношения, определяющие криминологическую характеристику преступлений в сфере компьютерной информации.

Предметом исследования являются нормы Конституции РФ, международно-правовых актов, Уголовного кодекса РФ, иных федеральных законов, уголовного законодательства других государств, материалы социологических исследований и следственно-судебной практики, статистические данные, научная литература, а также электронные ресурсы информационно-телекоммуникационной сети Интернет.

Цель настоящего исследования состоит в разработке научно обоснованных рекомендаций по выработке мер по предупреждению преступлений в сфере компьютерной информации.

Цель исследования предопределила задачи исследования:

- рассмотреть понятие, признаки и общественную опасность преступлений в сфере компьютерной информации;
- показать особенности состояния, структуры, динамики преступлений в сфере компьютерной информации;
- изучить опыт зарубежных государств по предупреждению и пресечению преступлений в сфере компьютерной информации;

- выявить причины и условия совершения преступлений в сфере компьютерной информации;
- охарактеризовать личность преступника в сфере компьютерной информации;
- рассмотреть место, время, способ совершения преступлений в сфере компьютерной информации;
- раскрыть меры предупреждения преступлений в сфере компьютерной информации.

Методологической основой исследования послужили основополагающие законы и категории материалистической диалектики и теории познания, общенаучный диалектический метод изучения социальных явлений. Использовались также, историко-правовой, статистический, сравнительно-правовой, конкретно-социологический методы.

Структура работы включает введение, три главы, девять параграфов, заключение и список использованной литературы.

ГЛАВА 1. ОБЩЕСТВЕННАЯ ОПАСНОСТЬ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С КОМПЬЮТЕРНОЙ ИНФОРМАЦИЕЙ

§1. Понятие, признаки и общественная опасность преступлений в сфере компьютерной информации

Одна из социальных проблем современного технократического общества – появление компьютерной преступности, причиняющей колоссальный вред общественным отношениям в информационной сфере. Ее возникновение стало возможным из-за того, что граждане, используя компьютерные устройства в личных, производственных или служебных целях, имеют слабое представление о программировании и возможностях программного обеспечения, особенностях функционирования средств создания, хранения, обработки, передачи, защиты компьютерной информации, тем самым становясь потенциальными жертвами компьютерных преступников.

Большую актуальность приобретает вопрос информационной безопасности физических и юридических лиц, т.е. их защиты от несанкционированного доступа к компьютерной информации, вредоносных компьютерных программ и иных компьютерных угроз.

При определении детерминантов «преступность в сфере компьютерной информации», в научном сообществе отсутствует единая позиция, что отражается в многочисленных дискуссиях о содержании и значении данного юридического понятия[6].

Компьютерная преступность – это совокупность преступлений, при совершении которых предметом преступных посягательств выступает

---

[6] Евдокимов К.Н. Политические факторы компьютерной преступности в России / К.Н. Евдокимов // Информационное право. – 2015. – № 1. – С. 41–47., Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий / М.А. Ефремова. – М.: Юрлитинформ, 2015. – С. 55, Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ / И.Г. Смирнова, К.Н. Евдокимов, О.А. Егерева [и др.]; под науч. ред. И.Г. Смирновой. – М. : Юрлитинформ, 2016. – С. 155-160.

компьютерная информация, и отождествляют при этом понятия компьютерного преступления и преступления в сфере компьютерной информации[7].

Т.М. Лопатина считает, что под преступностью в сфере компьютерной информации следует понимать совокупность совершенных на определенной территории за конкретный период преступлений (лиц, их совершивших), непосредственно посягающих на отношения по сбору, обработке, накоплению, хранению, поиску и распространению компьютерной информации, а также преступлений, совершенных с использованием компьютера в целях извлечения материальной выгоды или иной личной заинтересованности[8].

Д.В. Добровольский определяет компьютерную преступность как совокупность всех преступлений в сфере информационных технологий, а не только общественно опасных деяний, предметом которых является компьютерная информация[9].

В ряде научных работ встречается упоминание о киберпреступности – юридическом понятии, которое часто употребляется в научном обороте за рубежом и наиболее полно, по мнению ряда авторов, отражает преступные деяния в сфере компьютерной информации, а также преступления, совершенные с помощью компьютерных устройств, информационно–телекоммуникационных сетей и информационных технологий. Такой подход предполагает, что компьютерная преступность является только частью киберпреступности как более широкого понятия.

Отдельные ученые в своих работах отождествляют понятия преступности в Интернете, киберпреступности, компьютерной преступности[10].

---

[7] Степанов-Егиянц В.Г. Проблемы разграничения неправомерного доступа к компьютерной информации со смежными составами / В.Г. Степанов-Егиянц // Право и кибербезопасность. – 2014. – № 2. – С. 27–32.

[8] Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. ... д-ра юрид. наук: 12.00.08 / Т.М. Лопатина. – М., 2006.

[9] Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: дис. … канд. юрид. наук: 12.00.08 / Д.В. Добровольский. – М., 2006. – С.88.

[10] Чирков Д.К., Саркисян А.Ж. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны / Д.К. Чирков, А.Ж. Саркисян // Актуальные проблемы экономики и права. – 2013. – № 3. – С. 219–226.

Еще один подход предполагает параллельное существование понятий интернет-преступности и компьютерной преступности как части и целого. По мнению, например, Р.И. Дремлюга, не каждое преступление в сфере компьютерной информации представляет собой интернет-преступление, в то же время такие традиционные преступления, как мошенничество, кража, вымогательство и др., совершенные посредством сети Интернет – это интернет-преступления. Причем их последствия не обязательно должны наступать в сети Интернет[11].

С учетом описанных выше подходов к пониманию компьютерной преступности, полагаем целесообразным рассматривать данное понятие в узком и широком смысле.

В узком смысле компьютерная преступность представляет собой совокупность преступлений, при совершении которых в качестве основного объекта выступают охраняемые законом общественные отношения в сфере безопасного создания, хранения, обработки и передачи компьютерной информации, а предметом являются компьютерная информация, средства ее хранения, обработки, передачи и защиты, информационно-телекоммуникационные сети[12].

Компьютерная преступность в широком смысле – это совокупность преступлений, при совершении которых объектом выступают любые общественные отношения в сфере информационных технологий и безопасного функционирования компьютерной информации[13]. При этом компьютерная информация, средства ее создания, хранения, обработки и передачи (компьютеры, смартфоны, кассовые аппараты, банкоматы, платежные терминалы и иные компьютерные устройства), информационно–телекоммуникационные сети не только являются предметом преступного

---

[11] Дремлюга Р.И. Интернет-преступность: монография / Р.И. Дремлюга. – Владивосток: Изд-во Дальневост. ун-та, 2008. – С.91.

[12] Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: дис. … канд. юрид. наук:12.00.08 / Д.В. Добровольский. – М., 2006. – С.88.

[13] Там же. С.89.

деяния, но и используются в качестве средства и орудия совершения преступления.

Таким образом, понятие компьютерной преступности в узком смысле охватывает преступления в сфере компьютерной информации, уголовная ответственность за которые предусмотрена в гл. 28 Уголовного кодекса Российской Федерации, а в широком смысле включает в себя понятия киберпреступности, интернет-преступности, преступности в сфере компьютерной информации, преступности в сфере информационных технологий. Представляется, что такой подход к пониманию компьютерной преступности позволит оценить всю сложность, многообразие рассматриваемого криминального явления и найти определенный баланс среди существующих научных позиций.

Рассуждая о сущности компьютерной преступности, можно прийти к выводу, что компьютерная преступность имеет следующие признаки:

– является разновидностью преступлений, существующих наравне с экономическими, насильственными, коррупционными, экологическими и иными видами преступности;

– тесно взаимосвязана с другими видами преступности, поскольку преступления в сфере компьютерной информации часто выступают способом совершения других уголовных деяний (кража, вымогательство, незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, государственная измена, шпионаж и др.);

– носит высокотехнологичный характер, что вызвано использованием IT–технологий, информационно–телекоммуникационных сетей, компьютерных устройств, носителей компьютерной информации и т.п., которые выступают орудиями и средствами совершения компьютерных преступлений;

– обладает высокой степенью латентности, которая составляет от нескольких десятков до нескольких тысяч процентов по разным видам преступных деяний, что обусловлено различными объективными факторами (нежелание жертв компьютерных преступлений обращаться в

правоохранительные органы, незаметность компьютерных преступлений для большинства населения в силу их совершения в виртуальной среде, сложность выявления компьютерных преступлений при отсутствии необходимого количества специалистов в правоохранительных структурах и т.д.);

– носит высокоорганизованный характер и тесно связана с организованной преступностью, так как значительное количество компьютерных преступлений (DDoS-атаки, банкинг, фишинг, создание ботнетов и др.) совершается организованными преступными группами;

– имеет «профессиональный» характер, так как лица, совершающие компьютерные преступления, обладают преступной специализацией, не совершая иных видов преступных деяний; получают преступный доход (прибыль) в результате преступной деятельности; имеют необходимые знания, умения, навыки в сфере IT-технологий для совершения преступления;

– придерживаются определенных правил, законов, понятий и терминологии, позволяющих им общаться, обмениваться опытом и находить единомышленников;

– характеризуется трансграничностью, так как киберпространство существует вне государственных границ и, будучи общедоступным, позволяет преступнику, находящемуся на территории одного государства, совершать преступления в отношении лиц, находящихся в другом государстве;

– носит транснациональный характер, так как компьютерные преступники в силу своей принадлежности к компьютерному «андеграунду» для получения преступных доходов, облегчения совершения преступных деяний на территории двух и более государств вынуждены, независимо от национальности, объединяться в международные преступные группы[14];

– находится в состоянии динамического развития, что обусловлено постоянным совершенствованием существующих и созданием новых IT-технологий, вовлечением в информационные отношения новых участников,

[14] Номоконов В.А. Киберпреступность как новая криминальная угроза / В.А. Номоконов // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 45–55.

расширением киберпространства за счет увеличения числа пользователей сети Интернет, мобильных компьютерных устройств, переходом к электронному документообороту все большего количества организаций, предприятий, учреждений;

– обрела черты экономической преступности, так как большинство компьютерных преступлений совершается в банковско-финансовом или корпоративном секторе (интернет-банкинг, банковский фишинг, кибервымогательство и т.д.), а деятельность преступников направлена на извлечение доходов (прибыли);

– трансформируется в преступность политического характера, что связано с активизацией противоправной деятельности в киберпространстве Российской Федерации представителей хактивистского движения, спецслужб и силовых структур зарубежных государств, международных экстремистских и террористических организаций (DDoS-атаки на правительственные сайты, кибершпионаж в отношении информационных ресурсов органов государственной власти, силовых ведомств, предприятий оборонно-промышленного комплекса, дипломатических представительств, распространение в сети Интернет экстремистских материалов, вербовка новых членов в террористические организации и т.д.)[15].

Обратимся к общественной опасности компьютерной преступности.

На современном этапе как никогда остро стоит задача обеспечить информационную безопасность в общественных отношениях по поводу функционирования кредитно-финансовых, банковских, информационных систем и баз данных. Это тем более необходимо, принимая во внимание довольно слабые системы защиты в этих учреждениях.

Однако наибольшая угроза информационной безопасности ощущается в посягательствах, осуществляемых в сфере политических отношений, национальной безопасности, обороны и других важнейших отраслях

[15] Номоконов В.А. Киберпреступность: прогнозы и проблемы борьбы / В.А. Номоконов, Т.Л. Тропина // Библиотека криминалиста. – 2013. – № 5 (10). – С. 148–160.

политической сферы общества.

Информационная безопасность общества в настоящее время подвергается серьезным испытаниям в связи с участившимися, особенно в глобальной сети Интернет нападениями и информационными атаками, потенциально способными привнести в жизнь людей хаос, панику, дезориентацию, вплоть до полного подавления здорового общественного сознания. В подтверждение можно привести трагические события в некоторых странах постсоветского пространства – Грузия, Украина, Кыргызстан (тюльпановые и оранжевые революции), «арабская весна» в Северной Африке и Ближнем Востоке, – когда зафиксированы действия группы религиозных экстремистов, убивая невинных людей, взрывая и внося разрушения, на население стран буквально обрушилась дезинформационная атака, особенно в Интернете велась информационная война с целью попытки дискредитации в глазах населения авторитета власти, правоохранительных органов, вызова недоверия к властям и их, якобы, бессилия против «народной воли».

В глобальных сетях существуют огромное число сайтов, содержащих информацию экстремистской направленности, где нередко ведется информационная пропаганда соответствующих антиобщественных взглядов и идей, публикуются призывы к свержению законных органов власти, к силовому захвату власти и другие. Многие развитые страны всерьез обеспокоены возможностью крупных терактов в информационном пространстве, в частности против объектов энергетики, телекоммуникаций, авиационных служб, правительственных структур и военных объектов, могущих блокировать деятельность целых отраслей, крупных предприятий, парализовать службу правительственных органов, спровоцировать техногенные катастрофы, аварии, вызвать панику среди населения, привести к другим деструктивным результатам.

В различных странах существуют стратегически важные объекты, где ведутся исследования секретного характера. Они представляют определенный интерес для лиц, совершающих преступления в сфере компьютерной

информации, специализирующихся на компьютерном шпионаже. Компьютерный шпионаж осуществляется в наиболее наукоемких и дорогостоящих сферах обороной деятельности: научных исследованиях, создании новых видов оружия и военной техники, сложных технологических процессах и т. д.[16]

В социально–духовной сфере компьютерные преступления посягают на не менее важные и значимые объекты уголовно-правовой охраны – честь и достоинство личности, нравственные и духовные устои общества, право личности на интеллектуальное творчество и его плоды. Возможность анонимности, широкий охват аудитории, несовершенство механизмов уголовного преследования в глобальных сетях способствует распространению в информационном пространстве таких опасных преступных деяний, как клевета, возбуждение ненависти или вражды из расовых, национальных и иных побуждений, нарушение неприкосновенности частной жизни и т. д.

Можно отметить коллизии, возникающие при разрешении вопросов, связанных с привлечением к уголовной ответственности лиц, совершивших преступления, находясь в одном государстве, в то время как объект преступного посягательства располагается в другом. По мнению экспертов «реальные пространства сжимаются в виртуальной реальности, и совершенно бессмысленно выстраивать в ней государственные границы»[17]. Соответственно, применение к возникающим в глобальной сети правоотношениям нормативными правовыми актами одного государства не может быть эффективно без учета и связи с законодательством других стран, международным правом.

Компьютерная преступность, в значительно большей степени, чем общеуголовная, способна составлять образ жизни значительной части

---

[16] Абдусаламов Р.А., Арсланов Ш.Д. К вопросу развития международной практики правового регулирования борьбы с преступлениями в глобальных компьютерных сетях // Вестник Дагестанского государственного университета. № 2. – 2016. – С.76.

[17] Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: дис. … канд. юрид. наук: 12.00.08 / Д.В. Добровольский. – М., 2006. – С.93.

населения и формировать полукриминальный менталитет. Количество преступлений в сфере компьютерной информации стремительно растет по мере развития телекоммуникационных сетей и увеличения числа персональных компьютеров.

Распространенность компьютерных преступлений обусловлена расширением сферы применения средств ЭВМ, ростом доверия к автоматизированным системам обработки данных. Ныне ЭВМ управляют технологическими процессами на предприятиях и АЭС, движением самолетов и поездов, контролем финансовых потоков, обрабатывают секретную информацию. В этих процессах участвует большое количество людей, удобность несанкционированного доступа к информационным системам в силу своей относительной простоты, скоротечности, анонимности, отсутствия непосредственного контакта с объектом преступления, подвигает людей к совершению такого рода преступлений.

Важно учитывать социально-психологические условия, в которых ведется расследование преступлений. Настрой общества по отношению к информационным преступлениям, под воздействием СМИ периодически меняется. Это обстоятельство влияет на поведение участников расследования. Их отношения могут быть совершенно полярны – от полного неприятия преступных действий, повлиявших на интересы некоторых слоев общества в конкретной стране, до возвеличивания отдельных преступников. В судах и СМИ к компьютерным преступникам редко подходят с той же строгостью, как и к лицам, совершившим обычные преступления, в действительности их часто превращают в героев.[18]

Вынуждены отметить, что правовая культура общества, не достаточная осведомленность о криминальности подобных деяний, о существовании в целом компьютерных правонарушений и понимании того, какие последствия

[18] Расулев А.К. Криминологическая характеристика преступлений в сфере информационных (компьютерных) преступлений // Вопросы современной юриспруденции. № 2(53). – 2016. – С. 131.

это влечет, резко снижает эффективность противодействия компьютерным преступлениям. Компьютерная преступность, нося по своей природе индивидуальный, сущностный признак, тем не менее, в последнее время приобретает более организованный и опасный характер. Организованность проявляется как в координации действий технического характера, так и в распределении ролей в группах. В компьютерных преступлениях экономической направленности высока вероятность сговора с персоналом информационных систем банков, финансовых учреждений и структур, что позволяет эффективно скрыть следы преступной деятельности. Нередки случаи, когда членом группы являются бывший сотрудник фирмы, хорошо осведомленный о системе кодов и паролей[19].

Организованные преступные группировки часто используют Интернет не только для осуществления преступной деятельности, но и для проведения разведки противодействующих мер против правоохранительных органов, поиска жертв и оказания на них давления. В последнее время наметился еще один политический оттенок в деятельности организованных групп – поддержка, в том числе финансовая, антигосударственных процессов, течений и подобного рода организаций. Политизация организованной преступности, замешанной на национализме и экстремизме, с учетом доступа к глобальным коммуникациям, представляет серьезную опасность[20].

Таким образом, компьютерная преступность – это сложная совокупность нескольких десятков составов преступлений, предусмотренных различными разделами уголовного закона (хищение, несанкционированный доступ, компьютерная фальсификация и мошенничество, компьютерное пиратство, компьютерный шпионаж, компьютерный терроризм и т. д.), а также не представленных пока в уголовном законе, в большинстве своем, связанных с неправильным использованием информационных ресурсов Интернета.

---

[19] Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: дис. … канд. юрид. наук :12.00.08 / Д.В. Добровольский. – М., 2006. – С.94.

[20] Вехов В.Б., Голубев В.А. Расследование компьютерных преступлений в странах СНГ: монография / под ред. Б.П. Смагоринского. Волгоград: ВА МВД России. – М., 2014. – С.87.

§2. Состояние, структура, динамика преступлений в сфере компьютерной информации

На современном этапе развития общества вызывает тревогу рост компьютерных преступлений, распространение которых приобрело транснациональный характер. Появились новые угрозы, опирающиеся на объективные реалии технического прогресса и массовое владение пользователями высокотехнологичных устройств передачи данных.

Для оценки структуры компьютерной преступности в России предпочтительней использовать классификацию и статистику совершенных компьютерных преступлений, применяемые правоохранительными органами, т.е. «нормативный» подход. Это обусловлено тем, что существующая методика учета зарегистрированных, расследованных, приостановленных и прекращенных уголовных дел по преступлениям данного вида уже апробирована временем, а уголовная статистика складывается из ежедневно поступающих данных от территориальных органов ФСБ, МВД, Следственного комитета Российской Федерации. В силу этого правоохранительные органы обладают значительным объемом аналитической информации о структуре и масштабах компьютерной преступности в России, чем экспертное или научное сообщество, что не умаляет роли последних в исследовании данного криминального явления.

Так, на основании статистических данных ГИАЦ МВД России можно утверждать, что примерная структура российской компьютерной преступности выглядит следующим образом (рис.1.1). (Более подробно в Приложении 1)

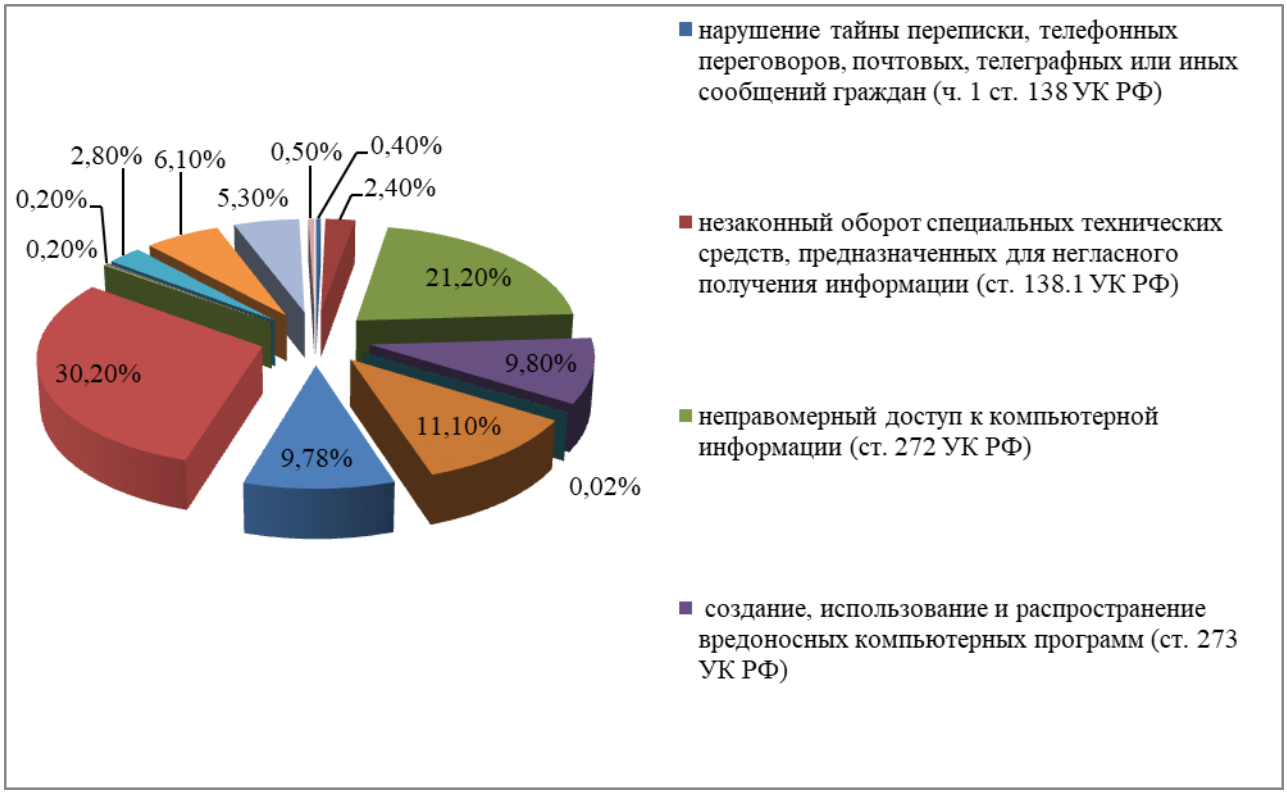


Рис. 1.1 Структура российской компьютерной преступности

Как видим, среди преступных деяний, образующих компьютерную преступность в Российской Федерации, преобладают следующие (таблица 1)[21]:

Таблица 1.

Преступные деяния, образующие компьютерную преступность в Российской Федерации	Удельный вес, %
Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и мошенничество, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 159 УК РФ)	30,20%
Неправомерный доступ к компьютерной информации (ст. 272 УК РФ)	1,20%
Нарушение авторских и смежных прав, совершенное с	11,10%

[21] Сводный сборник состояния преступности по России за январь – декабрь 2011-2017 г. URL: http://mvd. ru (Дата обращения: 04.04.2018)

использованием компьютерных и телекоммуникационных технологий (ст. 146 УК РФ)	
Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)	9,80%
Кража, совершенная с использованием компьютерных и телекоммуникационных технологий (ст. 158 УК РФ)	9,78%

Таким образом, наибольший удельный вес среди совершенных компьютерных преступлений приходится на мошенничество в сфере компьютерной информации и преступления в сфере компьютерной информации, которые в настоящее время составляют основу компьютерной преступности в России.

Однако мнение специалистов и экспертов в сфере информационной безопасности о структуре компьютерной преступности и компьютерных преступлениях несколько отличается от нормативного подхода правоохранительных органов, т.к. основывается на «программно-технических» критериях, однако не противоречит ему, поскольку практически все, так называемые киберугрозы, подпадают под действие Уголовного кодекса РФ (например, под действие ст. ст. 146, 159.3, 159.6, 163, 165, 272, 273, 274 УК РФ) как преступные деяния, и, следовательно, охватываются уголовным законодательством и формами отчетности, принятыми в генеральной прокуратуре РФ, следственном комитете РФ, МВД России для анализа компьютерной преступности.[22]

В свою очередь, исследование научной литературы по рассматриваемой теме также показывает неоднозначность мнений исследователей относительно структуры компьютерной преступности в России. Например, Д.К. Чирков и А.Ж. Саркисян в структуре компьютерной преступности выделяют только те

[22] Евдокимов К.Н. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации/ К.Н. Евдокимов // Всероссийский криминологический журнал. – 2016. – № 2. – С. 322–330.

преступные деяния, которые учитываются ГИАЦ МВД России как преступления, совершенные в сфере телекоммуникаций и компьютерной информации[23]. По мнению М.Б. Эмирова, А.Д. Саидова, Д.А. Рагимханова, «к наиболее распространенным видам преступлений в глобальных компьютерных сетях можно отнести: промышленный шпионаж; саботаж; вандализм; спуфинг (взлом паролей); мошенничество»[24]. Другие авторы исходят из сложной структуры компьютерной преступности и рассматривают входящие в нее преступные деяния по нескольким критериям: в зависимости от объекта, предмета посягательства, способов совершения и т.п.[25]

Например, по объекту посягательства выделяются следующие группы компьютерных преступлений:

– преступления против конфиденциальности, целостности, доступности компьютерных данных и компьютерных сетей,

– экономические компьютерные преступления,

– компьютерные преступления против личных прав и неприкосновенности частной сферы,

– компьютерные преступления против общественных и государственных интересов[26].

Однако анализ нормативных, научных и иных источников показывает, что для иллюстрации структуры компьютерной преступности в России лучше использовать классификацию и статистику, касающуюся совершенных

---

[23] Чирков Д.К., Саркисян А.Ж. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны // Актуальные проблемы экономики и права. – 2013. – № 3. – С. 219-226.

[24] Эмиров М.Б., Саидов А.Д., Рагимханов Д.А. Борьба с преступлениями в глобальных компьютерных сетях // Юридический вестник ДГУ. – 2011. – №2. – С. 63-66.

[25] Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. ... д-ра юрид. наук. М., – 2007. – С. 350; Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 45-55.; Номоконов В.А., Тропина Т.Л. Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. – 2013. – № 5 (10). – С. 148.

[26] Чирков Д.К., Саркисян А.Ж. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны // Актуальные проблемы экономики и права. – 2013. – № 3. – С. 219.

компьютерных преступлений, применяемую информационными центрами правоохранительных органов. Это связано с тем, что существующая методика учета зарегистрированных преступлений, расследованных, приостановленных и прекращенных уголовных дел по преступлениям данного вида уже апробирована временем, а уголовная статистика складывается из ежедневно поступающих данных от территориальных органов ФСБ России, СК России, МВД России, а также из служебных отчетов, докладных записок, информационных писем, обзоров (квартальных, полугодовых, годовых).

Таким образом, наибольший удельный вес среди совершенных компьютерных преступлений приходится на преступления в сфере компьютерной информации (ст.ст. 272, 273 УК РФ) и мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), которые в данное время и составляют основу компьютерной преступности в России[27].

Приведем примеры из судебной практики. Так, гражданин Ч. совершил незаконное использование объектов авторского права, хранение контрафактных экземпляров произведений в целях сбыта, в крупном размере, кроме того, осуществил неправомерный доступ к охраняемой законом компьютерной информации, повлекший модификацию компьютерной информации, из корыстной заинтересованности, а также использовал компьютерные программы, заведомо предназначенные для несанкционированной модификации компьютерной информации и нейтрализации средств защиты компьютерной информации, из корыстной заинтересованности. В судебном заседании подсудимый гражданин Ч. показал, что существо предъявленного ему обвинения понимает, с ним полностью согласен, вину признает в полном объеме и поддерживает свое ходатайство о постановлении приговора в особом порядке, которое было заявлено им своевременно, добровольно, после проведения консультаций с защитником и в его присутствии, и он осознает

[27] Абдусаламов Р.А., Арсланов Ш.Д. К вопросу развития международной практики правового регулирования борьбы с преступлениями в глобальных компьютерных сетях // Вестник Дагестанского государственного университета. – № 2. – 2016. – С.76.

характер и последствия заявленного им ходатайства[28].

Отдельно можно выделить информацию, распространение которой в Российской Федерации подпадает под особый режим распространения: информация, охраняемая законодательством об авторских и смежных правах. Особый режим использования подобного рода информации устанавливается Конституцией РФ и гражданским законодательством.

Так, гр. П. был привлечен к уголовной ответственности за совершение преступления, выразившегося в незаконном использовании объектов авторского права, совершенном в крупном размере с использованием программного обеспечения «FlylinkDC++» в сети Интернет. Гр. П., имея умысел на незаконное использование объектов авторского права, принадлежащих правообладателю – корпорация «Аутодеск Инкорпорейтед», скопировал контрафактные экземпляры программного обеспечения «AutoCAD Architecture 2012 – Русский», исключительные права на который принадлежат корпорации «Аутодеск Инкорпорейтед», произведя их запись на накопитель на жестком магнитном диске (далее НЖМД).

Далее, гр. П., достоверно зная, что программное обеспечение «FlylinkDC++» является программным обеспечением для обмена файлами между пользователями пиринговой сети, то есть среди неограниченного круга лиц, без использования файлообменного сервера, создал настройки для подключения к серверам внутренней сети и незаконно открыл для общего доступа и копирования пользователям сети каталог «AutoCAD.Architecture». Стоимость лицензионного экземпляра указанного программного продукта составила 3000 евро за один экземпляр. Суд признал гр. П. виновным в совершении преступлений, предусмотренных ч. 2 ст. 146 УК РФ, и назначил ему наказание в виде 1 года исправительных работ с удержанием 5% заработка в доход государства. Рост подобного рода правонарушений коррелирован с

[28] Приговор Советского районного суда г. Томска по делу № 1-41/2017 от 16 января 2017 года //Архив Советского районного суда г. Томска. URL: http://sudact.ru. (дата обращения: 10.01.2018).

возрастанием числа пользователей всемирной сети Интернет[29].

В судебной и следственной практике могут возникнуть вопросы, связанные с отграничением неправомерного доступа к компьютерной информации от такого преступления, как, например, нарушение неприкосновенности частной жизни (ст. 137 УК РФ).

Приведем пример из судебной практики по ч. 1 ст. 137 УК РФ. Суд, рассмотрев материалы уголовного дела, установил следующее. Обвиняемый В. в вечернее время, действуя умышленно и незаконно, в связи с возникшей у него к потерпевшей Р. личной неприязнью, вызванной ревностью, с целью распространения сведений о частной жизни лица, составляющих личную тайну для публичной демонстрации, используя свой мобильный телефон «LG», подключенный к сети Интернет, достоверно зная, что данная сеть является средством массовой информации, используемым неопределенным кругом лиц, через свою страницу в социальной сети «В контакте», действуя в нарушение ч. 1 ст. 23, ч. 1 ст. 24 Конституции РФ, ст. 12 Всеобщей декларации прав человека и ст. 17 Международного пакта о гражданских и политических правах, гарантирующих права на неприкосновенность частной жизни, личной тайны, желая создать о потрепевшей Р. перед неопределенным кругом лиц мнение, как о женщине вульгарного поведения, умышленно разместил в группе «Курицы & Бабники», фотографии с изображением потерпевшей Р. без ее согласия, в том числе содержащие интимные изображения ее тела, составляющие личную тайну Р., то есть незаконно распространил сведения о её частной жизни, публично демонстрируя указанную информацию в СМИ в сети Интернет. Рассмотрев материалы уголовного дела, суд признал виновным гр. В. в совершении преступления, предусмотренного по ч. 1 ст. 137 УК РФ[30].

Между тем трудно не признать, что неправомерный доступ к

---

[29] Приговор Ленинского районного суда г. Мурманска по делу № 1-133/14 1-133/2014 от 14 мая 2014 г. // Архив Ленинского районного суда г. Мурманска. URL: http://sudact.ru. (дата обращения: 10.01.2018).

[30] Приговор мирового судьи судебного участка № 13 Кировского района г. Перми от 07.12.2015 по делу № 1-103/2015 // Архив Кировского района г. Перми. URL: https://rospravosudie.com/ (дата обращения: 10.01.2018).

компьютерной информации, содержащей сведения о частной жизни лица, составляющие его личную или семейную тайну, представляет собой не что иное, как специфическую разновидность сбора этих сведений, иными словами, совершение действий, образующих оконченный состав нарушения неприкосновенности частной жизни. Поэтому неправомерный доступ к компьютерной информации, содержащей сведения о частной жизни лица, совершенный с прямым умыслом и из корыстной или иной личной заинтересованности, при условии причинения вреда правам и законным интересам граждан, квалифицируется по совокупности со ст. 137 УК РФ.

Согласно официальной статистике, динамика совершения преступлений в сфере компьютерной информации носит регрессивный характер, т.е. количество зарегистрированных уголовных дел из года в год неуклонно снижается.

По данным ГИАЦ МВД России, общее количество преступлений в сфере компьютерной информации, предусмотренных ст. ст. 272, 273, 274 УК РФ составило[31](таблица 2):

Таблица 2.

Годы	Общее количество преступлений в сфере компьютерной информации, предусмотренных ст.ст. 272, 273, 274 УК РФ
2009	11586
2010	7142
2011	2698
2012	2820
2013	2593
2014	1739

[31] Сводный сборник по России за январь – декабрь 2009-2017 г. URL: http://mvd.ru (дата обращения: 04.04.2018).

2015	2382
2016	1748
2017	1883
2018 (январь–апрель)	758

Таким образом, за последние восемь лет количество выявленных преступлений в сфере компьютерной информации сократилось в 6 раз (количество уголовных дел уменьшилось с 11 586 до 1883). При этом необходимо отметить серьезные проблемы не только в выявлении преступлений в сфере компьютерной информации, но и в деятельности органов дознания и предварительного следствия при расследовании данной категории преступлений[32].

Например, статистика расследованных уголовных дел, возбужденных по признакам преступлений, предусмотренных ст. 272 УК РФ, показывает следующее (таблица 3):

Таблица 3.

Итоговое решение:	2011	2012	2013	2014	2015	2016	2017
прекращены по реабилитирующим основаниям	35	78	163	166	87	112	116
приостановлены за не розыском лица либо в случае не установления лица совершившего преступление	58	75	108	106	119	193	211
направлено в суд	914	558	664	575	344	369	399

Однако можно констатировать, что количество выявляемых

[32] Паненков А.А. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности (кибертерроризм) как реальная угроза внешнему и внутреннему контурам национальной безопасности России // Военно-юридический журнал. № 4. – 2014. – С. 3-13.

преступлений в сфере компьютерной информации и, соответственно, возбужденных уголовных дел сокращается, около 20 % зарегистрированных уголовных дел прекращается либо приостанавливается на стадии предварительного следствия (дознания), в суд направляется немногим более 50 % уголовных дел[33].

Анализируя динамику компьютерной преступности, можно прийти к выводу о том, что в 2018 году следует ожидать роста количества хакерских атак на правительственные сайты, сайты государственных и муниципальных учреждений, а также сайты средств массовой информации для продвижения различных социальных и политических идей (борьба с коррупцией и бюрократизмом, отстаивание политических требований оппозиционных движений; предвыборная агитация; отстаивание информационных прав и свобод в российском сегменте сети «Интернет» и др.). Кроме того, увеличится количество направленных атак на банкоматы, банки и финансово-кредитные организации. Продолжится рост количества заражений POS–терминалов (терминалов для приема к оплате по пластиковым картам) и мобильных устройств. Однако следует ожидать снижения «фишинговой» активности в сети «Интернет», в связи с неэффективностью используемых преступниками схем при совершении этой разновидности компьютерного мошенничества[34].

Таким образом, количество преступлений, предусмотренных ст. 272 УК РФ (неправомерный доступ к компьютерной информации), ст. 273 УК РФ (создание, использование и распространение вредоносных компьютерных программ), ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации), в ближайшей перспективе будет возрастать, что, к сожалению, не обязательно найдет реальное отражение в официальной уголовной статистике и судебно-следственной практике в силу множества объективных причин.

---

[33] Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью : дис. … канд. юрид. наук :12.00.08 / Д.В. Добровольский. – М., 2006. – С.89.

[34] Абдусаламов Р.А., Арсланов Ш.Д. К вопросу развития международной практики правового регулирования борьбы с преступлениями в глобальных компьютерных сетях // Вестник Дагестанского государственного университета. № 2. – 2016. – С.73.

§3. Опыт зарубежных государств по предупреждению и пресечению преступлений в сфере компьютерной информации

Проблема сдерживания и противодействия киберпреступности сегодня является одной из наиболее актуальных и обсуждаемых. Очевидно, что в эпоху глобализации противодействие вызовам современному информационному обществу возможно лишь при консолидации усилий всех государств мира.

Данной проблемы коснулся Генеральный секретарь ООН Пан Ги Мун, отметивший в своем Послании по случаю третьей международной встречи высоких представителей, курирующих вопросы безопасности, что бороться с угрозами международной безопасности, среди которых и киберпреступность, «необходимо комплексно и скоординировано»[35]. В отчете Международного союза электросвязи против преступлений в сфере информационных и коммуникационных технологий (далее ИТК), также отмечается, что успешно противодействовать киберпреступности возможно лишь в случае если «будет принято эффективное международное и национальное законодательство, содействующее оперативному расследованию, судебному преследованию и наказанию преступников в информационной сфере»[36].

Тем не менее, несмотря на осознание государствами необходимости законодательного закрепления уголовно-правовой охраны компьютерной информации от противоправных посягательств со стороны киберпреступников, принятых мер явно недостаточно. Красноречива и показательна в этом плане статистика кибепреступности. Так, согласно результатам Norton Cybercrime Report 2012 ущерб, причиненный пользователем от киберпреступлений, составил 110 млрд. долларов США. Жертвами преступлений стали 556 млн. человек по всему миру (431 млн. – в 2011 г.). В 2012 г. в России жертвами киберпреступников стали 31,4 млн человек, а причиненный ущерб составил 2

---

[35] Послание Генерального секретаря ООН Пан Ги Муна // Право и Безопасность. – № 4. – 2010. – С. 15.

[36] МСЭ делает информационную среду безопасной // Век качества. – № 6. – 2011. – С. 48-50.

млрд долларов[37].

Однако эксперты зачастую расходятся в своих оценках. Например, в 2011 году глава МИД Великобритании Уильям Хейг озвучил цифру в 1 трлн. долларов в год[38]. В отчете Norton Cybercrime Report 2011 общий ущерб оценивался в 388 млрд. долларов в год[39]. Во многом такие расхождения вызваны высоким уровнем латентности компьютерных преступлений: к примеру, в РФ он самый высокий – 90%; в Великобритании – до 85 %; в США – 80 %; в Японии – до 70 %, в КНР – 80%, в ФРГ – 75 %[40]. По этой причине подсчитать реальный ущерб практически невозможно. В любом случае, как мы видим, «цена» киберпреступности колоссальна. К примеру, незаконный оборот на мировом рынке марихуаны, кокаина и героина, вместе взятых, составляет около 288 млрд долларов[41].

Аналитиками рынка киберугроз также отмечается рост количества атак на интернет-пользователей. Отмечается тенденция к изменению вектора компьютерной преступности. Продолжающийся рост числа компьютерных преступлений свидетельствует о необходимости принятия более эффективных и решительных мер. Стремительное развитие высоких технологий привело к тому, что правовые системы государств значительно отстают от современных реалий развития компьютерной преступности. Привычные для нас принципы и институты территориальной юрисдикции уголовного закона, государственных границ, экстрадиции теряют свое значение применительно к кибепространству. Как отмечает А.Б. Попов, «роль национального законодательства снижается, и

---

[37] Киберпреступность. URL: http://www.tadviser.ru/index.php (Дата обращения: 04.05.2018)

[38] Ущерб от кибепреступлений составляет 1 трлн в год во всем мире / Официальный сайт РИА Новости. URL: http://ria.ru/defense_safety/20111021/465985701.html (Дата обращения: 04.05.2018)

[39] Оценен глобальный ущерб от киберпреступлений. URL: http://soft.compulenta.ru /632887/(Дата обращения: 04.05.2018)

[40] Голубев В. DoS-атака: преступление без наказания. URL: http://www.crime-research.ru/analytics/Golubev0305/2 (Дата обращения: 04.05.2018).

[41] Оценен глобальный ущерб от киберпреступлений // URL: http://soft.compulenta.ru/632887/. (Дата обращения: 04.04.2018).

на первый план выходят инструменты международного регулирования»[42].

Договорное сотрудничество государств по противодействию компьютерной преступности осуществляется путем заключения многосторонних, региональных и двусторонних соглашений. Так, основополагающим документом в этой сфере стала Европейская конвенция по кибепреступлениям (преступлениям в кибепространстве), принятая в Будапеште 23 ноября 2001 г. и вступившая в силу 1 июля 2004 года[43], а также Дополнительный протокол к ней от 28 января 2003 года[44], касающийся вопросов уголовной ответственности за распространение информации расистского и ксенофобского характера. На сегодняшний день конвенция подписана 46 государствами и ратифицирована 26 из них. Среди компьютерных преступлений Конвенция называет: незаконные доступ к компьютерным данным (ст. 2); подлог компьютерных данных (ст. 7); компьютерное мошенничество (ст. 8); преступления, связанные с детской порнографией (ст. 9); преступления, связанные с нарушениями авторского права и смежных права (часть 4); и др.

Основной целью принятия Конвенции о киберпреступности явилась необходимость сближения уголовно–правовых и процессуальных систем государств. Определение перечня общественно опасных деяний, совершаемых в сфере компьютерных технологий по замыслу авторов Конвенции, должно было значительно облегчить привлечение киберпреступников к уголовной ответственности.

По мнению российского законодателя, данное положение противоречит

---

[42] Попов А.Б. Международное сотрудничество государств в борьбе с компьютерной преступностью // Вестник Тамбовского университета, Серия: Гуманитарные науки. – Т. 84. – № 4. – 2010. – С. 310-313.

[43] Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) Будапешт, 23 ноября 2001 года // URL: http://mvd.gov.by/main.aspx?guid=4603 (дата обращения 11.05.2018).

[44] Дополнительный протокол к Конвенции по киберпреступлениям в отношении криминализации деяний расистского и ксенофобского характера, осуществляемых при помощи компьютерных систем г. Страсбург, 28 января 2003 года // URL: http://mvd.gov.by/main.aspx?guid=4603 (дата обращения 11.05.2018).

принципу государственного суверенитета и нуждается в пересмотре. В настоящее время широко обсуждается предложенный Россией проект Конвенции ООН «Об обеспечении международной информационной безопасности»[45]. В проекте значительно расширен терминологический аппарат, предлагается ряд новых понятий, ранее встречаемых лишь на доктринальном уровне. В настоящее время проект находится в завершающей стадии обсуждения. Предполагается, что он станет альтернативой во многом уже устаревшей Европейской Конвенции о киберпреступности.

Таким образом, можно констатировать, что в настоящее время накоплена определенная правовая база в сфере противодействия компьютерной преступности. Тем не менее, приведенные статистические данные позволяют нам сделать суждение о малоэффективности принятых международных документов. В частности, Конвенция о кибепреступности 2001 г. в большинстве своих положений, касающихся, прежде всего, понятийного и категориального аппарата, определяющего перечень киберпреступлений, термин компьютерные данные (информация) уже давно потеряла свою актуальность.

Современные реалии таковы, что законодательство должно адекватно и своевременно реагировать на новые вызовы и угрозы киберпреступности. Существенным препятствием, тормозящим международное сотрудничество по противодействию киберпреступности, является недопонимание некоторыми государствами всей остроты данной проблемы. По этой причине в ряде стран до сих пор отсутствует адекватное законодательство по борьбе с киберпреступлениями. Одной из главных проблем является отсутствие официально закрепленного на международном уровне понятия компьютерного преступления и его основных признаков, элементов.

В связи с этим, за последние 30 лет рядом стран выработаны свои подходы к регулированию вопросов уголовной ответственности за

[45] Конвенция об обеспечении международной информационной безопасности (концепция) // URL: http://www.mid.ru (дата обращения 11.05.2018).

преступления в сфере компьютерной информации. Так, в уголовном законодательстве одних государствах компьютерные преступления выделены в качестве отдельных составов преступлений. В других – в качестве квалифицированных либо специальных по отношению к общим составам. (Приложение 2)

Например, в Уголовном Уложении ФРГ[46], в отдельные составы преступлений выделены «информационный шпионаж» (ст. 202 a); «компьютерное мошенничество» (ст. 263 a); «подделка используемых данных» (ст. 269); «компьютерный саботаж» (ст. 303 b) и др. В уголовном кодексе Франции от 1992 года[47] в некоторых статьях указывается на способы совершения традиционных видов преступлений. Например, ст. 411, 9 отдела IV «О саботаже» определяет ответственность за причинение вреда интересам нации, в том числе путем внесения неполадок в работу системы автоматизированной обработки данных. Уголовные кодексы государств предусматривают и разное количество составов компьютерных преступлений. Например, Уголовным Кодексом КНР 1997 г.[48], а также Постановлением комитета ВСНП КНР об охране компьютерных сетей 2000 г., уголовная ответственность установлена за 15 видов компьютерных преступлений; в Уголовном Уложении Германии 1998 г. 8 составов компьютерных преступлений; в УК Республики Казахстан 1997 г. компьютерным преступлениям посвящена и вовсе одна статья – ст. 227.

Подобного рода различия значительно осложняют привлечение к уголовной ответственности киберпреступников.

На наш взгляд, данная тенденция обусловлена следующими обстоятельствами: во-первых, «андройд-устройства» сегодня есть практически у каждого жителя нашей планеты. Во–вторых, по своим функциональным

---

[46] Уголовное Уложение Федеративной Республики Германии в ред. от 21 июня 2017. URL: http://legislationline.org/documents/section/criminal-codes. (дата обращения: 25.03.2018).

[47] Уголовный кодекс Франции от 22 июля 1992 года. URL: http://legislationline.org/documents /section/criminal-codes. (дата обращения: 25.03.2018).

[48] Уголовный кодекс Китайской Народной Республики в ред. от 14 марта 1997 года URL: http://legislationline.org/documents/section/criminal-codes. (дата обращения: 25.03.2018).

признакам современные мобильные устройства практически не уступают компьютерам. В-третьих, развитие телекоммуникационных систем связи привело к тому, что около 2/3 всех пользователей ежедневно выходят в интернет через мобильные устройства. В-четвертых, около 60 % людей не используют антивирусное программное обеспечение для мобильных устройств, и тем самым становятся легкой добычей для киберпреступников. Данные факторы делают мобильное пространство весьма привлекательным для злоумышленников. Практически ни в одном нормативно-правовом акте не встречается термин «мобильных телекоммуникаций».

Названные обстоятельства заставляет нас искать новые подходы к определению компьютерных данных (информации), которое бы учитывало современные тенденции «рынка» киберпреступности. Еще одной проблемой является необходимость создания внутригосударственных и международных органов по противодействию киберпреступности.

На наш взгляд, наиболее эффективно противодействовать компьютерной преступности возможно лишь в рамках специализированных подразделений правоохранительных органов. Очевидно, что для раскрытия «hi-tech преступлений» необходимо обладание специальными познаниями в области информационных технологий.

Отсутствие квалифицированных кадров в данной сфере уголовно–правовых знаний создает благоприятную почву для киберпреступников. Поэтому в настоящее время во многих государствах уже созданы соответствующие подразделения. Так, в апреле 2001 года в Великобритании был создан Британский национальный отдел по борьбе с преступлениями в сфере высоких технологий (National Hi-Tech Unit NHTCU). В настоящее время он входит в Агентство по борьбе с тяжкими преступлениями и организованной преступностью (Serious Organised Crime Agency SOCA), основанное 1 апреля 2006 года. Его задачами являются борьба с мошенничеством, торговлей людьми, наркотиками и т.д. В 2009 году было создано Центральное полицейское подразделение по борьбе с электронными преступлениями (Police

Central ecrime Unit-PCeU), осуществляющее координацию усилий по борьбе с киберпреступностью и обеспечение расследования компьютерных преступлений на национальном уровне. В результате принятия 25 ноября 2002 г. «Закона о внутренней безопасности» в США было создано Министерство внутренней безопасности, в структуре которого в 2003 г. было выделено Национальное подразделение кибернетической безопасности (National Cyber Security Division).

Противодействие киберпреступности осуществляет также ФБР, в рамках которого существует отдел по борьбе с киберпреступностью. Специальные его представительства действуют в различных государствах, в том числе в Италии, Румынии, Нидерландах и др. Свой штат сотрудников по борьбе с компьютерными преступлениями имеет и Пентагон. Специализированные подразделения по борьбе с киберпреступности созданы также в России (управление «К» МВД РФ); Азербайджане (Главное управление по борьбе с кибернетической преступностью); Украине (Отдел по борьбе с киберпреступностью при Департаменте МВД по борьбе с преступлениями, связанными с торговлей людьми) и т.д.

Как мы видим, многие государства сегодня весьма озабочены проблемой роста киберпреступности. Однако, одного лишь национального регулирования в условиях трансграничного характера компьютерной преступности явно недостаточно. Необходимо создание единого координирующего органа, который бы мог обеспечить должное организационное и информационное сопровождение деятельности правоохранительных органов государств по раскрытию и привлечении к уголовной ответственности лиц, причастных к совершению компьютерных преступлений. И такой орган был создан.

Так, 11 января 2013 г. в Гааге состоялось официальное открытие Европейского центра по борьбе с киберпреступностью в рамках Европола. Предполагается, что он станет центральным ведомством Евросоюза по вопросам компьютерных преступлений.

Таким образом, резюмируя все вышеизложенное, мы приходим к выводу,

что к решению проблемы киберпреступности необходимо подходить комплексно.

В этой связи актуальным представляется принятие взамен устаревшей Конвенции о киберпреступности 2001 г. нового международно-правового акта, который бы отвечал современным потребностям борьбы с компьютерными преступлениями. Целесообразно проведение научных исследований с привлечением соответствующих специалистов и разработка на их основе примерного перечня компьютерных преступлений, который бы соответствовал современным тенденциям киберпреступности.

Необходимым является обновление понятийного аппарата, четкое определение терминов «компьютерная информация» и «компьютерное преступление»; создание согласованной стратегии по унификации действующего уголовно-правового законодательства государств всего мирового сообщества. Реализации указанных целей и задач должна быть осуществлена в двуединстве международного и национального регулирования. Тем не менее, принимая во внимание трансграничный характер киберпреступлений, приоритет должен быть отдан именно международному сотрудничеству.

ГЛАВА 2. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§1. Причины и условия совершения преступлений в сфере компьютерной информации

По мнению Ю. Гульбина, одной из основных причин возникновения компьютерной преступности 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. Появилась заманчивая возможность как бы обменивать продукт своего неправомерного труда на иные материальные ценности[49].

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

– неконтролируемый доступ сотрудников к пульту управления (клавиатуре) компьютера, используемого как автономно, так и в качестве рабочей станции автоматизированной сети для дистанционной передачи данных первичных бухгалтерских документов в процессе финансовых операций;

– бесконтрольность действий обслуживающего персонала, что позволяет преступнику свободно использовать 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

[49] Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. 1997. – № 10. – С. 24 – 25.

доступа к рабочей станции и программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

– отсутствие категорирования (разграничения) допуска сотрудников к документации строгой финансовой отчетности, в том числе находящейся в форме машинной информации;

– отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации[50].

Между тем У.В. Зинина в качестве причин указывает, 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»[51].

Таким образом, У.В. Зинина делает акцент на технические и организационные причины совершения преступлений в сфере компьютерной информации.

Интересной, на наш взгляд, является позиция В.А. Бессонова, который считает, что компьютерные технологии непроизвольно формируют, возбуждают – вызывают у преступника «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

---

[50] Вехов В.Б., Голубев В.А. Расследование компьютерных преступлений в странах СНГ: монография / под ред. Б.П. Смагоринского. – 2014. – С.87.

[51] Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: дис. … канд. юрид. наук:12.00.08 / У.В. Зинина. – М., 2007. – С.125.

особое свойство – «компьютерная» уязвимость. Таким образом, «компьютерная» уязвимость подразумевает под собой способность персонального компьютера в силу своих технических, потребительских свойств быть виктимным. При этом виктимологические факторы, влияющие на совершение компьютерных преступлений, делятся по содержанию на социальные, поведенческие и нравственно-психологические[52].

Можно согласиться с А.Н. Копырюлиным, который полагает, что «специфические факторы, способствующие совершению преступлений в сфере компьютерной информации, относятся к социально-экономической, правовой и организационно-управленческим сферам»[53].

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.

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

3. Несерьезное отношение российского общества к компьютерной преступности

Экономические причины компьютерной преступности:

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

2. Быстрое и относительное безопасное обогащение преступников и др.

Можно заключить, что причинный комплекс компьютерной преступности становится все более разнообразным, что обусловлено тотальным

---

[52] Бессонов В.А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации: дис. ... к.ю.н. Н. Новгород, 2007. - С. 65.

[53] Копырюлин А.Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты: Автореф. дис. ... к.ю.н. Тамбов, 2007. С. 39.

использованием и развитием информационных технологий. Поэтому наряду с факторами и причинами юридического, социально–экономического, организационно–технического, кадрового и иного характера в компьютерной преступности и сфере информационной безопасности все более активно заявляют о себе факторы и причины политической направленности.

Политические причины совершения преступлений в сфере компьютерной информации не выделяется в качестве значимых, хотя политические мотивы совершения компьютерных преступлений теоретически допускаются некоторыми учеными[54].

На данный момент ситуация кардинально изменилась, и, по нашему мнению, при анализе причинного комплекса компьютерной преступности в России можно указать на следующие факторы и причины политического характера.

Во-первых, это хактивистское движение как политическая причина компьютерной преступности.

Хактивизм (hacktivism от англ. to hack – «рубить» и acktivism – «активизм») предусматривает борьбу за права и свободы личности (свобода слова, свобода информации и т.д.) посредством использования компьютерных технологий и информационно-телекоммуникационных сетей, включая сеть Интернет. Наиболее известными международными хактивистскими движениями являются WikiLeaks и Anonymous. Считается, что термин был придуман в США (штат Техас) в 1996 г. членом организации Cult of the Dead Cow («Культ мертвой коровы») по кличке Омега[55].

Протестными формами хактивистского движения является гражданское неповиновение в виде: блокирования веб–сайтов государственных органов, перенаправления URL, DDos-атаки, кражи компьютерной информации и

---

[54] Вехов В.Б., Голубев В.А. Расследование компьютерных преступлений в странах СНГ: монография / под ред. Б.П. Смагоринского. – 2014. – С.87.

[55] Криминологический журнал Байкальского государственного университета экономики и права. – 2015. – Т. 9, № 1. URL: http://translate.yandex.net/tr-url/en-ru.ru/en.wikipedia.org/wiki/CNet_News. (Дата обращения: 04.05.2018)

демпинга, веб-сайта пародии и т.д.

Так, например, российские хакеры из группы Anonymous в марте – мае 2012 г. 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 г. УФСБ РФ по Красноярскому краю направило в суд уголовные дела в отношении двух жителей г. Красноярска – граждан С. и Х., которые 6, 7 и 9 мая 2012 г. при помощи вредоносных компьютерных программ осуществили DDoS-атаки, временно блокировав сайты Президента и Правительства РФ. Действия обвиняемых были квалифицированы по ч. 1 ст. 273 УК РФ, т.е. создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации[56].

Таким образом, хактивистское движение, несмотря на свою политическую направленность и благородную цель «обеспечить свободу информации», без стеснения использует вредоносные компьютерные программы, осуществляя взломы сайтов средств массовой информации, государственных учреждений и органов власти либо с применением уже известного вредоносного программного обеспечения, либо привлекая к сотрудничеству вирусописателей для получения от них новых компьютерных вирусов.

Во-вторых, политическим фактором компьютерной преступности в России, условно назовем его «геополитическим», выступает причинение вреда национальной безопасности Российской Федерации со стороны иных государств, путем использования вредоносного программного обеспечения как информационного оружия для уничтожения или повреждения объектов ее

[56] РИА Новости: Красноярского хакера будут судить за атаку на сайт Правительства РФ. 2013. URL: http://ria.ru/incidents/20130117/918552526.html. (Дата обращения: 04.04.2018)

транспортной, энергетической, военной, информационной, финансово–экономической инфраструктуры.

Так называемое «кибероружие» может быть использовано в политических целях для оказания информационного давления или пропаганды, путем получения контроля над электронными средствами массовой информации, вывода из строя средств связи и массовых коммуникаций, блокирования объектов энергоснабжения и транспортной инфраструктуры, нарушения производственной деятельности предприятий оборонно-промышленного комплекса, а также причинение вреда иным объектам стратегического значения.

Так, например, в сентябре 2010 г. вирусу Stuxnet удалось проникнуть в компьютеры иранской атомной станции в Бушере и вывести из строя пятую часть центрифуг по обогащению урана, но, к счастью, он не смог вывести из строя основную операционную систему АЭС, что могло бы привести к катастрофическим последствиям[57].

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

Третьим политико-информационной причиной компьютерной преступности в России является необходимость получения разведывательными службами иностранных государств конфиденциальной информации геополитического, военно-технического, финансово-экономического, дипломатического и иного стратегического характера о Российской Федерации.

В частности, уже вышеуказанной компанией по производству антивирусного программного обеспечения «Лаборатория Касперского» при исследовании вышеуказанного инцидента с вирусом Wiper была обнаружена вредоносная программа Flame и, как следствие, достаточно масштабная

[57] РИА Новости: Компьютерный червь не повредил системе АЭС Бушер. URL: http://ria.ru/science/20100926/279475025.html. (Дата обращения: 04.04.2018)

кампания по кибершпионажу на Ближнем Востоке.

Вирус Flame стал одной из наиболее сложных угроз за всю историю вредоносного программного обеспечения. После полного своего развертывания на компьютере суммарный размер входящих в его состав модулей составляет более 20 мегабайтов. Эти модули выполняют широкий набор вредоносных функций, таких как перехват аудиоданных, сканирование устройств, подключенных по протоколу Bluetooth, кража документов и снимков экрана на зараженном компьютере, информацию об использовании клавиш клавиатуры и др.

Специалисты обнаружили тесную связь между Flame и Stuxnet. Это позволило прийти к выводу, что разработчики Flame действовали в сотрудничестве с разработчиками Stuxnet, возможно, в рамках одного проекта и самому проекту Flame не меньше пяти лет. Эксперты «Лаборатории Касперского» считают, что вредоносные программы Stuxnet, Wiper, Flame и Gauss, обнаруженные на Ближнем Востоке в 2010 – 2012 гг., являются несомненно кибероружием, разработанным при государственной поддержке[58].

В настоящее время с уверенностью можно утверждать, что «кибероружием», средствами «кибершпионажа» и условно назовем их «кибервойсками» обладают США и Китай, при этом какая-либо информация об их структуре и деятельности носит строго засекреченный характер, но в средства массовой информации периодически просачиваются сведения о деятельности «кибервойск» этих государств.

Учитывая серьезность вышеуказанных политических причин компьютерной преступности и исходящих угроз национальной безопасности, Россия сделала первые шаги по защите своих интересов и суверенитета.

В частности, Президент РФ издал Указ № 31с от 15 января 2013 г. «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы

[58] Kaspersky Security Bulletin 2012. Кибероружие. URL: http://www.securelist.com/ru/analysis /208050777/Kaspersky_Security_Bulletin (Дата обращения: 04.04.2018).

Российской Федерации»[59], в соответствии с которым возложил на Федеральную службу безопасности Российской Федерации полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации – информационные системы и информационно–телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.

На данный момент проходят правовую экспертизу проекты Федеральных законов «О безопасности критической информационной инфраструктуры Российской Федерации»[60] и «О внесении изменений в законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»[61], разработанные ФСБ России.

В свою очередь, устранение Российским государством и обществом рассмотренных причин и условий совершения компьютерных преступлений должно носить политический, правовой, социально-экономический, организационно–технический, т.е. комплексный характер (совершенствование законодательства, развитие экономики, более качественная подготовка сотрудников правоохранительных органов в сфере информационной безопасности, развитие отечественной электроники и программного обеспечения, привлечение талантливых программистов на государственную службу, правовое просвещение населения и т.д.).

---

[59] Указ Президента РФ от 15.01.2013 № 31с (ред. от 22.12.2017) «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»// Собрание законодательства РФ. – 2013. – № 3. – Ст. 178.

[60] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»// Собрание законодательства РФ. – 2017. – № 31 (Часть I). – Ст. 4736.

[61] Федеральный закон от 26.07.2017 № 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»// Собрание законодательства РФ. – 2017. – № 31 (Часть I). – Ст. 4742.

§2. Личность преступника в сфере компьютерной информации

Актуальным представляется исследование личности преступника в сфере компьютерной информации ввиду интенсивной компьютеризации общественных отношений. Обращаясь к данным криминологических исследований личности преступника можно заметить, что в системе их ценностей лидирующие позиции отводятся индивидуальным либо клановo-эгоистическим ориентациям.

Превыше всего в таких случаях ставятся личное материальное благополучие, свободное проявление своего «Я», создание для этого наиболее комфортных условий, либо клановый, групповой эгоистический интерес (например, ничем неограниченное совершение компьютерных преступлений и общедоступность компьютерных технологий с безраздельным использованием компьютерной информации приводит к объединению «хакеров» в преступные группировки, имеющие иногда транснациональный характер). Правовое и нравственное начала в сознании преступников чаще всего деформировано или ослаблено.

Г.Т. Мегрелишвили делит киберпреступников на несколько групп[62]:

1. К первой группе автор относит лиц, отличительной особенностью которых является сочетание профессионализма и фанатизма в области компьютерной техники и программирования. Такие лица не имеют четкого противоправного намерения, действуют исключительно для проявления своих профессиональных и интеллектуальных способностей. Они любознательны и азартны. Повышение мер по обеспечению компьютерной безопасности рассматривают как вызов их способностям. Особенностями совершения киберпреступлений данной группой лиц выражается в отсутствии подготовки и плана действий, оригинальности способа совершения, а также в том, что меры

---

[62] Мегрелишвили Г.Т. Криминологический и психологический портрет личности преступников в сфере высоких технологий // Вестник Том. гос. ун-та. – 2017. – № 2. – С. 180 – 181.

по сокрытию преступления не принимаются.

2. Во вторую группу входят лица, страдающие информационными заболеваниями или компьютерными фобиями – это новый вид психических расстройств, тем не менее, признанный Всемирной организацией здравоохранения. Киберпреступления, совершаемые этими лицами, чаще всего связаны с уничтожением компьютерных данных.

3. Третья группа лиц – высококвалифицированные специалисты, чаще всего имеющие высшее техническое образование. Однако, в отличие от первой группы, это профессионалы с устойчивыми преступными навыками и ярко выраженными корыстными целями. Совершают киберпреступления многократно и принимают меры по сокрытию своих действий.

В статье «Общая характеристика психологии киберпреступника» А.Н. Косенковым и Г.А. Черным в зависимости от мотивации выделены следующие типы киберпреступников[63].

Корыстный тип. Помимо характерных для обыкновенного корыстного типа преступников свойств, киберпреступники могут совершать преступления для получения специфических предметов, имеющих особую ценность в киберпространстве, например, хищение игровых предметов, учетных записей игроков, игровой валюты и иных предметов, без цели их дальнейшей продажи.

Насильственный тип. Несмотря на отсутствие физического контакта, такие насильственные преступления, как доведение до самоубийства или угроза убийством, могут быть совершены при помощи электронных устройств и сетей.

Сексуальный тип. Наиболее распространенная деятельность – незаконное распространение порнографических материалов или предметов, понуждение к действиям сексуального характера, развратные действия.

Социально-дезорганизующий тип. Основная цель – нарушение законодательно закрепленных социальных норм, разрушительное влияние на общественные отношения.

---

[63] Косенков А.Н., Черный Г.А. Общая характеристика психологии киберпреступника // Криминологический журнал БГУЭП. – 2012. – № 3 (21). – С.87–94

Идеологически или политически мотивированный тип – совершающий преступления по политическим или идеологическим убеждениям.

Статусный тип. Преступники этого типа, совершая преступления, стремятся получить высокий неформальный социальный статус. В среде киберпреступников статус может иметь большое значение, как мотив.

Исследовательский тип. Основой мотиваций данного типа является изучение программных и аппаратных составляющих электронных устройств и их сетей, поиск уязвимостей, возможности их использования и устранения.

Н.Н Федотовым также описаны несколько типичных образов киберпреступников:

1. «Хакер» (условное наименование). Основными мотивами данного типа являются исследовательский интерес, честолюбие, желание показать свои возможности. Наличие сложных средств защиты компьютерных систем и компьютерных данных воспринимаются хакерами как вызов своим способностям. Казалось бы, что к подобному типу преступников должны относиться пользователи с высоким уровнем знаний в области IT. Однако практика показывает, что основная часть хакеров имеет средний уровень знаний. Можно предположить, что успехов в своей деятельности среднестатистический хакер достиг, получив конкретные знания в Сети – в настоящее время популярно выкладывать в Интернет различные инструкции (так называемые «гайды»).

2. «Инсайдер» (условное наименование). По мнению Н.Н. Федотова является наиболее распространенным типом киберпреступника, с невысоком уровнем знаний в области IT[64]. Его отличительная особенность заключается в том, что в силу служебного положения он обладает доступом в информационную систему. По мнению многих исследователей, большая «взломов» производится сотрудниками, то есть изнутри.

3. «Белый воротничок» (условное наименование). Данный тип представляется как заядлый казнокрад, для которого компьютерные системы

[64] Федотов Н.Н. Форензика – компьютерная криминалистика. М., – 2012. – С.45.

стали новым инструментом преступной деятельности. Наиболее распространенными преступлениями, совершаемыми данным типом киберпреступников являются хищение средств, взяточничество, коммерческий подкуп и продажа информации, которая может составлять коммерческую тайну и так далее. Среди «белых воротничков» могут выделяться личности, злоупотребляющие своим служебным положением из-за обиды на начальство или компанию и т.п., а также расхитители с полным отсутствием моральным принципов, которые занимаются данной преступной деятельностью только потому, что у них имеется такая возможность. Также Н.Н. Федотов выделяет и тех, кто попал в тяжелое материальное положение («квазивынужденные расхитители»).

4. «Е-бизнесмен» (условное наименование). Как правило, не является квалифицированным специалистом в области IT и не имеет служебного положения, которым может злоупотребить. Решение о совершении правонарушения принимается исключительно ради выгоды. Чаще всего «е-бизнесмены» отличаются хорошими способностями к предпринимательству и организации. Данный тип преступников обычно занимается кардингом и фишингом.

5. «Антисоциальный тип» (условное наименование). В данном случае мотивом киберпреступника является социопатия, то есть патологическая тяга к подобного рода деятельности. Такие личности действуют импульсивно, так как не способны к предварительному планированию.

Экспертно-криминалистическим центром МВД РФ также был составлен портрет хакера. Прежде всего, указывают на такие черты как:

– мужчина в возрасте от 15 до 45 лет, имеющий многолетний опыт работы на компьютере;

– является мыслящей личностью, способной принимать ответственные решения;

– добросовестный работник, по характеру нетерпимый к насмешкам;

– любит уединенную работу; часто задерживается на работе[65].

В результате обобщенный криминологический портрет компьютерного преступника обладает следующими характеристиками.

Значительная часть компьютерных преступлений совершена мужчинами, что говорит о гендерной предрасположенности к совершению рассматриваемых деяний. Что касается возраста преступника, то 52, 1 % – это лица в возрасте от 16 до 25; 34, 3 % – от 26 до 35 и 13, 6 % в возрасте от 36 до 45[66].

Таким образом, мы можем наблюдать преобладание среди них молодого поколения. Это объясняется тем, что навык владения компьютером формируется уже в раннем возрасте[67]. Немаловажным является и тот факт, что темпы компьютеризации России значительно увеличиваются, создавая тем самым основу для формирования информационного общества. Уровень образования также играет немаловажную роль в формировании личности хакера.

Доля лиц со средним образованием составляет 40 %, со средним специальным 37 %, а с высшим образованием 23 %[68].

Социальное положение человека является определяющим фактором в побуждении к совершению общественно–опасного деяния. Работниками технической сферы и сферы обслуживания совершается более половины компьютерных преступлений (59,3 %). На долю безработных приходится 28,3 %, доля учащихся (студентов) составляет 11,4%, а служащих всего 1 %[69]. Указанные цифры позволяют сделать вывод о том, что преступления в

---

[65] Чирков Д.К., Саркисян А.Ж. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны // Актуальные проблемы экономики и права. – 2013. – № 3. – С. 219–226.

[66] Василенко Н.А. Преступления в сфере информационных технологии// Старт в науке. – 2016. – № 5. – С. 31–34.

[67] Бессонов В.А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации: Дис. ... к.ю.н. Н. Новгород, – 2017. – С. 65.

[68] Чирков Д.К., Саркисян А.Ж. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны // Актуальные проблемы экономики и права. – 2013. – № 3. – С. 219–226.

[69] Василенко Н.А. Преступления в сфере информационных технологии// Старт в науке. – 2016. – № 5. – С. 31–34.

основном совершаются лицами, имеющими низкий уровень доходов либо не имеющими его вовсе.

В заключение следует указать, что криминологический портрет типичного компьютерного преступника обладает следующими чертами: мужчина 16-25 лет, имеющий среднее или среднее специальное образование, зачастую незанятый в трудовой сфере либо выполняющий низкооплачиваемую работу, холостой, ранее не судимый, уверенный в себе, стремящийся к самоутверждению и получению средств к достойному существованию[70].

§3. Место, время, способ совершения преступлений в сфере компьютерной информации

Определение места совершения преступлений в сфере компьютерной информации вызывает значительные сложности. Разумеется, в случае совершения таких преступлений, как кража, грабеж, разбой, умышленное или неосторожное уничтожение или повреждение компьютерной техники, ее составляющих, носителей информации в виде дисков, флеш-накопителей и т.п., определение места преступления проводится в соответствии с традиционными требованиями и ограничено законодательными положениями о территориальной, воздушной, водной границе, континентальном шельфе, исключительной экономической зоне и т. п. Лица, совершившие такие деяния, подлежат привлечению к уголовной ответственности по УК РФ на основании принципа территориальности. Сложнее обстоит дело в случае совершения криминальных деяний в компьютерных сетях, связывающих несколько регионов или государств, ведущее место среди которых принадлежит глобальной компьютерной сети Интернет.

---

[70] Чирков Д.К., Саркисян А.Ж. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны // Актуальные проблемы экономики и права. – 2013. – № 3. – С. 219–226.

Определенную сложность для определения места совершения преступления представляет наличие офшорных зон, в которых расположены офшорные компании. Офшорные компании можно рассматривать с двух точек зрения. Их можно рассматривать как место совершения преступления вследствие международных трансферных операций, но тогда такое преступление выходит за рамки отечественного уголовного права. С другой стороны офшорную компанию можно рассматривать как абстрактного субъекта уголовно-правовых отношений, тогда данный субъект подпадает под юрисдикцию национального уголовного права. Российский уголовный кодекс не предусматривает привлечение к ответственности юридических лиц, что создает некие проблемы для применения санкций в отношении офшорных компаний. Но выходя за рамки проблемы, можно привлекать учредителей данных компаний, ведь, как правило, численность участников её не превышает 5-10 человек.

В связи с этим место совершения такого криминального деяния и место наступления преступного результата могут находиться друг от друга на больших расстояниях, разделяться таможенными и государственными границами. Можно проанализировать проблему определения места совершения преступления на примере совершения деяний в киберпространстве в сфере хищений с помощью поддельных банковских карт.

В правоотношениях с использованием банковских (кредитных, расчетных, предоплаченных, подарочных, виртуальных) карт участвуют держатели таких карт; выпускающий карты и заключающий договор с держателем банковской карты банк-эмитент; обеспечивающее технологическое и информационное взаимодействие между участниками безналичных расчетов, обработку и хранение информации, необходимой для осуществления расчетов, управление базами данных держателей карт (процессинговый центр); банк-эквайер, осуществляющий прием к оплате платежных карт в качестве средства оплаты товара, работ, услуг; организация, принимающая к оплате банковские

карты (мерчант)[71].

В целях устранения всех споров, возникающих при несанкционированном списании денежных средств со счета законного пользователя банковской карты, с 01.01.2013 г. вступили в силу отдельные положения ст. 9 «Порядок использования электронных средств платежа» Федерального закона от 27.06.2011 г. № 161–ФЗ «О национальной платежной системе»[72]. В новых положениях устанавливается обязанность банков информировать держателей банковских карт о произведенном переводе денежных средств. В свою очередь, пользователь банковской карты обязан известить банка-эмитента об утрате банковской карты или ее несанкционированном использовании. Сторона, нарушившая эти правила считается ответственной за операцию. При соблюдении установленных правил обеими сторонами банк должен возместить сумму транзакции до момента направления уведомления держателем, если не аргументирует вину клиента в нарушении порядка использования банковской карты, повлекшем совершение операции без согласия клиента.

Если незаконная банковская операция совершена через глобальную сеть Интернет, в торгово-сервисной точке, находящейся за пределами Российской Федерации, служба безопасности банка требует от пострадавшего клиента предоставления справки торговой точки о том, что данный клиент не совершал никаких покупок. Это требование на практике неосуществимо. Навстречу могут пойти только пользующемуся услугами данного банка VIP-клиенту. Не вдаваясь в вопросы квалификации, следует отметить, что в приведенных случаях сложно определить место совершения преступления: в одних случаях им признается место совершения покупки, в других – место нахождения банка-эквайера, в третьих – место нахождения банка-эмитента. Например, что считать местом преступления в случаях нарушения известными коммерческими банками законодательства о противодействии легализации (отмывания)

---

[71] Василенко Н.А. Преступления в сфере информационных технологии// Старт в науке. – 2016. – № 5. – С. 31-34.

[72] Там же. С. 30-31.

денежных средств, полученных незаконным путем.

Сложность при определении места совершения преступления, связанного с виртуальным пространством в анализируемых группах преступлений, объясняется еще и тем, что в соответствии с договором банковского счета клиент не имеет права собственности или иного вещного права на денежные средства, находящиеся на счете в банке, или утрачивает его в момент зачисления денежных сумм на банковский счет. Указанные денежные средства с этого момента отходят в собственность коммерческого банка и могут быть использованы им при гарантии прав клиентов на свободное распоряжение данными средствами. Права клиентов носят обязательственный характер и учитываются в виде остатка по счету.[73]

По договору об условиях их использования карты являются собственностью банков-эмитентов и выдаются клиентам во временное пользование. Списание денежных средств с такого счета, в соответствии со ст. 854 ГК РФ[74], осуществляется банком на основании распоряжения клиента, и именно банк должен нести ответственность за последствия исполнения поручения, выданного неуполномоченным лицом, включая случаи, когда банк не мог установить факт выдачи распоряжения неуполномоченным лицом. При расчетах с помощью банковских карт на территории Российской Федерации, банк-эквайер перечисляет на расчетный счет торгово-сервисной организации денежные средства за оплаченные покупателем товары и услуги, и осуществляет выдачу наличных денежных средств пользователям банковских карт, не являющихся их клиентами.

В случае совершения преступного деяния первоначально умысел преступника направлен на незаконное списание денежных средств оплачивающего товары и услуги банка-эквайера и перечисляющего денежные суммы на счет торгово-сервисной точки. Согласно договору между эквайером и

---

[73] Архипов А.В. Проблемы определения места совершения мошенничества в отношении безналичных денежных средств // Старт в науке. – 2016. – № 6. – С. 30-34.

[74] Василенко Н.А. Преступления в сфере информационных технологии// Старт в науке. – 2016. – № 5. – С. 31-34.

торговой точкой, эквайер несет самостоятельные денежные обязательства перед торгово-сервисной организацией по оплате сумм транзакций с помощью банковских карт.

На момент использования поддельной банковской карты потерпевшей стороной будет банк-эквайер, так как именно ему причиняется непосредственный ущерб от преступления, т. е. местом преступления следует считать место нахождения банка-эквайера. Хотя впоследствии указанный ущерб возмещается эквайеру банком-эмитентом.

Хотя УК РФ содержит положения о действии уголовного закона на территории Российской Федерации, но норма, определяющая место совершения преступления, отсутствует. Исходя из принципа территориальности уголовной ответственности (ст. 11 УК РФ) можно определить место преступления как место совершения деяния, наступления последствий либо то место, в котором деяние завершено или пресечено. Существует предложение о применении по аналогии, к определению места совершения преступления, норму УК РФ о времени совершения преступления, в результате чего под местом совершения преступления с использованием компьютерных технологий можно считать место отдачи последней компьютерной команды. Однако в российском праве применение уголовного закона по аналогии не допускается в соответствии с ч. 2 ст. 3 УК РФ.

В том случае, если преступление в сфере компьютерной информации и компьютерной технологии по конструкции имеет материальный состав, то оно считается оконченным с момента наступления общественно опасных последствий. В таких ситуациях и место совершения компьютерного преступления будет не в месте подачи компьютерной команды, а в месте проявления общественно опасных последствий.

В зависимости от вида конструкции состава компьютерного преступления (формального или материального) общественную опасность его будет представлять в первом случае само деяние, поскольку последствия такого деяния находятся за рамками состава и на квалификацию влияния не

оказывают, а во втором – причиненный вред, прописанный в диспозиции, непосредственно влияющий на квалификацию.

В связи с этим место наступления преступного результата как элемент объективной стороны является определяющим, поскольку в соответствии со ст. 8 УК РФ единственным основанием уголовной ответственности является наличие в деянии всех признаков состава преступления.

Преступления в сфере цифровых технологий и цифровой информации все чаще и чаще приобретают транснациональный характер. Указанное обстоятельство служит основанием повышения роли международного сообщества при разработке совместных мероприятий и системы коллективной безопасности в исследуемом направлении.

Достаточно остро в настоящее время стоит проблема унификации уголовно–правового регулирования квалификации преступлений с использованием цифровых технологий на межгосударственном уровне. При наступлении общественно опасных последствий на территории другого государства, причинение в результате преступления вреда гражданам или учреждениям и организациям другого государства делает возможным признание местом совершения преступления территорию данного государства. В случае совершения таких компьютерных преступлений российским гражданином сложным является вопрос о возможности привлечения его к уголовной ответственности на территории такого государства.

Так, в соответствии с ч. 1 ст. 12 УК РФ гражданин Российский Федерации и постоянно проживающий в России апатрид, совершившие вне пределов нашего государства деяние с использованием компьютерных технологий, предусмотренное УК РФ в качестве преступления, подлежат уголовной ответственности, как по уголовному законодательству нашего государства, так и по соответствующему законодательству иностранного государства. Если в отношении общеуголовных преступлений законодательство более или менее единообразно, то законодательство о компьютерных преступлениях и практика его применения весьма различаются.

Бурное развитие информационного пространства, повышение ценности информации настоятельно требует определения места совершения преступлений, связанных с посягательствами на информацию. Это затруднено тем, что информация не материальна, виртуально, существует в виртуальном пространстве, если речь идет об информации, находящейся и передающейся на цифровых носителях.

Полагаем возможным считать местом совершения преступлений, связанных с компьютерной информацией, ноосферу[75], т.е. виртуальное киберпространство. Ответственность должна наступать по месту наступления преступных последствий, либо в силу принципа универсальности в отношении информационно-компьютерных преступлений, если имеет формальной состав – по месту совершения деяния или покушения на деяние по законодательству Российской Федерации в случае совершения преступлений против интересов нашего государства.

Время совершения преступлений рассматриваемой категории лишь в относительно редких случаях устанавливается с точностью до дня и очень редко – до часов и минут. Такая точность обычно требуется при выявлении отдельных эпизодов преступной деятельности. Как правило, время совершения данных преступных деяний исчисляют различными по продолжительности периодами, связанными с деятельностью определенных лиц или организаций. При этом согласно ч. 2 ст. 9 УК РФ временем совершения каждого преступления признается время окончания общественно опасного деяния независимо от момента наступления последствий.

Применительно к компьютерным преступлениям, вполне обоснованно все способы совершения преступлений разделить на три группы:

а) способы, в которых объектом посягательства становится информация, находящаяся на машинных носителях – компьютерах, телефонах, пейджерах,

---

[75] Шестакова И.Г. Ноосфера: материализация идеи как ключевой фактор современного прогресса// Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – 2013. -№ 29. – С. 202-206.

электронных записных книжках и т.д.;

б) способы, в которых компьютерная техника, средства коммуникации и т.д. выступают в роли орудий и средств совершения преступления, а, кроме того, и способы их сокрытия;

в) способы, при совершении которых применяются высокотехнологичные устройства, и их использование направлено на получение незаконного доступа к информации, ее модификацию или блокирование, а также оперирование ею в преступных целях[76].

Резюмируя сказанное, необходимо подчеркнуть, что способ совершения преступления является центральным звеном характеристики деяния. Все другие элементы, так или иначе, связаны с ним, хотя и имеют самостоятельное значение. Также немаловажным является и установление места совершения данного вида преступлений для объективного расследования и привлечения виновных лиц к ответственности. Однако в силу того, что информация не материальна, существует в виртуальном пространстве установить место совершения преступления затруднено, а в некоторых случаях вовсе невозможно. Исходя из этого, необходимо считать местом совершения преступления виртуальное пространство. Ответственность должна наступать по месту наступления преступных последствий, либо в силу принципа универсальности в отношении информационно–компьютерных преступлений, если имеет формальной состав – по месту совершения деяния или покушения на деяние по законодательству Российской Федерации.

[76] Василенко Н.А. Преступления в сфере информационных технологии// Старт в науке. – 2016. – № 5. – С. 31-34.

ГЛАВА 3. ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§1. Общие меры предупреждения преступлений в сфере компьютерной информации

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 2015 г. составил 1,93 млрд. дол., а с середины 2016 по середину 2017 г. в России и СНГ русскоговорящие хакеры «заработали» 2,5 млрд. дол., что составляет 2 % от глобального рынка[77].

В свою очередь, американская корпорация Symantec оценила ущерб от киберпреступности в России в 2016 г. в 1 млрд. долларов, в 2015 г. – в 1,48 млрд. долларов. При этом общий ущерб от киберпреступности в мире в 2017 г. составил 113 млрд. долларов.[78] По данным исследования Cost of Cyber Crime Study, проведенного компанией Ponemon Institute при поддержке HP Enterprise Security, среднегодовой ущерб российских организаций от киберпреступлений в 2018 г. достигает 3,3 млн. долларов. Поэтому в настоящее время профилактика компьютерных преступлений является одним из главных направлений деятельности правоохранительных органов по обеспечению

---

[77] Расследования высокотехнологичных преступлений. URL: http://www.group-ib.ru /index.php/investigation/1063-link-nezavisimye. (Дата обращения: 04.02.2018)

[78] Norton Report 2017: Средний ущерб от одной жертвы кибератаки. URL: http://go.symantec.com/norton-report-2017. (Дата обращения: 04.02.2018)

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[79].

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, 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

---

[79] Преступления, совершаемые с использованием высоких технологий и коммуникаций Шевко Н.Р., Каримов А.М., Турутина Е.Э.// Казань, – 2017. – С. 50-57; Родивилин И.П. Проблемы квалификации преступлений в сфере компьютерной информации, совершаемых с использованием дистанционного управления банковским счетом, и их предупреждение / И.П. Родивилин // Пролог. – 2014. – № 2 (6). – С. 61–64.; Степанов-Егиянц В.Г. Проблемы разграничения неправомерного доступа к компьютерной информации со смежными составами / В.Г. Степанов-Егиянц // Право и кибербезопасность. – 2014. – № 2. – С. 27–32.

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.[80]

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[81]. Схожей точки зрения

---

[80] Евдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации / К.Н. Евдокимов // Академический юридический журнал. – 2015. – № 1 (59). – С. 25–26.

[81] Вехов В.Б., Голубев В.А. Расследование компьютерных преступлений в странах СНГ: монография / под ред. Б.П. Смагоринского. – 2014. – С.87.

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[82]. 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[83]. 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.).[84]

Меры общей превенции 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» от 31 декабря 2015 г. № 683[85].

Например, к общеполитическим мерам предупреждения преступлений в

---

[82] Маслакова Е.А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: дис. ... канд. юрид. наук / Е.А.Маслакова. – М., 2008. – С.98.

[83] Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. ... д-ра юрид. наук / Т.М. Лопатина. – М., 2007. – С.91.

[84] Евдокимов К.Н. Предупреждение компьютерной преступности в Российской Федерации / К.Н. Евдокимов // Академический юридический журнал. – 2015. – № 1 (59). – С. 265–276.

[85] Стратегия национальной безопасности Российской Федерации: указ Президента РФ от 31 декабря 2015 г. № 683 // Российская газета. – 2016. – 15 января.

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 мерам общей превенции 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. [86]

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[87].

Общие меры предупреждения преступлений в сфере компьютерной информации являются основополагающими. Целью мер общей превенции выступает обеспечение в РФ условий для безопасного создания, обработки и распространения компьютерной информации, нормального функционирования компьютерных устройств и информационно–телекоммуникационных сетей. На их основе вырабатываются, реализуются комплексы мер, направленных на решение узкого круга задач.

§2. Специальные и индивидуальные меры предупреждения преступлений в сфере компьютерной информации

Представляется необходимым остановиться именно на специальных индивидуальных 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.

---

[86] Василенко Н.А. Преступления в сфере информационных технологии// Старт в науке. – 2016. – № 5. – С. 31-34.

[87] Стратегия национальной безопасности Российской Федерации: указ Президента РФ от 31 декабря 2015 г. № 683 // Российская газета. – 2016. – 15 января.

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 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 1000 рублей. При этом виновное лицо получает доступ к компьютерной информации, которая представляет для ее владельца 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»[88].

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[89].

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

---

[88] Степанов-Егиянц В.Г. Проблемы разграничения неправомерного доступа к компьютерной информации со смежными составами / В.Г. Степанов-Егиянц // Право и кибербезопасность. – 2014. – № 2. – С. 27–32.

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

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.

Недостаточная жесткость наказания, назначаемого лицам, ранее судимым и продолжающим совершать компьютерные преступления, безусловно, будет способствовать рецидиву со стороны данной категории преступников[90]. 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

[90] Василенко Н.А. Преступления в сфере информационных технологии// Старт в науке. – 2016. – № 5. – С. 37-40.

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 – 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.

Между тем Россия до сих пор не ратифицировала Конвенцию Совета Европы о киберпреступности, участниками которой являются 47 государств. 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.

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[91].

Кроме того, по мнению некоторых 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. Необходимо, 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, веб-страниц, получении

---

[91] Евдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации / К.Н. Евдокимов // Академический юридический журнал. – 2015. – № 1 (59). – С. 25–26.

аккаунтов в социальных сетях указывать свои персональные данные (Ф.И.О., год рождения, данные паспорта)[92].

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.

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.

---

[92] Евдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации / К.Н. Евдокимов // Академический юридический журнал. – 2015. – № 1 (59). – С. 27–28.

3. 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).

4. 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.

5. 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.

6. 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).[93]

Индивидуальные меры предупреждения преступлений в сфере компьютерной информации направлены на устранение неблагоприятных воздействий на конкретную личность, которые могут привести к

---

[93] Евдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации / К.Н. Евдокимов // Академический юридический журнал. – 2015. – № 1 (59). – С. 27.

формированию ее антиобщественной направленности и общественно опасному поведению. Если личность уже сформирована в антиобщественном духе, то индивидуальные меры предупреждения должны изменить антиобщественную направленность характера личности. Кроме того, они призваны предупреждать уже готовящиеся преступления и пресекать попытки их совершения.

Можно выделить следующие методы индивидуальной профилактики: убеждение, оказание помощи, принуждение. К убеждению относятся: индивидуальные и коллективные беседы, общественное обсуждение поведения лица, установление над ним шефства, стимулирование участия в общественно–полезной деятельности. К оказанию помощи относятся: трудоустройство, улучшение бытовых условий, помощь в поступлении на учебу, организация досуга, выборе жизненных целей и нравственных ориентиров. К принуждению относятся: штрафы, принудительное лечение, административный надзор, привлечение к уголовной ответственности.

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.

2. Обратить внимание на правовое воспитание молодежи. 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 деяния, можно снизить риск появления компьютерных преступников в среде технических специалистов, поскольку 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 УК РФ. Через несколько дней в Сети появилось его письмо, в котором он сообщил, что прекращает разрабатывать новые компьютерные вирусы»[94].

3. Необходимо провести индивидуальную виктимологическую профилактику преступлений в сфере компьютерной информации, включающий выявление потенциальных жертв преступлений, организацию обучения населения и обеспечение личной, групповой и семейной безопасности.

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.).

---

[94] Касперский Е.В. Компьютерное зловредство / Е.В. Касперский. – СПб. 2012. – С. 180

§3. Деятельность органов внутренних дел по предупреждению преступлений в сфере компьютерной информации

Предупреждение преступности – одно из приоритетных направлений деятельности органов внутренних дел. Органы внутренних дел играют особую роль в предупреждении преступности и правонарушений. Предупредительная деятельность ОВД осуществляется в значительной части на уровне специального предупреждения. Однако при расследовании и предупреждении преступлений в сфере компьютерной информации возникают некоторые трудности.

Последствия совершения компьютерных преступлений в сфере компьютерной информации в достаточной мере не осознаются федеральными и региональными властями, институтами правовой защиты гражданского населения.

Правоохранительные органы не располагают достаточной информационно-технической и программной базой для расследования преступлений в сфере компьютерной информации. Все структуры правоохранительных органов действуют по-разному при обнаружении факта совершения преступления.

Отсутствие четкого алгоритма взаимодействия подразделений полиции и других структур ведет к тому, что большая часть преступлений остается нераскрытой, оперативники не могут получить достаточно данных для того, чтобы квалифицировать преступление, опираясь на его признаки. Кроме того, кадровый состав суда, прокуратуры и полиции не имеет достаточного уровня подготовки для профилактики таких преступлений и их эффективного расследования.

В России действует единая система учета совершенных преступлений, однако она морально устарела, не отвечает специфике совершения преступлений в сфере компьютерной информации. Средства и технологии информации в настоящее время недостаточно защищены от действий

преступных элементов. Порою пренебрежительность и незнание владельцев компьютерной информации ведет к привлечению внимания к ним преступных элементов.

На мировом уровне уже приняты совершенные законы и внедрены единые системы безопасности, которые позволяют проводить специалистам работу по профилактике преступлений в сфере компьютерной информации, эффективно расследовать преступления и отслеживать преступные действия не только для защиты государственных, но и гражданских интересов. С целью повышения эффективности профилактики преступлений в сфере компьютерной информации, расследования преступлений и защиты интересов граждан предлагается применить несколько необходимых мер. Во-первых, разработать и внедрить проект, который бы предусматривал постоянное функционирование и отслеживание потоков компьютерной информации.

Такая система могла бы выявлять при помощи алгоритмов попытки совершения преступлений, а также устанавливать слежение за активными элементами, которые ведут подозрительную деятельность. Эта система могла бы использоваться и для профилактики преступлений.

Правоохранительная система и судебная система могут взаимодействовать более эффективно, если будут разработаны единые регламенты взаимодействия между структурами. Кроме того, требуется обеспечить подразделения и спецслужбы необходимой программно-технической базой[95].

В связи с активизацией преступных элементов за рубежом требуется разработать и внедрить стандарты, которые бы стали регулировать порядок взаимодействия российских правоохранительных органов и органов других стран. В связи с тем, что обеспечение компьютерной безопасности возложено не только на специальные подразделения и полицию, но и на владельцев, носителей и хранителей компьютерной информации, необходимо наладить взаимодействие между социальными фондами, банками, владельцами серверов

[95] Крылов В.В. Расследование преступлений в сфере информации. — М., 2015. — С 57.

и оборудование путем регламентирования норм взаимодействия. Координированные действия заинтересованных в обеспечении компьютерной безопасности структур позволили бы проводить профилактику преступлений, отслеживать действия подозрительных лиц и эффективно взаимодействовать при обнаружении признаков совершения преступления[96].

С совершенствованием материально-технической базы можно было бы ввести единую систему учета преступлений в сфере компьютерной информации. Ее анализ мог бы быть использован для разработки профилактических мер в сфере обеспечения компьютерной безопасности. К настоящему времени не разработано единой специфики расследования преступлений в сфере обеспечения компьютерной безопасности, что осложняет ведение оперативно-розыскной деятельности.

Знание специфики совершения таких преступлений могло бы улучшить результаты оперативно-розыскной деятельности. Поэтому требуется получение качественных знаний специалистами, как в рамках профессиональной подготовки, так и в рамках программа переподготовки специалистов соответствующих подразделений.

Основными научными дисциплинами в рамках преподавания программ для специалистов в сфере обеспечения безопасности компьютерной информации могли бы стать психология и кибернетика, информационные технологи и психолингвистика. Реализация данного подхода в данное время является затруднительной, поскольку нет достаточного оснащения и необходимой базы для обучения специалистов.

Учитывая тот факт, что повысить эффективность расследования преступлений в сфере компьютерной информации необходимо срочно, следует на базе подразделений обеспечения правопорядка в самом широком смысле использовать последние достижения в сфере информационных технологий.

---

[96] Гарбатович Д.А. Проблемные аспекты эффективности норм, предусматривающих ответственность за совершение преступлений в сфере компьютерной информации // Библиотека криминалиста. – 2013. – № 5. – С. 6-14.

В арсенал оперативной техники следует включить современные технические приборы и устройства (компьютеры и программное обеспечение). Для личного состава правоохранительных структур необходимо предусмотреть разработку и принятие программ подготовки. С целью выполнения долгосрочной стратегии следует предусмотреть возможности для организации переподготовки специалистов в сфере обеспечения компьютерной безопасности[97].

Данными программами должна преследоваться не только качественная теоретическая подготовка специалистов, но и практическая работа по освоению современной компьютерной техники и программных средств. Без соблюдения этих требований итоги оперативно-розыскной деятельности по фактам преступлений в сфере компьютерной информации останутся неудовлетворительными.

Таким образом, повышению эффективности расследования и предупреждения преступлений ОВД в сфере компьютерной информации будет способствовать усовершенствование правовой, технической базы и внедрение программ подготовки специалистов в сфере обеспечения компьютерной безопасности.

[97] Крылов В.В. Расследование преступлений в сфере информации.— М., 2015. — С 85.

ЗАКЛЮЧЕНИЕ

На современном этапе развития общественных отношений большую роль набирают информационные технологии, так как проникают во все сферы общественной жизни. В результате этого появилась необходимость осмысления последствий их создания и практического использования. Особую роль приобретает обеспечение информационной безопасности.

На сегодняшний день сохраняется устойчивая тенденция роста компьютерных преступлений.

Эксперты международной компании Group-IB, специализирующейся на предупреждении и расследовании киберпреступлений, считают, что основными преступными деяниями, образующими рынок киберпреступности в России, являются:

1) мошенничество в системах интернет–банкинга;

2) фишинг;

3) хищение электронных денег;

4) услуги обналичивания иных нелегальных доходов;

5) спам (информация о медикаментах и различной контрафактной продукции, поддельном программном обеспечении, сфере услуг, образования, туризма и др.);

6) продажа трафика;

7) продажа эксплойтов;

8) продажа загрузок;

9) анонимизация;

10) DDoS–атаки.

Анализируя динамику компьютерной преступности, можно прийти к выводу о том, что в 2018 году следует ожидать роста количества хакерских атак на правительственные сайты, сайты государственных и муниципальных учреждений, а также сайты средств массовой информации для продвижения различных социальных и политических идей (борьба с коррупцией и

бюрократизмом, отстаивание политических требований оппозиционных движений; предвыборная агитация; отстаивание информационных прав и свобод в российском сегменте сети «Интернет» и др.). Кроме того, увеличится количество направленных атак на банкоматы, банки и финансово–кредитные организации. Продолжится рост количества заражений POS-терминалов (терминалов для приема к оплате по пластиковым картам) и мобильных устройств, однако следует ожидать снижения «фишинговой» активности в сети «Интернет» в связи с неэффективностью используемых преступниками схем при совершении этой разновидности компьютерного мошенничества.

Разработка теоретических и прикладных правовых вопросов защиты компьютерной информации является одной из важных проблем развития правовой науки и непременным условием комплексного обеспечения информационной безопасности информационной сферы. Следовательно, и проблема развития законодательства в области борьбы с компьютерными преступлениями, выходит далеко за рамки одного лишь уголовно–правового законодательства и требует, в силу своей специфики, комплексного подхода к развитию правовых норм ряда отраслей права и других научных направлений.

Анализ полученных выводов позволил сформулировать следующие предложения по предупреждению и профилактике преступлений в сфере компьютерной информации, совершенствованию уголовного законодательства и сложившейся правоприменительной практики:

1. Совершенствование действующего уголовного законодательства. 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».

Кроме того, для более эффективного противодействия преступлениям в сфере компьютерной информации, необходимо 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».

2. Совершенствование судебной практики по уголовным делам о компьютерных преступлениях.

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.

4. Совершенствование информационного законодательства РФ. Например, нужно принять федеральный закон 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.

5. Активизировать деятельность средств массовой информации по

предупреждению компьютерных преступлений.

6. Обратить внимание на правовое воспитание молодежи.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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).

Дальнейшее усовершенствование законодательства, мер предупреждения в области преступлений в сфере компьютерной информации поможет не только избежать проблем в настоящее время, но и будет способствовать предотвращению появления еще более глобальных проблем в будущем.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Законы, нормативные правовые акты и иные официальные документы

1. Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) Будапешт: принят 23 ноября 2001 г.: по состоянию на 02 февраля 2018 г. URL: http://mvd.gov.by/main.aspx?guid=4603 (дата обращения 02.02.2018).

2. Дополнительный протокол к Конвенции по киберпреступлениям в отношении криминализации деяний расистского и ксенофобского характера, осуществляемых при помощи компьютерных систем г. Страсбург: принят 28 января 2003 г.: по состоянию на 02 февраля 2018 г. URL: http://mvd.gov.by/main.aspx?guid=4603 (дата обращения 02.02.2018).

3. Конвенция об обеспечении международной информационной безопасности (концепция). URL: http://www.mid.ru (дата обращения 04.02.2018)/

4. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г.: по состоянию на 1 февраля 2018 г. – СПб.: Щит, 2018. – 94 с.

5. Уголовный кодекс Российской Федерации: Федеральный закон: принят Гос. Думой 13 июня 1996 г.: № 63–ФЗ: по состоянию на 01 февраля 2018 г. – М.: Издательство «Омега–Л», 2018. – 237 с.

6. Уголовно–процессуальный кодекс Российской Федерации: Федеральный закон: принят Гос. Думой 18 декабря 2001 г.: № 174–ФЗ: по состоянию на 01 февраля 2018 г. – Москва: Проспект, 2018. – 320 с.

7. Гражданский кодекс Российской Федерации (Часть четвертая): Федеральный закон: принят Гос. Думой 18 декабря 2006 г.: № 231–ФЗ: по состоянию на 01 февраля 2018 г. // Справочно–правовая система «Консультант Плюс».

8. Федеральный закон «Об основах системы профилактики правонарушений в Российской Федерации»: принят Гос. Думой 23 июня 2016 г.: № 182–ФЗ: по

состоянию на 01.02.2018 г.// Справочно–правовая система «Консультант Плюс».

9. Федеральный закон «Об информации, информационных технологиях и о защите информации»: принят Гос. Думой 27 июля 2006 г.: № 149–ФЗ: по состоянию на 02.02.2018 // Справочно–правовая система «Консультант Плюс».

10. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»: принят Гос. Думой 26 июля 2017 г.: № 187–ФЗ //Справочно–правовая система «Консультант Плюс».

Федеральный закон от 26.07.2017 N 193–ФЗ

11. Федеральный закон от 26.07.2017 № 193–ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"// Собрание законодательства РФ. – 2017. – № 31 (Часть I). – Ст. 4742.

12. Закон РФ «О государственной тайне»: принят Гос. Думой 21 июля 1993 г.: № 5485–1–ФЗ: по состоянию на 02.02.2018 // Справочно–правовая система «Консультант Плюс».

13. «Стратегия национальной безопасности Российской Федерации»: утв. указом Президента РФ от 31 декабря 2015 г.: № 683: по состоянию на 01.02.2018 г.// Справочно–правовая система «Консультант Плюс».

14. «Доктрина информационной безопасности Российской Федерации»: утв. указом Президента РФ от 05 декабря 2016 г.: № 646: по состоянию на 01.02.2018 г.// Справочно–правовая система «Консультант Плюс».

15. «О стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы»: утв. указом Президента РФ от 09 мая 2017 г.: № 2033: по состоянию на 01.02.2018 г.// Справочно–правовая система «Консультант Плюс».

16. «Об утверждении Перечня сведений, отнесенных к государственной тайне»: утв. Указом Президента РФ от 30 ноября 1995г.: № 1203: по состоянию на 02.02.2018 г. // Справочно–правовая система «Консультант Плюс».

17. «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»: утв. указом Президента РФ от 15 января 2013 г.: №31с: по состоянию на 01.02.2018 г.// Справочно–правовая система «Консультант Плюс».

18. Уголовный кодекс Соединенных Штатов Америки: по состоянию на 02.02.2018 г // Справочно-правовая система «World Business Law». URL: http://www.worldbiz.ru/.

19. Уголовный кодекс Японии: по состоянию на 02.02.2018 г // Справочно-правовая система «World Business Law». URL: http://www.worldbiz.ru/

20. Уголовный кодекс Китайской Народной Республики: по состоянию на 02.02.2018 г // Справочно-правовая система «World Business Law». URL: http://www.worldbiz.ru/.

21. Уголовное Уложение Федеративной республики Германия: по состоянию на 02.02.2018 г // Справочно-правовая система «World Business Law». URL: http://www.worldbiz.ru/.

22. Уголовный кодекс Британской Империи: по состоянию на 02.02.2018 г // Справочно-правовая система «World Business Law». URL: http://www.worldbiz.ru/.

23. Уголовный кодекс Франции: по состоянию на 02.02.2018 г // Справочно-правовая система «World Business Law». URL: http://www.worldbiz.ru/

Монографии, учебники, учебные пособия

24. Абов А.И. Преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации/ А.И. Абов. – М.: Прима – Пресс, – 2013. – 25 с.

25. Абов А.И., Велиев Э.Э., Ткаченко С.Н. Экономическая безопасность и компьютерные преступления/ под ред. А.И. Абов, Э.Э. Велиев, С.Н. Ткаченко. – М.: Прима–Пресс, – 2013. – 24 с.

26. Антонян Ю.М. Криминология: учебник для академического бакалавриата / Ю.М. Антонян. – М.: Издательство Юрайт, – 2015. – 388 с.

27. Бессонов В.А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации: автореф. дис... канд. юрид. наук: 12.00.08 / Нижегородский юридический институт МВД РФ. – Нижний Новгород, 2000. – 28 с.

28. Вехов В.Б., Голубев В.А. Расследование компьютерных преступлений в странах СНГ: монография / под ред. Б.П. Смагоринского. – Волгоград: ВА МВД России, 2014. – 304 с.

29. Дашян М.С. Право информационных магистралей: вопрос правового регулирования в сети Интернет. / М.С. Дашян. – М.: Юрлитинформ, 2007. – 150 с.

30. Добровольский Д.В. Актуальные проблемы борьбы с компьютерной преступностью: дис. … канд. юрид. наук: 12.00.08 / Д.В. Добровольский. – М., 2006. – 225 с.

31. Дремлюга Р.И. Интернет–преступность: монография / Р.И. Дремлюга. – Владивосток: Издательсво Дальневост. ун–та, 2008. – 240 с.

32. Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно–телекоммуникационных технологий: монография / М.А. Ефремова. –М.: Юрлитинформ, 2015. – 200 с.

33. Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: дис. ... канд. юрид. наук: 12.00.08 / У.В. Зинина. – М., 2007. – 160 с.

34. Касперский Е.В. Компьютерное зловредство / Е.В. Касперский. – СПб.: Питер, 2012. – 208 с.

35. Кесареева Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: дис. ... канд. юрид. наук: 12.00.08 / Т.П. Кесареева. – М., 2002. – 195 с.

36. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью / В.Е. Козлов. – М.: Проспект, 2016. – 330 с.

37. Копырюлин А.Н. Преступления в сфере компьютерной информации: уголовно–правовой и криминологический аспекты: дис. ... канд. юрид. наук: 12.00.08 / А.Н. Копырюлин. – М., 2007. – 242 с.

38. Лопатина Т.М. Криминологические и уголовно–правовые основы противодействия компьютерной преступности: дис. ... д–ра юрид. наук: 12.00.08 / Т.М. Лопатина. – М., 2006. – 418 с.

39. Малыковцев М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дис. ... канд. юрид. наук: 12.00.08 / М.М. Малыковцев. – М., 2007. – 186 с.

40. Маслакова Е.А. Незаконный оборот вредоносных компьютерных программ: уголовно–правовые и криминологические аспекты: дис. ... канд. юрид. наук: 12.00.08 / Е.А.Маслакова. – М., 2008. – 198 с..

41. Киберпреступность: криминологический, уголовно–правовой, уголовно–процессуальный и криминалистический анализ: монография / И.Г. Смирнова, К.Н. Евдокимов, О.А. Егерева [и др.]; под науч. ред. И.Г. Смирновой. – М.: Юрлитинформ, 2016. – 306 с.

42. Криминология. Особенная часть: учебник для курсантов и слушателей образовательных организаций высшего образования системы МВД России / под общ. ред. Ф. К. Зиннурова. – Казань: КЮИ МВД России , 2016. – 524 с.

43. Смирнов, А. М. Латентная преступность в России: учебное пособие / Смирнов А. М. – Москва: Юрлитинформ, 2013. – 184 с.

44. Суслопаров А.В. Информационные преступления: дис. ... канд. юрид. наук: 12.00.08 / А.В. Суслопаров. – Красноярск, 2007. – 249с.

45. Чекунов И.Г. Криминологическое и уголовно–правовое обеспечение предупреждения киберпреступности: дис. … канд. юрид. наук: 12.00.08 / И.Г. Чекунов. – М., 2013. – 223 с.

46. Шевко Н.Р., Каримов А.М., Турутина Е.Э. Преступления, совершаемые с использованием высоких технологий и коммуникаций / Н.Р. Шевко, А.М. Каримов, Е.Э. Турутина. – Казань: КЮИ МВД России, 2017. – 79 с.

47. Ягудин А.Н. Уголовная ответственность за нарушение правил

эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно–телекоммуникационных сетей: автореф. дис. ... канд. юрид. наук: 12.00.08 / А.Н. Ягудин. – М., 2013. – 27 с.

Статьи, научные публикации

48. Абдусаламов Р.А., Арсланов Ш.Д. К вопросу развития международной практики правового регулирования борьбы с преступлениями в глобальных компьютерных сетях/ Р.А. Абдусаламов, Ш.Д. Арсланов // Вестник Дагестанского государственного университета.– 2016. – № 2.– С. 33 –37.

49. Василенко Н.А. Преступления в сфере информационных технологии / Н.А. Василенко // Старт в науке. – 2017. – № 5. – С. 31–34.

50. Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации / К.Н. Евдокимов // Юридическая наука и правоохранительная практика. – 2016. – № 1(35). – С. 86–94.

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

52. Евдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации / К.Н. Евдокимов // Академический юридический журнал. – 2015. – № 1 (59). – С. 25–26.

53. Згадзай О.Э., Казанцев С.Я. Киберпреступность: факторы риска и проблемы борьбы / О.Э. Згадзай, С.Я. Казанцев //Вестник НЦБЖД. – 2013. – № 4 (18). – С. 80–86.

54. Косенков А.Н., Черный Г.А. Общая характеристика психологии киберпреступника // Криминологический журнал БГУЭП. – 2012. – № 3 (21). – С. 87–94.

55. Мегрелишвили Г.Т. Криминологический и психологический портрет личности преступников в сфере высоких технологий / Г.Т. Мегрелишвили // Вестник Том. гос. ун–та. – 2017. – № 2. – С. 180 – 181.

56. Номоконов В.А. Киберпреступность как новая криминальная угроза /

В.А. Номоконов // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 45–55.

57. Паненков А.А. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности (кибертерроризм) как реальная угроза внешнему и внутреннему контурам национальной безопасности России // Военно–юридический журнал. № 4. – 2014. – С. 3–13.

58. Попов А.Б. Международное сотрудничество государств в борьбе с компьютерной преступностью // Вестник Тамбовского университета. – Т. 84. – № 4. – 2015. – с. 310–313.

59. Родивилин И.П. Проблемы квалификации преступлений в сфере компьютерной информации, совершаемых с использованием дистанционного управления банковским счетом, и их предупреждение / И.П. Родивилин // Пролог. – 2014. – № 2 (6). – С. 61–64.

60. Степанов–Егиянц В.Г. Проблемы разграничения неправомерного доступа к компьютерной информации со смежными составами / В.Г. Степанов–Егиянц // Право и кибербезопасность. – 2014. – № 2. – С. 27–32.

61. Чирков Д.К., Саркисян А.Ж. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны / Д.К. Чирков, А.Ж. Саркисян // Актуальные проблемы экономики и права. – 2013. – № 3. – С. 219–226.

62. Шалагин А.Е. Криминологическое объяснение причин преступности / А.Е. Шалагин // Библиотека криминалиста. Научный журнал. –2017. –№ 2 (31). –С. 176–181.

63. Шевко Н.Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути решения / Н.Р. Шевко // Ученые записки Казанского юридического института МВД России. – 2016. – № 1(1). – С. 13–16.

64. Широков В.А., Беспалова Е.В. Киберпреступность: история уголовно–правового противодействия // Информационное право. – 2006. – № 4. – С. 44–47.

65. Эмиров М.Б., Саидов А.Д., Рагимханов Д.А. Борьба с преступлениями в глобальных компьютерных сетях // Юридический вестник ДГУ. – 2011. – № 2. – С. 63–66.

Эмпирические материалы

66. Приговор Ленинского районного суда по делу № 1–133/14 1–133/2014 от 14 мая 2014 г. // Архив Ленинского районного суда г. Мурманска (Мурманская область). URL: http://sudact.ru. (дата обращения 01.02.2018).

67. Приговор мирового судьи судебного участка № 13 Кировского района г. Перми от 07.12.2015 по уголовному делу № 1– 103/2015.// Архив судебного участка № 13 Кировского района г. Перми. URL: https://rospravosudie.com/court–sudebnyj–uchastok–13–kirovskogorajona–g–permi–s/act–225265116/ (дата обращения: 10.01.2018).

68. Приговор Советского районного суда г. Томска по делу № 1–41/2017 от 16 января 2017 года //Архив Советского районного суда г. Томска. URL: http://sudact.ru. (дата обращения: 10.01.2018)

69. Уголовное дело № 1–26/2014 // Архив Кронштадтского районного суда г. Санкт–Петербурга. – 2014. URL: http://sudact.ru. (дата обращения: 10.01.2018)

70. Уголовное дело № 1–382/2014 // Архив Псковского городского суда Псковской области. – 2014. URL: http://sudact.ru. (дата обращения: 10.01.2018)

71. Уголовное дело № 1–521/2014 // Архив Октябрьского районного суда г. Уфы. – 2014. URL: http://sudact.ru. (дата обращения: 10.01.2018)

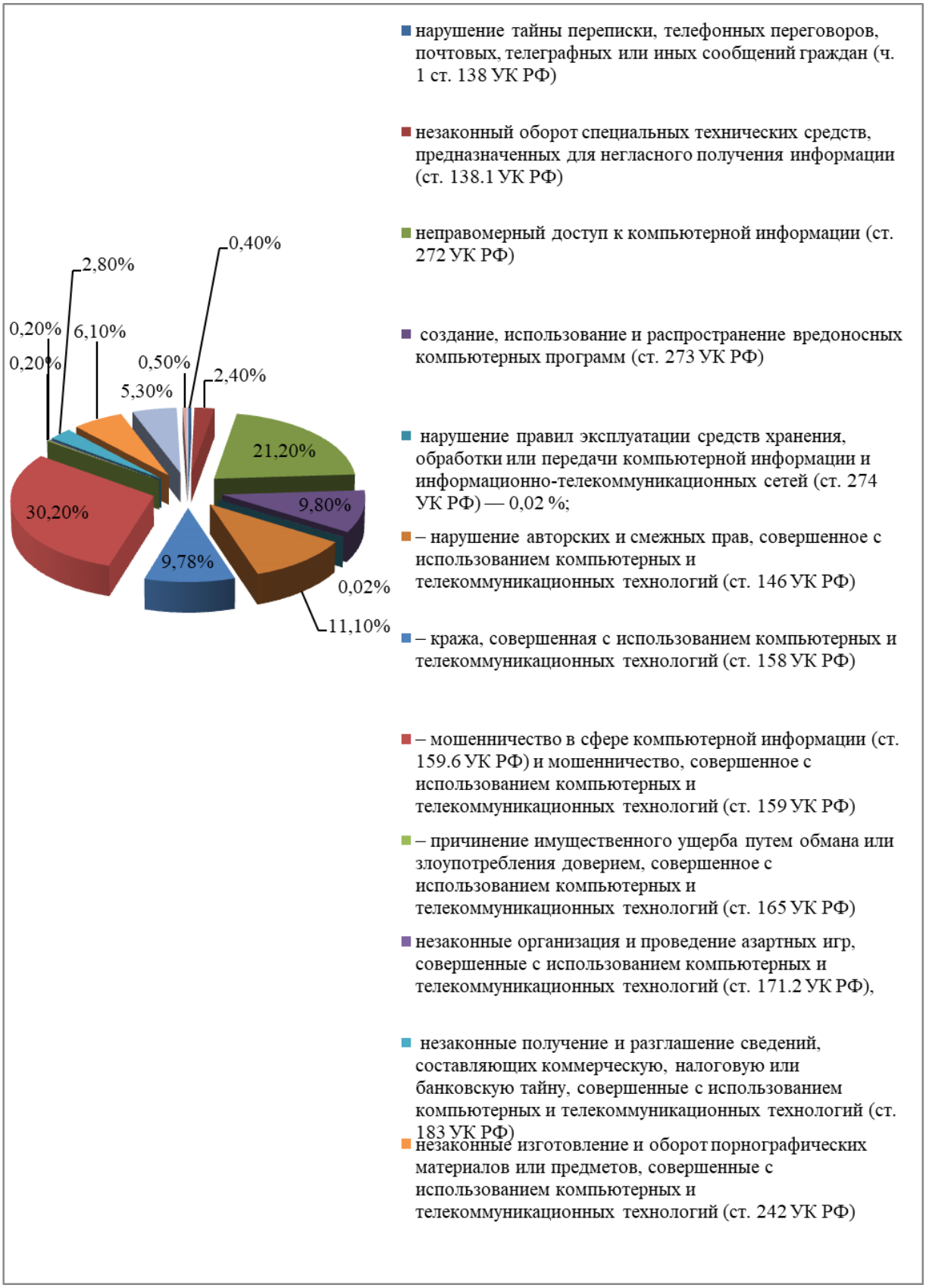
Справочная литература

72. Обзор киберпреступности за 2016 год. URL: http://www.pwc.ru/ru/ res2016.pdf (дата обращения: 10.01.2018).

73. Сводный сборник состояния преступности в России за январь – декабрь 2009–2017 г. URL: http://mvd.ru (дата обращения: 03.04.2018).

Приложение 1

Структура преступности в сфере компьютерной информации



Приложение 2

Уголовная ответственность за преступления в сфере компьютерной информации в зарубежном законодательстве

США	В 1984 г. был принят Закон о мошенничестве и злоупотреблении с использованием компьютеров – основной нормативно–правовой акт, устанавливающий уголовную ответственность за преступления в сфере компьютерной информации. В последующем он неоднократно (в 1986, 1988, 1989, 1990, 1994 и 1996 гг.) дополнялся. Нынче он включен в виде §1030 Титула 18 Свода законов США, которая предусматривает уголовную ответственность за: - компьютерный шпионаж, состоящий в несанкционированном доступе или превышении санкционированного доступа к информации, а также получение информации, имеющее отношение к государственной безопасности, международным отношениям и вопросам атомной энергетики (§1030 (a)(1)); - несанкционированный доступ или превышение санкционированного доступа к информации из правительственного ведомства США, из какого бы то ни было защищенного компьютера, имеющего отношение к межштатной или международной торговле, а также получение информации из финансовых записей финансового учреждения, эмитента карт или информации о потребителях, содержащейся в файле управления учета потребителей (§1030 (a)(2)); - воздействие на компьютер, находящийся в исключительном пользовании правительственного

	ведомства США, или нарушении функционирования компьютера, используемого полностью или частично Правительством США (§1030 (a)(3)); - мошенничество с использованием компьютера - доступ, осуществляемый с мошенническими намерениями, и использование компьютера с целью получения чего бы то ни было ценного посредством мошенничества, включая незаконное использование машинного времени стоимостью более 5 тысяч долларов в течении года, т.е. без оплаты использования компьютерных сетей и серверов (§1030 (a)(4)); - умышленное или по неосторожности повреждение защищенных компьютеров (§1030 (a)(5)); - мошенничество путем торговли компьютерными паролями или аналогичной информацией, позволяющей получить несанкционированный доступ к информации, если такая торговля влияет на торговые отношения между штатами и с другими государствами, или на компьютер, используемый правительством США (§1030 (a)(6)); - угрозы, вымогательство, шантаж и другие противоправные деяния, совершаемые с использованием компьютерных технологий (§1030 (a)(7))
Великобритания	С августа 1990 г. вступил в силу Закон о злоупотреблениях компьютерами. В соответствии с ним к уголовно наказуемым деяниям относятся: – умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам (ст. 1); – умышленный противозаконный доступ к компьютеру или

	содержащимся в нем компьютерной информации или программам для их последующего использования в противозаконных целях (ст. 2); – неправомерный доступ к компьютерной информации на машинном носителе, в компьютере, компьютерной системе или сети, с целью, или если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушения работы компьютера, компьютерной системы или сети (ст. 3).
Германия	В Германии встал вопрос о закреплении уголовной ответственности за преступления в сфере компьютерной информации в УК уже в 1986 г. (по данным статистики в 1987 г. было зарегистрировано 3355 таких преступлений, а в 2002 г. – уже 57 488). Эти составы преступлений были введены «Вторым законом о борьбе с экономической преступностью» в УК ФРГ 1 августа 1987 г. В Уголовном кодексе Германии не существует специального раздела, посвященного компьютерным преступлениям (преступлениям в сфере компьютерной информации); нормы, содержащие ответственность за преступления в сфере компьютерной информации рассредоточены по разделам Особенной части кодекса: – § 263 а компьютерное мошенничество (Compu–terbetmg); –§ 269 фальсификация данных, имеющих доказа–тельственное значение (Falschung beweiserhe–blicher Daten); – § 270 обман при помощи ЭВМ при обработке данных (Tauschung in Rechtsverkehr bei Daten–verarbeitung); – § 303a изменение данных (Datenveranderung); – § 303b компьютерный саботаж (Computer–sabotage).

Япония	Среди законодательных актов Японии, регулирующих правонарушения в сфере информационных технологий, является Уголовный кодекс и Закон «О несанкционированном проникновении в компьютерные сети», принятый 3 февраля 2000 г. Также имеются специальные законы. В Законе «О несанкционированном проникновении в компьютерные сети» установлена ответственность за: – незаконное (несанкционированное) проникновение в компьютерные системы и информационные сети с целью кражи, порчи информации, ее использование с целью извлечения дохода и причинение ущерба законным владельцам сетей, систем и информационных баз данных. В УК Японии имеются следующие составы преступлений в сфере компьютерной информации: – внесение неверных записей в официальный документ; – распространения сфальсифицированного официального документа; – уничтожение государственных и частных документов; – вывод из строя ЭВМ; – уничтожение или модификация информации на электромагнитных носителях, совершенные в целях воспрепятствования ведения предпринимательской деятельности; – компьютерное мошенничество.
Франция	В УК Франции предусмотрена ответственность за преступления, посягающие на системы автоматизированной обработки данных, такие как: – незаконный доступ к автоматизированной системе

	обработки данных или незаконное пребывание в ней (ст. 323–1); – воспрепятствование работе или нарушение работы системы (ст. 323–2); – ввод обманным путем в систему информации, а также изменение или уничтожение содержащихся в автоматизированной системе данных (ст. 323–3). – осуществление или отдача указания об осуществлении автоматизированной обработки поименных данных без осуществления предусмотренных в законе формальностей (ст. 226–16); – осуществление или отдача указания об осуществлении обработки этих данных без принятия всех мер предосторожностей, необходимых для того, чтобы обеспечить безопасность данных (ст. 226–17); – сбор и обработка данных незаконным способом (ст. 226–18); – ввод или хранение в памяти ЭВМ запрещенных законом данных (ст. 226–19); – хранение определенных данных сверх установленного законом срока (ст. 226–20); – использование данных с иной целью, чем это было предусмотрено (ст. 226–21); – сбор или передача содержащейся в памяти ЭВМ или картотеке информации иностранному государству, уничтожение, хищение, изъятие или копирование данных, носящих характер секретов национальной обороны, содержащихся в памяти ЭВМ или в картотеках (ст.ст. 411–7, 411–8, 413–9, 413–10, 413–11).