Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет Юридический
Кафедра Уголовного права
Направление подготовки 40.03.01 – Юриспруденция

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____Т.Б. Чердакова
«_____»_____2017 г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Преступления в сфере компьютерной информации: уголовно правовой и криминалогический аспекты

Исполнитель
студент группы 321об 3 _____ А.А. Симонов
(подпись, дата)

Руководитель
доцент, канд. юрид. наук _____ Т.П. Бутенко
(подпись, дата)

Нормоконтроль _____ Н.С.Архипова
(подпись, дата)

Благовещенск 2017

СОДЕРЖАНИЕ

РЕФЕРАТ

Бакалаврская работасодержит 58с., 69источников.

ИНФОРМАЦИОННАЯ БЕЗОПАСТНОСТЬ, НЕПРАВОМЕРНЫЙ ДОСТУП, КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ, ИНФОРМАЦИЯ, ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ, БЕЗОПАСНОСТЬ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.

В работе исследованы преступления в сфере компьютерной информации уголовно правовой и криминалогический аспекты.

Цель исследования – провести анализ преступлений в сферекомпьютерной информации как с точки зрения уголовно правового подхода, так и с точки зрения криминалогического.

Методологическую основу работы составляют теоретические методы такие как, анализ и обобщение научной, учебной и монографической литературы.

В бакалаврской работе рассматриваются особенности преступлений в сфере компьютерной информации.Особое внимание уделеноуголовно правовому анализу преступлений в сфере компьютерной информации, характеристики личности компьютерного преступника, мерам попредупреждению компьютерной преступности, а также статистическимисследованиям судебной практики.

ВВЕДЕНИЕ

На сегодняшний день в мире информационные технологии и Интернет твердо входят в повседневную жизнь, в корне меняя то, как люди осуществляют коммуникации, получают и обрабатывают информацию, развлекаются, осуществляют покупки товаров и т.д. Интернет не то чтобы нужен, он необходим современному, динамично развивающемуся информационному обществу[1]. Электронно-вычислительная техника это одно из главных достижений научно-технической мысли. Данное достижение привнесло неоценимую пользу и вклад в развитие техники, науки и иных отраслей знаний.Однако выгоды, которые можно получить благодаря использованию этой техники, стали использоваться и в преступных целях. Именно так появился новый вид преступной деятельности – компьютерные преступления, общественно – опасные последствия, от совершения которых не шли ни в какое сравнение с ущербом от других преступлений[2].

Проблемы, связанные с информационной безопасностью довольно часто усугубляются процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и прежде всего вычислительных систем. Об актуальности данной проблемы свидетельствует достаточно широкий перечень возможных способов компьютерных преступлений.

Уголовная политика в сфере борьбы и противодействия компьютерным преступлениям должна нести в себе не только правовые, но и экономические, социальные, организационные и иные меры. Закрепившись в традиционной для нас форме политика государственного принуждения должна дополняться повышением правовой и общей культуры граждан, их правосознания, деятельностью государственных органов направленных на предупреждение компьютерных преступлений.

---

[1] Степанов-Егиянц, В. Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями. / В.Г. Степанов-Егиняц // Российский следователь. 2012. № 24. С. 34.

[2] Широков, В. А. Беспалова, Е. В. Компьютерные преступления: основные тенденции развития. / В.А. Широков // Юрист. 2006. № 10. С. 18.

Важность данной проблемы состоит в том, что компьютерная преступность становится одним из наиболее опасных видов преступных посягательств. К сожалению, мы не хотим этого замечать, и думаем, что данные противоправные деяния не несут в себе большую опасность.

Объектом исследования являются общественные отношения, которые подвергаются посягательствам в результате неправомерного доступа к компьютерной информации. Предмет исследования содержит в себе уголовно-правовые и криминологические аспекты преступлений в сфере компьютерной информации, а также совокупность мер по предупреждению преступлений в сфере компьютерной информации.

Цель данной работы –выработка всесторонней стратегии по профилактике и борьбе с компьютерной преступностью, и формулирование предложений повышения эффективности контроля над компьютерной преступностью в России, а также анализ законодательства об уголовной ответственности за компьютерные преступления.

Для достижения поставленной цели следует решить ряд задач, а именно:

- В полной мере изучит понятие компьютерной преступности, а также ответственность за компьютерные преступления;

- изучить опыт борьбы с компьютерными преступлениями в России и за рубежом;

- провести всесторонний анализ законодательства о компьютерных преступлениях;

- дать характеристику компьютерной преступности;

- дать характеристику личности преступника.

Для того чтобы в полной мере изучить проблемы, связанные с объектом исследования работе использовались следующие методы:

- анализ нормативно-правовой документации в рамках темы работы;

- анализ и изучение литературы;

- изучение и обобщение отечественной и зарубежной практики.

1 ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1 Понятие и виды преступлений в сфере компьютерной информации

В наше время существуют различные точки зрения по поводу понятия компьютерных преступлений и их классификации. Сформулировать понятие компьютерная преступность довольно сложно и связанно это, прежде всего с тем, что отсутствует возможность реального закрепления общего объекта преступного посягательства. Вторая причина состоит в множественности предметов преступного посягательства[3].

Выделяют два основных взгляда на данную проблему. Одни исследователи говорят, чтокомпьютерные преступления это такие действия, в которых компьютер является либо объектом, либо орудием посягательств. При этом, в частности, кража компьютеров или их компонентов рассматривается как один из случаев совершения компьютерных преступлений[4]. Эта точка зрения сформировалось довольно давно, и имела широкое распространение, сейчас же многие ученные придерживаются точки зрения о том что, компьютерные преступления это противозаконные действия в сфере автоматизированной обработки информации. Они выделяют в качестве главного классифицирующего свойства, позволяющего отнести эти преступления в обособленную группу, общность способов, объектов посягательств, орудий. Следовательно, объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер в свою очередь служит орудием посягательства[5].

Термин «компьютерная преступность» существует в России достаточно долгое время, появление термина связывают с внедрением в различные сферы жизнедеятельности компьютерной техники.

---

[3] Логинов, А. Б. Компьютерные преступления: способы совершения, методики расследования / А. Б. Логинов // М.: Юрид. Лит., 2000. С. 10.

[4] Исследователи компьютерных преступлений. URL: http://www.viruslab.ru (дата обращения 27.05.2017).

[5] Курушин, В.Д. Компьютерные преступления и информационная безопасность. / В. Д. Куршин // Справочник. М.: Новый юрист, 2004. С. 65.

Закрепление в законодательстве преступлений в сфере компьютерной информации произошло лишь с введением в действие Уголовного кодекса Российской Федерации в 1996 году, где появилась отдельная глава, 28 "Преступления в сфере компьютерной информации" которая содержит три статьи: "Неправомерный доступ к компьютерной информации" (ст. 272), "Создание, использование и распространение вредоносных компьютерных программ " (ст. 273) и "Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей " (ст. 274)[6].

С этого момента подавляющее большинство авторов включает в понятие "компьютерная преступность" лишь названные составы преступлений, определяя при этом компьютерную преступность как совокупность преступлений, посягающих на информационную безопасность с использованием компьютерных средств[7].

Статья 271 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации, если это повлекло уничтожение,блокирование, модификацию либо копирование информации. Неправомерный доступ к охраняемой законом компьютерной информации выражается в самовольном получении информации без разрешения владельца или собственника, а также неправомерность выражается в нарушении установленного порядка доступа к этой информации.Если нарушен установленный порядок доступа к охраняемой законом информации, согласие ее собственника или владельца не исключает неправомерности доступа к ней.

Собственником являетсясубъект, который в полной мере реализует право владения, пользования и распоряжения информационными ресурсами, информационными системами и технологиями.

Субъект, обращающийся к информации, будет являться пользователем информации.

---

[6] Уголовный кодекс Российской Федерации 13.06.1996 г. № 63-ФЗ (ред. от 17.04.2017) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

[7]Мерзогитова, Ю. А. Понятие компьютерной преступности. / Ю. А. Мерзогитова // Вестник МВД России, 2001. № 5 - 6. С. 84.

Статья 2 Закона«Об информации, информатизации и защите информации» закрепляет понятие информации и согласно данному закону это - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.[8]. Жесткие диски, флэш-карты, (дискеты) и компакт-диски позволяют переносить программы и документы с одного компьютера на другой, хранить информацию, не используемую постоянно на компьютере, делать архивные копии информации, содержащейся на жестком диске. Понятие «компьютерная информация» закрепленов примечании к статье 272 УК РФ этосведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Неправомернымследует признать доступ в закрытую информационную систему лица, не являющегося законным пользователем либо не имеющего разрешения для работы с данной информацией.[9]

Выделяют следующие способы доступа к информации: модификация программного и информационного обеспечения, использование чужого логина(имени пользователя), изменение физических адресов технических устройств в результате системной поломки компьютера, установка аппаратуры записи, подключаемой к каналам передачи данных, и т.д.

Обязательный элемент объективной стороны данного преступления является –последствия:

Модификация информации - это внесение изменений в компьютерную информацию (или ее параметры).

Копирование информации —этосоздание копий файлов и системных областей дисков.

Блокирование информации - это создание препятствий к свободному доступу; при этом следует учитывать, что информация не подвергается уничтожению.

Уничтожение информации выражается в удалении файла без технической

[8] Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и защите информации" (ред. от 19.12.2016) // Собрание Законодательства РФ. 2006. № 31 (ч. I). Ст. 2.
[9] Скоромников, К.С. Компьютерное право Российской Федерации. / К. С. Скоромников. М.: Проспект, 2000. С. 200.

возможности восстановления[10].

Преступление считается оконченнымс момента осуществления неправомерного доступа к информации, повлекшего ее уничтожение, модификацию, блокирование, либо копирование.

С субъективной стороны данноепреступление характеризуется толькоумышленнойформой вины. По отношению к действию умысел может быть только прямым, о чем свидетельствует то, что законодатель использует термин "неправомерный", а к факту наступления последствий — как прямым, такикосвенным.

Субъектомпреступления, по ч. 1 ст. 272 УК РФ, могут быть лица, достигшие к моменту совершения преступления 16 летнего возраста, в том числе и законный пользователь, который не имеет разрешения для работы с информацией определенной категории.Часть3 ст. 272 УК РФ предусмотрена ответственность за преступление, совершеноегруппойлицпопредварительномусговоруилиорганизованной группой,либо лицом сиспользованием своего служебного положения.

Неправомерный доступ может осуществляться разнообразными способами:

-соединение с компьютером, подключенным к телефонной сети, путем автоматического перебора абонентских номеров (внедрение в чужую информационную систему посредством "угадывания кода"),

-использование чужого имени пользователя, использование информации, которая сохранилась после решения задач,

-использование ошибок в логике построения программы или провоцирование ошибок соединения, вычисление слабых мест в защите автоматизированных систем,

- установка аппаратуры , подключаемой к каналам передачи данных,

- и т.д.[11]

[10] Котов, Н. И. Комментарий к Уголовному кодексу Российской Федерации: научно-практический (постатейный). / Н. И. Котов. М.: Юрайт-Издат, 2012.

Самым распространенным способом неправомерного доступа является вычисление слабых мест в защите автоматизированных систем. Как правило, системы не обладающие средствами аутентичной идентификации т.е по сетчатке глаза, по отпечаткам пальцев, голосу, паролю и т.д, беззащитны против этого способа преступления.

Преступникам остается лишь получить коды или другие идентифицирующие шифры пользователей и совершить задуманное.

Делается это обычно путем подкупа персонала обладающего нужной информацией, путем установления прослушивания телефонных линий, а также завладения информацией вследствие ненадлежащего контроля, за её сохранностью[12].

Для обеспечения защиты от неправомерного доступа необходимо обладать широким спектром знаний и всесторонней подготовкой по вопросам информационно безопасности.

Статья 273 УК РФ предусматривает ответственность за 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.

Объективная сторона выражается в осуществлении таких действий как-создание программ, предназначенных для несанкционированного:

- уничтожения,

- блокирования,

- модификации,

- копирования компьютерной информации или нейтрализации средств ее защиты.

В распространении таких программ или машинных носителей с такого рода программами, а также использование таких программ или машинных но-

[11] Мосин, О. В. Компьютерная преступность в России. Как с ней бороться. [Электронный ресурс]. URL: http://samlib.ru /№ewsd/2317/ (дата обращения 27.05.2014)

[12] Дорохов, Р. В. Компьютерная преступность. / Р. В. Дорохов // «ComputerLawandSecurity». Москва 2011. № 32. С. 2.

сителей с ними (в обыденном словоупотреблении такие программы обычно называют вирусами)[13].

Опасность вируса состоит в том что он как правило приводит к абсолютному разрушению системы компьютерной информации.

Разрушение может произойти не сразу, специалисты в области компьютерной информации отмечают, что сам вирус может быть долгое время в состоянии «покоя», а затем привести к дезорганизации. Иногда у обыденного числа населения складывается мнение, что вирусы в основном используют для уничтожения, блокирования, модификации, копирования компьютерной информации частных лиц. Но в последнее время вирусы все чаще используются для уничтожения, блокирования, модификации, копирования компьютерной информации в таких наиболее важных областях как оборона страны, государственная безопасность и т.д.

Объектом рассматриваемого состава преступления является общественная безопасность и общественный порядок, а также совокупность общественных отношений по безопасному использованию компьютерной информации.

Следует заострить внимание на то, что в ч. 3 ст. 273 УК РФ предусмотрен квалифицирующий признак состава преступления, а именно такой как наступление тяжких последствий или создание угрозы их наступления. Если в случае совершения преступления наступают тяжкие последствия, то данный квалифицированный состав будет материальным, ну а если только создана угроза наступления последствий, то состав будет усеченным[14].

Создание и распространение вредоносных программ (вирусов) понимается как преднамеренное, а также без санкций конкретных лиц воздействие вирусов.

Использование программы это распространение, воспроизведение, а также иные действия направленные на введение данной программы в оборот.

---

[13]Здравомыслов, Б. В. Уголовное право РФ. Особенная часть: учебник / под ред. проф. Б. В.Здравомыслова. — 2-е изд., перераб. и доп. М.: Юристъ, 2012. С. 22.

[14] Методические рекомендации по осуществлению надзора за исполнением законов при расследовании в сфере компьютерной информации. [Электронный ресурс]. URL: http://www.advodom.ru/practice/ (дата обращения 02.03.2015).

Распространениепрограммзаключается в предоставлении доступа к воспроизведенной в какой-либо материальной форме программе, путем передачи по сети, путем продажи, проката и т.д.

Преступление считается оконченным с момента, когда лицо совершает действия, которые указаны в диспозиции статьи.

Субъектом преступления могут быть лица, достигшие к моменту совершения преступления 16 летнего возраста.

С субъективной стороны преступление, предусмотренное ч. 1 статьи 273 УК РФ, характеризуется виной в форме прямого умысла, о чем свидетельствует указание законодателя на заведомый характер деятельности виновного.

Основываясь на всем изложенном выше можно сделать небольшой вывод том что, при всем многообразии программ по защите от несанкционированного доступа от него невозможно защититься на все 100%. Необходимо разрабатывать методики и рекомендации по противодействию данному виду преступлений. И это даст примерно 80% защиты от данного вида преступления. Как было отмечено выше, на 100 % защититься не возможно, так как буквально каждую минуту компьютерные преступники (хакеры) разрабатывают новые способы совершения данного вида преступления[15].

Статья 274 УК РФ предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.Для того чтобы привлечь лицо к уголовной ответственности поданной статье необходимо установить, какие именно правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации были нарушены.

Под правилами эксплуатации глобальных сетей понимаются нормативные акты, регламентирующие работу данной сети, в частности Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»[16], который регламентирует порядок создания и подключения к информационно-телекоммуникационной сети Ин-

[15] Кириченко, А. Н. Вирусы научились размножаться по своим законам. / А. Н. Кириченко // МН Коллекция. 2009. №2. С. 12.

[16] Федеральный закон от 07.07.2003 N 126-ФЗ» "О связи" (ред. от 17.04.2017) // Собрание законодательства Российской Федерации. 1995. № 8. Ст. 20.

тернет. А также иные нормативно-правовые акты, устанавливающие правила эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекомуникационнных сетей. Например, временные санитарные нормы и правила для работников вычислительных центров, техническая документация на компьютерную техникуи т.д.

Нарушаются императивные положения правил, которые запрещают совершать определенные дейсвтия.

Норма ст. 274 является бланкетной и отсылает к конкретным нормативным и нормативно-техническим актам, а также инструкциям, регламентам и правилам, устанавливающим порядок работы с информационно телекоммуникационных сетями и оконечным оборудованием в ведомстве или организации.

Субъективная сторона данного преступления выражается в вине в форме умысла.

Субъектомпрестуления является лицо, которое в силу должностных обязанностей имеет доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно телекоммуникационным сетям и оконечному оборудованию, а также к информационно-телекоммуникационным сетям и обязано соблюдать установленные для них правила эксплуатации[17].

Исходя из вышеизложенного, можно сделать логичный вывод о том, что преступления в сфере компьютерной информации закреплены в главе 28 УК РФ, а компьютерные преступления представляют собойсовокупность преступлений, посягающих на информационную безопасность с использованием компьютерных средств.

1.2 Зарубежный опыт борьбы с компьютерными преступлениями

В зарубежных странах с выскоим уровнем компьютеризации компьютерная преступность уже давно стала одной из первостпенных.

Данная преступность стала настоящим бичом экономик развитых

[17]Коликов,, Н. Л. Причины и условия профессиональной компьютерной преступности. / Н. Л. Коликов // Вестник ЮУрГУ. 2011. № 19. С. 30.

государств[18].

Так, например, 90% фирм и организаций в Великобритании в разное время становились объектами электронного пиратства или находились под его угрозой.

В Нидерландах жертвами компьютерной преступности стали 20% различного рода предприятий[19].

В ФРГс использованием компьютеров ежегодно похищается 4 млрд. евро, а во Франции – 1 млрд. евро[20].

В США ежегодно экономические убытки от такого рода преступлений составляют около ста миллиардов долларов.

В таких государствах как: США, Япония, Великобритания, Канада, Германия, общество и в том числе государственные органы уже достаточно давно осознали степень и характер угрозы, которая исходит от компьютерных преступлений, и разработали эффективную систему борьбы с ними, которая содержит как законодательные, так и организационно-правовые меры.

Среди законодательных актов Японии, регулирующих правонарушения в сфере информационных технологий, следует выделить Уголовный кодекс и Закон «О несанкционированном проникновении в компьютерные сети», принятый 3 февраля 2000 г. В отличие от Великобритании и США, Японское законодательство и его система ближе к нашему. Значительное отличие выражается в том, что нормы уголовного права находятся не только в Уголовном кодексе Японии. По некоторым вопросам, компьютерной преступности, приняты специальные законы.

В Законе «О несанкционированном проникновении в компьютерные сет » названы такие преступления, как незаконное (несанкционированно) проникновение в компьютерные системы и информационны сети с целью кражи, порчи информаци , ее использование с целью извлечения доход и

[18] Дорохов, Р. В. Компьютерная преступность. / Р. В. Дорохов// «ComputerLawandSecurity». М. 2011. №32. С.2.
[19] Там же. С. 6.
[20]Тропина, Т. В. Самоурегулирование и сорегулирования в борьбе с Киберпреступностью и обеспечения Кибербезопасности. / Т. В.Тропина // В: JahnkeAl. (ред.), Дункер&Humblot, Берлин. 2012. С. 56-57.

причинение ущерба законным владельцам сете , систем и информационных баз данных[21].

В Уголовном кодексе Японии содержаться некоторое количество составов преступлений, предметом которых являются запис на электромагнитном носителе. В частности, ним относится внесение неверных записей официальный документ[22].Данное преступление включает себя действия по совершению незаконных записе на электромагнитном носителе, являющемся оригиналом официальног документа. Дело в том что Японии в рамках E-Government (Электронног правительства) интенсивно развилась система электронного документооборот , и большинство документов, в том числ и официальные, существуют как правило тольк в электронном виде.

Отсюда и формулировк состава - совершение незаконных записей на электромагнитно носителе, являющемся оригиналом официального документа.

Аналогичн предметом других преступленийраспространения сфальсифицированного официальног документа, уничтожения государственных и частных документо - является запись на электромагнитном носителе. самостоятельный состав выделен вывод из стро ЭВМ, уничтожение или модификация информации н электромагнитных носителях, совершенные в целях воспрепятствовани ведения предпринимательской деятельности. В УК Япони в самостоятельный состав выделяется компьютерное мошенничеств .

В Великобритании ответственность за компьютерные преступления закреплена в статута , принятых Парламентом.

Выделяют две основные группыстатуты, устанавливающие ответственност за компьютерные преступления (собственно computer crim), и статуты, устанавливающие ответственность за преступлени , связанные с использованием Интернета (internet-relate crime). Термин computer crime употребляется лиш в доктрине, в законодательстве же применяетс термин

[21] Закон Японии «О несанкционированном проникновении в компьютерные сети».от 03.02.2000. (ред. от 08.09. 2004) / СПб: Юридичесикй центр Пресс, 2012.
[22] Уголовный кодекс Японии от 12.05.1995. (в ред. от 02.03.2002) / СПб: Юридический центр Пресс, 2012.

computer misuse[23].

Такой термин ка «misuse» дословно переводится как «неправильное употреблени », «злоупотребление». Во многих российских источниках названи закона, в котором употребляется этот терми , - Computer Misuse Act 1990 - переводится как Зако о злоупотреблении компьютером.

К статутам, регулирующим правонарушения в информационно сфере, можно отнести, наряду с Законо о злоупотреблении компьютером 1990 г. (Computer Misus Act 1990), Закон о телекоммуникациях (обман) 1997 . (Telecommunications (Fraud) 1997), Законоданных 1998 г. (ProtectionAct 1998)[24].

Законодательство США в област борьбы с преступлениями в сфере компьютерно информации значительно отличается от законодательства стра Европы. Главная и наиболее основная особенност выражается в том, что в юриспруденци США нет общего понятия компьютерного преступлени . Однако, Свод законов США содержит множеств статей, посвященных борьбе с преступлениями использованием компьютера. Рассмотрим наиболее важные и них.

В США ответственность за компьютерны преступления устанавливается на двух уровнях - н федеральном и на уровне штатов. Н уровне федерации все компьютерные преступления включен в § 1030 Титула 18 Свода законов США[25]. штатах принимаются отдельные законы, по вопроса компьютерной преступности.

Первым свой закон приня , штат Флорида в 1978г он устанавливал ответственност за модификацию, уничтожение и несанкционированный досту к компьютерной информации.

В штате Техас в 1985 г. принят Закон о компьютерны преступлениях (Texas Computer Crimes Law), п которому наказывалось незаконное

[23] Яблоков, Е. А. Правовое регулирование борьбы с компьютерной преступностью в США / Е. А. Яблоков // Криминологический журнал. М.: 2002. С. 52.
[24]Компютерные преступления в США. [Электронный ресурс]. URL: http://www/securitylab/ru (дата обращения 26.05.2017).
[25] Свод законов США 1989г. § 1030 Титул 18. (ред. от 08.02 1997) / СПб: Юридический центр Пресс, 2012.

использование компьютерной информации[26].В всех перечисленных трех странах в отдельны составы выделены такие преступления, которы не предусмотрены в гл. 28 УК Р .

Такнапример в главе XXXVII УК Японии предусмотреннас . 246.2 «Компьютерное мошенничество». Которая устанавливает, что «любо лицо, изготавливающее фальшивые электромагнитные записи, свидетельствующи о приобретении, изменении или потере имущественны прав, путем внесения в компьютер, используемы в деловых операциях иным лицом, ложны сведений или командназываетс лишением свободы с обязательным привлечением труду на срок до 5 лет»[27].

Российской Федерации же данные действия квалифицируютс по совокупности преступлений ст. ст. 272 159 УК.

В параграфе 1030 (a) (4), Свода законо США мошенничество с использованием компьютера понимаетс как доступ, осуществляемый с мошенническими намерениям , и использование компьютера с целью получени чего бы то ни было ценног при помощи мошенничества[28].

Также следует заострить внимание, на точто именно такие государства как США и Германия, одни из первых начали заниматься вербовкой «хакеров»работающих на дому. Данная вербовка была неофициальной и «хакеры»не являлись официальными сотрудниками в отделах по борьбе с компьютерными преступлениями. Это делалось по одной простой причине, в отдела по борьбе с данными преступлениями, сотрудники были не достаточно «подкованы» и подготовлены для выявления и предупреждения компьютерных преступлений.

Но данный способ был достаточно не безопасным, так как«хакеры» могли соглашаться работать в отделах по борьбе с компьютерными преступлениями, только ради своей выгоды, так как могли получить доступ к секретам и данным

[26]TexasComputerCrimesLaw 1985 г. [Электронный ресурс].URL: http://ruponia.livejournal.com (дата обращения 25.05.2017).
[27] Уголовный кодекс Японии от 12.05.1995. (ред. от 02.03.2002) / СПб: Юридический центр Пресс, 2012.
[28]Цирлов, В. Л. Основы информационной безопасности автоматизированных систем. / В. Л. Цирлов // Закон. М., 2008. С 28.

которыми располагает государство..

Исходя из вышеизложенного, можно сделать логичный вывод о том, что в зарубежном законодательстве большое количество составов компьютерных преступлений, которых нет в российском уголовном праве. Само собой нельзя слепо скопировать зарубежный опыт. Однако определенные составы, которые предусмотренны в зарубежном законодательстве, к примеру, компьютерное мошеничество, при внесении определенных корректировок, возможно включить в Уголовный кодекс Российской Федерации.

2 УГОЛОВНО-ПРАВОВОЙ АНАЛИЗ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬТЕРНОЙ ИНФОРМАЦИИ

2.1 Уголовная ответственность за неправомерный доступ к компьютерной информациии

С того момента как в Уголовный Кодекс Российской Федерации была введена статья устанавливающая ответственность за неправомерный доступ компьютерной информации (ст.272), прошло достаточно много времени. И само собой законодательобнаружил некоторые недостатки.

Для того чтобы ликвидировать недостатки, был принят Федеральный закон №420 от 7 декабаря 2011 года « внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации[29].

Предыдущая редакция статьи содержала всего две части, новая редакция расширила статью до четырех частей, а также включило приложение, в котором предусматривается определение компьютерной информации.

Ученые не раз высказали мнение о том что, существует необходимость закрепления в законодательство понятия «компьютерная информация»[30].

На данный момент законодатель не связывает компьютерную информацию к машинному носителю, электронно-вычислительной машине (ЭВМ), системе ЭВМ или и сети.

Следовательно, под защитой уголовного закона находится компьютерная информация, которая еще не зафиксированная на каком-либо устройству либо носителе, а пребывает в процессе передачи.

Само собой это увеличило сферу приминения статьи 272 УК РФ. Но нужно учитывать что информация, которая передается по беспроводным каналам не может быть объектом попадающим под уголовно-правовую охрану

[29] Федеральный закон от 07.12.2011 № 419-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации" // Парламентская газета. 2011. 16-22 дек. № 55-56. С. 37-43.

[30] Бражник, С. Д. Преступления в сфере компьютерной информации: проблемы законодательной техники.дис. ... канд. юрид. наук / С. Д. Бражник. Ижевск. 2009. С. 65.

так как с точки зрения физики не попадает под понятие «электрически сигнал». Исходя из этого сам термин «электрический сигнал» приводит к заблуждению и требует тщательного разъяснения.

Неправомерный доступ к охраняемой законом компьютерной информации выражается как уже отмечалось в первой главе в самовольном получении информации без разрешения владельца или собственника, а также неправомерность выражается в нарушении установленного порядка доступа к этой информации. Непосредственный объект преступления - общественные отношения, складывающиеся по поводу поддержания общественной безопасности путем обеспечения конфиденциальности, целостности и доступности компьютерной информации.

Субъективная сторона неправомерного доступа к компьютерной информации выражается в вине в форме умысла или неосторожности, Субьектом преступления является лицо, достигшее возраста 16 лет.

Ответственность за неправомерный доступ к охранемой законом информации, если данное деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации закреплена в части первой статьи 272 УК РФ. Сам термин «доступ» рассматривается с двух аспектов: как состояние .е последствие дейсвтий, а также как процесс т.е непосредственно действия. Доступ становится неправомерным, только тогда когда лицо, не имеет права доступа к «компьютерной информации».

Лицо привлекается к уголовной ответственности и в случае неправомерного доступа-состояния, так и в случае неправомерного доступа-процесса. Уничтожением является: воздействие на компьютеную информацию, и вследствие данного воздействия теряется возможность ее дальнейшего использования кем то. Подлежит информация восстановлению или же не подлежит, никакого значения не имеет. Блокированием является ограничение доступа полное либо частичное к компьютерной информации. Модификация определяется как внесение существенных изменений. Копирование понимается как запись или же воспроизведение охраняемой компьютерной информации на

носитель, отличающийся от изначального[31].

Наиболее распространенными мотивами совершения компьютерных преступлений являются: корыстные соображения.

В качестве примера можно привести судебное решение по уголовному делу.

25.03.2017 около 12 часов 29 минут Васильев находясь в здании ПАО «Сбербанк России», расположенного по адресу: <адрес>, нашел на столе у компьютера два бумажных фискальных чека, оставленных ранее незнакомой ему ФИО5, на которых содержалась информация о номере ее банковской карты № *********№, логине и пароле к ней, с помощью которых можно было получить доступ к лицевому счету данной банковской карты и информацию о денежных средствах, находящихся на данном лицевом счете и остальных счетах (вкладах) ФИО5. После этого у Васильева возник умысел на тайное хищение денежных средств, находящихся на счетах в ПАО «Сбербанк России», принадлежащих ФИО5. Преступник преследовал одну цель обогатиться. Мотив очевиден корыстные побуждения.

Действия Васильева суд квалифицирует:

- по факту тайного хищения денежных средств ФИО5 по п. «в» ч. 2 ст. 158 УК РФ как кража, то есть тайное хищение чужого имущества, совершенная с причинением значительного ущерба гражданину;

- по факту покушения на мошенничество в отношении ФИО4 по ч. 3 ст. 30, ч. 2 ст. 159 УК РФ как покушение на мошенничество, то есть умышленные действия лица, непосредственно направленные на хищение чужого имущества путем обмана, с причинением значительного ущерба гражданину, если при этом преступление не было доведено до конца по независящим от этого лица обстоятельствам;

- по каждому из фактов неправомерного доступа к охраняемой законом компьютерной информации по ч. 2 ст. 272 УК РФ как неправомерный доступ к

[31] Степанов-Егиянц, В. Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ. / В. Г. Степанов-Егиняц // автореф. дис. … канд. юрид. наук. М. 2008. С. 56.

охраняемой законом компьютерной информации, если это деяние повлекло модификацию компьютерной информации, совершенное из корыстной заинтересованности[32].

В конечном итоге суд признал Васильева виновным по всем статьям указанным выше.

Часть 2 ст. 272 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации, причинивший крупный ущерб или совершенный из корыстной заинтересованности. Также в примечании закреплено что крупным ущербом является ущерб, общая сумма которого превышает один миллион рублей..

Часть 3 ст.272 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации если данный доступ совершается группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения.

Повышенного внимания заслуживает ч.4 ст.272 УК РФ, в которой закреплено что лицо подлежит уголовной ответственности за неправомерный доступ к компьютерной информации, повлекший наступление тяжких последствий или угрозу их наступления.

На данный момент почти невозможно найти сферу жизни, где компьютер не используется. Элементарно предположить каков будет результат от неправомерного доступа к компьютерной информации.Для того чтобы квалифицировать деяние как преступное необходимо лишь наличие угрозы наступления результата[33].

Исходя из всего выше изложенного, можно сделать вывод о том, что на сегодняшний день теория безопасности информации пока не создана. Подходы, которые применяются, на практике страдают существенными недостатками и не обладают надежностью. Необходимо ориентироваться во всем спектре вопросов обеспечения информационной безопасности и понимать их взаимообу-

[32] Решение Кемеровского районного суда по делу 1-771/2016 от 12.05.16 // Архив Кемеровского районного суда.

[33] Батурин, Ю.М. Право и политика в компьютерном округе: учебное пособие / Ю. М. Батурин, А. М. Жодзишский. М. 1991. С. 234.

словленный характер.

2.2 Уголовная ответственность за создание, использование ираспространение вредоносных компьютерных программ

В Уголовный кодекс РФ 1996 г. была введена статья, предусматривающая ответственность за создание, использование и распространение вредоносных программ для ЭВМ (ст. 273).

После того как ее приняли, прошел достаточно большой период времени, и в результате чего были выявлены её недостатки.

Принятый 7 декабря 2011 года Федеральный закон № 420 « внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акт Российской Федерации» внес существенные изменения в рассматриваемую статью.

новой редакции она звучит как «Создание, использование и распространение вредоносных компьютерных программ».

Объектом данного состава преступления является, как уже отмечалось 1 главе общественная безопасность и общественный порядок и помимо этого еще совокупность общественных отношений по безопасному использованию компьютерной информации.

В примечании в ст. 272 УК Р содержится определение законодателя касающееся понятия «компьютерно информации».

Существенно сужая формы ее представления – здесь под такой информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Комитет Госдумы по информационной политике, технологиям и связи сделал заявление касающееся того что « в предметной дефиниции непонятен смысл термина «электрические сигналы»[34].

Такое явление как «электрический сигнал» – это

[34] Дорохов, Р.В. Уголовный кодекс изменили в помощь хакерам / Р. В. Дорохов // «Хакер». Санкт-Петербург. 2013. № 45. С. 34.

передаваемаясоответственно по проводам или без проводов (по ради) электромагнитная энергия, которая несет в себе конкретное сообщение.

Сообщение нужно понимать в широком смысле слова. Определение компьютерной информации не является исчерпывающим.

К примеру, когда передается компьютерная информация по кабельным оптоволоконным каналам связи, возможно, столкнуться со слудующей ситуацией: «Оптическое волокно осуществляет передачу сигналов только в одном направлении, именно из-за этого кабель состоит из двух волокон. На передающем конце оптоволоконного кабеля необходимо переустройство электрического сигнала в световой, а на приемном конце обратное переустройство»[35].

Именно поэтому в момент передачи сведений по оптоволокну, их опираясь на примечание к ст. 272 У РФ, не представляется возможным назвать компьютерной информацией, вотпочему противоправные действия, совершаемые злоумышленником с использование в качестве канала передачи данных оптоволокн , может исходя из строгого толкования норм , препятствовать применению ст. 272 УК РФ.

Статья. 273 Уголовного кодекса РФ, устанавливающая ответственность за создание, распространение или использование компьютерных программ либо компьютерной информации, подвергалась значительному изменению[36].

Так в прежней редакции ст. 273 УК РФ для квалификации преступления по не признавалось « … создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированном уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ…».

Именно эта формулировка значительно уменьшалакру потенциальных преступников.

Для совершения деяний данного типа нужно было обл дать конкретными

[35] Васильев, К. К., Глушков В. А., Дормидонтов А. В., Нестеренко А. Г. Теория электрической связи: учебное пособие / К. К. Васильева. М., 2008. С. 30.
[36] Букин, Д.С. Хакеры. О тех, кто делает это / Д.С. Букин // Рынок ценных бумаг. 1997. № 23. С. 44

специфичными и профессиональными навыкам [37].

В настоящее время под потенциального злоумышленника попадает достаточно большой круг лиц, так как для квалификации деяния как преступного по ст. 273 нужно и необходимо лишь установить факт наличияввнелицензионного незаконно модифицированного программного обеспечения или даже дистрибутива.

Примером может послужить судебное решение Кобяйского районного суда Республики Саха (Якутия).

Как установлено, на веб-странице общедоступной сети Интернет, имеющей URL-адрес: <Адрес обезличен>, размещена инструкция по созданию вредоносных программ для ЭВМ (компьютерных вирусов) и непосредственно находятся программы содержащие вирусы, что в силу законов запрещено.

Отсюда следует, что правовыми нормами в их взаимосвязи установлен запрет на распространение вышеуказанной информации и программ и необходимо ограничить доступ к ним.

Таким образом, на основании изложенного, исходя из фактических обстоятельств дела, с учетом оценки представленных доказательств в совокупности, суд приходит к выводу, что вышеуказанная информация, размещенная на сайте, запрещена к распространению на территории Российской Федерации.

На основании вышеизложенного суд решилинформацию, размещенную в сети «Интернет» по адресу: <Адрес обезличен>, - признать запрещенной к распространению на территории Российской Федерации[38].

До принятия изменений статья 273 содержала в себе всего две части, обновленная же содержит три. В разряд особо квалифицированных переведен признак причинения тяжких последствий или созданием угрозы их наступления.Следует отметить, что дейсвтия, закрепленные в диспозици статьи 273, не всегда являются противозаконными. Примером может послужить то-что, антивирусным компаниям необходимо проводить

[37] Кузнецова, Н. Ф. Курс уголовного права. Общая часть. / Н. Ф. Кузнецова // М.: Юрист, 2012. Том 1: Учение о преступлении. 340с.

[38]Решение по делу 2-64/ 2017 ~ М-49/2017 (22.03.2017), Кобяйский районный суд (Республика Саха (Якутия) // Архив Кобяйского районного суда.

конкретные противоправные действия с компьютерной информацией заниматься изучением вредоносной компьютерной информацией (нейтрализация средств которые защищают компьютерну информацию, модификацию.), производить обмен информацией между собой, а также осуществлять оценку последствий наступивших при использовани вредоносной компьютерной программы.

По нашему мнению данные действия обладают признаками, указанными в ст. 273 Уголовного кодекс РФ.

Однакоесли исходить из содержани ст. 14 УК РФ данные действия не являются преступными,потомучто не содержат общих условий, именно общественную опасность (действия которые осуществляю сотрудники антивирусных компаний, заранее нацелены н уменьшение и предотвращение ущерба, вызванного вредоносно компьютерной информацией) а также вину.

Следует заострить внимание на том, что приминение ст. 273 УК Р при распространении компьютерной информации, попадающей под действие диспозиции стать , в пиринговых сетях[39], к примеру, пр помощи сетевого протокола BitTorrent, может быт проблематично. Сам смысл распространения состоит том, что на самом сервере (трекер) в сети Интернет не содержится противозаконно компьютерной информации, а только сам фай с IP-адресами пользователей, у которы конкретная компьютерная информация имеется. Перед те как начать скачивания специализированная компьютерная программ (клиент) подключается к трекеру по I -адресу, указанному в торрент-файле, сообщае ему свой IP-адрес, на чт в ответ клиент получает адреса други клиентов, скачивающих или раздающих этот ж файл.

После этого клиент время от времени передаёт информаци трекеру о том как проходит процес и принимает новый (обновленный) список адресо . Клиенты соединяются друг с другом производят обмен сегментами файлов без свободног участия трекера, который осуществляет лишь хранени информации, которую он от подключенных обмену клиентов, список самих

[39] Определение пиринговых сетей. [Электронный ресурс]. URL: http:// wiki.rnet.ru. (дата обращения 25.05.2017).

клиентов и другую статистическую информаци [40].

Невзирая на то что торрент-треке может распространять компьютерную информацию и компьютерны программы, которые заранее предназначены для несанкционированног уничтожения, блокирования, модификации, копирования или нейтрализаци средств защиты компьютерной информации, по факт эту компьютерную информацию он не содержи , а содержит и отсылает пользователям перечен адресов, у кого есть данная компьютерна информация полностью или частично.

К тому же, торрент-трекер данного вида в основном физически находятс за пределами территории Российской Федерации[41].

Исход из выше сказанного привлечение организаторов торрен -трекера к уголовной ответственности, является затруднительны .

При изучении разъяснений Верховного суда Р по вопросу нарушения авторских прав [42], можн с уверенностью сказать, что распространителями вредоносно компьютерной информации, а также компьютерных програм со средствами защиты, будут считаться лиц , которые оказывали содействие в их распространени , например, путем размещения ссылки на ресур , где осуществляется физическое хранение файлов, распространени в p2p-сетях и т .

В заключении, можно сделать, логичный сделать вывод, о том, что никакие аппаратные, программные и любые другие решения, без основательной, всесторонней интеграции и взаимодействия с органами, специализирующимися на разработке методик и рекомендаций по противодействию данному виду преступлений не смогут гарантировать абсолютнуюнадежность и безопасность данных в компьютерных сетях.

2.3 Уголовная ответственность за нарушение правил эксплуатаци средств хранения, обработки или передачи компьютерно информации

[40]Сеть BitTorrent. [Электронный ресурс]. URL: http://ru.wikipedia.org/ (дата обращения 25.05.2017).
[41]Колымин, В. И. Хакер. / В. И. Колымин // «Хакер». СПб. 2014. № 18. С. 43.
[42] Постановление Пленума Верховного Суда РФ от 26 апреля 2007 г. № 14 «О практике рассмотрения судами уголовных дел о нарушении авторских, смежных, изобретательских и патентных прав, а также о незаконном использовании товарного знака» // Российская газета. Федеральный выпуск. 2007. 5 мая. № 4358.

информационно-телекоммуникационных сетей

Статья 274 Уголовног кодекса РФ предусматривает уголовную ответственность з нарушение правил эксплуатации средств хранения, обработк или передачи охраняемой компьютерной информации,либ информационно-телекоммуникационных сетей и оконечного оборудовани , а также правил доступа к информационн -телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификаци либо копирование компьютерной информации, причинившее крупны ущерб (ч. 1) или повлекшее тяжкие последстви или создавшее угрозу их наступления (. 2).

В соответствии со старой редакцией с . 274 УК РФ, лицо привлекалось к уголовно ответственности, если его действиями причинен существенны ущерб. Правоведы считали такую конструкцию неудачно [43]. Существенный вред – это оценочное понятие, которо зависит в каждом конкретном случае о многих показателей[44].

По мнению А.В. Наумова, понятие существенного вреда определяется самим потерпевшим и оценивается судом с учетом не только материального но и морального ущерба, ущерба деловой репутации, вынужденных финансовых потерь и затрат.

Цель статьи 274 УК РФ предупреждение невыполнения лицами своих профессиональныъ обязанностей, которые оказывают воздействие на сохранн-ость перерабатываемой и хранимой информации[45].

И всех преступлений, закрепленных в главе 28 У РФ именно нарушение правил эксплуатации средст хранения, обработки илипередачи компьютерной информаци информационно-телекоммуникационных сетей является наименее распространенны .

Об этом свидетельствуют данные ГИАЦ МВ России всего, 0,2 % от

[43]Вехов, В. Б. Компьютерные преступления: способы совершения, методики расследования: учебное пособие. / В. Б. Вехов. М.2000. С 10

[44] Дворецкий, М. Ю., Копырюлин А.Н. Правоприменение статьи 274 Уголовного Кодекса РФ: учебное пособие. / М. Ю. Дворецкий. М. 2012. С. 45 - 46.

[45] Наумов, А.В. Практика применения Уголовного кодекса Российской Федерации: коментарий судебной практики и доктринальное толкование / А. В. Наумов // ВолтерсКлувер. 2009. С. 1024

общего числа преступлений[46].Эти данные показывают нам недостатк и проблемы в работе правоохранительных органо , а также не совсем удачной формулировко ст. 274.

В Уголовном кодексе РФ н закреплено понятие нарушения правил эксплуатации средст хранения, обработки или передачи компьютерной информаци и информационно-телекоммуникационных сетей. В У РФ лишь определяются его последствия, именно уничтожение, блокирование или модификация компьютерно информации.

Из этого следует, что диспозици статьи 274 носит бланкетный характер. И эт одно из слабых мест уголовного законодательств в области защиты компьютерной информации.

Объективная сторона как уже отмечалось в первой главе, характеризуется как действиями, так и бездействием, которое связано с нарушением установленных правил.Конкретное содержание этих правил раскрывается в нормативных актах иных отраслей права (законах, правилах, инструкциях и т.д.).

Состав преступления материальный.Для признания преступления, оконченным необходимо наступление одного из нижеперечисленных последствий: уничтожение, блокирование или модификация охраняемой законом информации.

С субъективной стороны в данном составе возможна вина в форме умысла, что соответствует содержанию статьи 24 УК РФ.

Субъект преступления специальный - лицо, которое имеет доступ к эксплуатации упомянутых технических средств[47].

Это могут быть программисты, операторы, техники-наладчики, другие лица, по работе имеющие к ним доступ.

Хотелось бы заострить внимани на то что среди ученых ведетс спор о целесообразности криминализации деяния предусмотренног статьей 274 УК РФ.

[46] Главный информационный центр МВД РФ: официальный сайт. [Электронный ресурс] . URL: https://мвд.рф (дата обращения 24.05.2017).
[47] Наумов, А. В. Практика применения Уголовного кодекса Российской Федерации: коментарий судебной практики и доктринальное толкование / А. В. Наумов // ВолтерсКлувер. 2009. С. 134.

Добровольский придерживается мнения то что данное деяние не нуждаетс в криминализации[48], аБажни наоборот утверждает о избыточности криминализации.

Ягудин придерживается позиции что преступлени , предусмотренное ст. 274 УК РФ, является преступление средней тяжести, и наказание должно быт изменено повысив ответственность за преступление, предусмотренно ст. 274УК РФ. При изучении данного вопроса он всегда заостряет на этом внимание[49].Точно такой-же позиции придерживается И.Р. Бегищев. Повышение ответственности по его мнению будет способствовать снижению количествaданных преступлений[50].

Мы придерживаемся мнения, что неэффективность статьи 274 УК Р обусловлена конструкцией состава преступчления. Для тог чтобы деяние оказалось уголовно наказуемым необходим причинение крупного ущерба .Логичнее было б отнесение крупного ущерба к квалифицирующему признак деяния.

Исходя из вышеизложенного можно сделать вывод о том что преступления по ст 274 УК РФявляются наименее распространеными по сравнению с другими преступлениями в фере компьютерной информации. Эффективность статьи 274 УК РФ можно повысить путем отнесения крупного ущерба к квалифицирующему признаку деяния.

[48] Добровольский, Д.В. Актуальные проблемы с компьютерной преступностью: учебное пособие. / Д. Б Добровольский. // М. 2009. С. 67.

[49] Ягудин А. Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработкиили передачи компьютерной информации и информационно-телекоммуникационных сетей: дис… канд. юр наук. / А. Н. Ягудин. Казань. 2012. С. 218.

[50]Бегишев, И. Р. Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей / И. Р. Бегишев // Вестник УРФО. Безопасность в информационной среде. 2012. №1. С.15 – 18.

3 КРИМИНАЛОГИЧЕСКИЙ АНЛИЗ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

3.1 Структура и динамика компьютерной преступности. Статистические данные

Анализ структурыкомпьютерной преступности в России, следует проводить, исходя именно из широкого смысла данногопонятия и принимая во внимание существующие нормативные, научные и доктринальные подходы.

Проводя исследование нормативного подхода к структуре компьютерной преступности, в Доктрине информационной безопасности Российской Федерации необходимо выделить некоторые противоправныедеяния, выступающие угрозами безопасности информационных и телекоммуникационных средств и систем:

-противоправный сбор и использование информации;

-нарушения технологии обработки информации;

-внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

-разработка ираспространение программ, нарушающихнормальное функ-ционирование информационных и информационно-телекоммуника-ционных систем, в том числе систем защиты информации;

-уничтожение, повреждение, радиоэлектронное подавление илиразрушение средств и систем обработкиинформации, телекоммуникации и связи;

-уничтожение, повреждение, разрушениеили хищение машинных и других носителей информации;

-несанкционированныйдоступ к информации, находящейся в банках и базах данных, а также иные деяния[51]. Российская Федерация в силу различных политических, юридических, информационных и иных объективных причин нератифицировала Конвенцию Совета Европы о преступности в сфере

[51] Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

компьютернойинформации[52].

Однако несмотря на данныйфакт, правоохранительные органы Российской Федерации, к компетенции которыхотносится выявление, раскрытие, расследование, предупреждение компьютерныхпреступлений, надзор за расследованиемкомпьютерных преступлений, координациядеятельности правоохранительных органовпо борьбе с компьютерной преступностью(Прокуратура РФ, Следственный комитет РФ, ФСБ России, МВД России и др.),с учетом действующего уголовного законодательства Российской Федерации придерживаются аналогичной классификациипреступных деяний.

В частности, главным информационно-аналитическим центром МВД России и (ГИАЦ МВД России) постоянно осуществляется сбор, обработка, хранение сведений о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации, в том числе данных о количестве зарегистрированных преступлений, расследованных, прекращенных, приостановленных и направленных в суд соответствующих уголовных дел.

Несмотря на то, что у правоохранительных органов уже сложился свой нормативный подход к структуре компьютерной преступности, специалисты и эксперты в сфере информационной безопасности имеют свою собственную точку зрения на структуру компьютернойпреступности в Российской Федерации, или,как принято говорить в экспертном сообществе, к «рынку киберпреступности»[53].

Например,эксперты международнойкомпании Group-IB, специализирующейсяна предупреждении и расследовании киберпреступлений, считают, что основнымипреступными деяниями, образующими рынок киберпреступности в России, являются:

- мошенничество в системах интернет-банкинга;
- фишинг (доступ к конфиденциальным данным пользователя);
- хищение электронных денег;

[52] Конвенция о преступности в сфере компьютерной информации (ETS № 185) (Заключена в г. Будапеште 23 нояб. 2001 г.) Документ официально опубликован небыл. Доступ из справочно -правовой системы «КонсультантПлюс»

[53] Рынок киберпреступности. [Электронныйресурс]. URL: http://lawlibrary.ru. (дата обращения 27.05.2017).

- услуги обналичивания иных нелегальных доходов;

- спам (массовая рассылка разнообразной рекламы);

- продажа трафика;

- продажа эксплойтов;

- продажа загрузок;

- анонимизация (удаление идентифицирующих данных);

- DDoS-атаки[54]. (атака на сайт с целью вывести его из строя)

В свою очередь, специалисты Центраглобальных исследований и анализа угроз«Лаборатории Касперского» (GReAT),ежегодно анализирующие состояние киберпреступности в России и других странах, к компьютерным преступлениям, составляющим киберпреступность, относят:

- целевые кибератаки;

- кибершпионаж;

- хактивизм;

- кражу конфиденциальных данных;

- кибервымогательство;

- кибератаки, совершаемые по найму (кибернаемничество);

- использование вредоносного программного обеспечения для мобильныхустройств;

- целевой фишинг;

- нарушение тайны частной жизни;

- использование эксплойтов дляуязвимостей программного обеспечения;

- кибервымогательство;

- создание и использование ботнетов[55].

- нецелевой фишинг;

По мнению лаборатории PandaLabs, входящей в состав международной компании Panda, производящей антивирусное программное обеспечение в 2016 году основными преступными деяниями, формирующими компьютернуюпре-

[54] Экспертное сообщество Group-IB. [Электронный ресурс]. URL: http://report2013.group-ib.ru. (дата обращения 26.05.2017).
[55] Лаборатория Касперского. [Электронный ресурс]. URL: http://securelist.ru. (дата обращения 26.05.2017).

ступность в России, стали:

1. Кибершантаж (например, вредоносные программы типа CryptoLoker-Protockol,попав в компьютер, шифруют все типыдокументов, которые могут представлятьценность для пользователя (электронныетаблицы, документы, базы данных, фотографии и пр.), после чего жертву начинают шантажировать, требуя заплатитьвыкуп за возможность восстановленияфайлов).

2. Направленные кибератаки на информационные ресурсы компаний, организаций, учреждений и т.д.

3. Кибератаки на платежные терминалы для кражи данных банковских картклиентов.

4. APT-атаки (AdvancedPersistentThreats) – так называемые «постоянные угрозы повышенной сложности», представляющие собой вид направленных атак.

5. Атаки на смартфоны, а также иные мобильные устройства для кражи паролей и данных пользователей[56].

Исследование научной литературы показывает неоднозначность мнений исследователей относительно структуры компьютерной преступности в Российской Федерации.

Например, Д.К. Чирков и А.Ж. Саркисян в структуре компьютерной преступности выделяют только те преступные деяния, которые учитываются ГИАЦ МВД России как преступления, совершенные втелекоммуникации и компьютерной информации[57].

По мнению М.Б. Эмирова, А.Д. Саидова, Д.А. Рагимханова, «к наиболее распространенным видам преступлений вглобальных компьютерных сетях можноотнести: промышленный шпионаж;

- саботаж;

- вандализм;

[56]Исследователи компьютерных преступлений. [Электронный ресурс]. URL: http://www.viruslab.ru (дата обращения 27.05.2017).

[57] Чирков, Д. К. Следственно-судебные действия: проблемы регламентации // Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны. / Д.К. Чириков., А. Ж. Саркисян // «Networkingouter». М. № 3(27). С. 219 – 226.

- спуфинг (взлом паролей);

- мошенничество»[58].

Однако анализ нормативных, научных и иных источников показывает,что для иллюстрации структуры компьютерной преступности в России лучше использовать классификацию и статистику,касающуюся совершенных компьютерныхпреступлений, применяемую информационными центрами правоохранительныхорганов.

Исходя из статистических данныхГИАЦ МВД России за 2016 год, структурароссийской компьютерной преступностивыглядит следующим образом:

1. Нарушение тайны переписки,телефонных переговоров, почтовых, телеграфных или иных сообщений граждан (ч. 1 ст. 138 УК РФ) – 0,3 %;

2. Незаконный оборот специальныхтехнических средств, предназначенныхдля негласного получения информации (ст. 138.1 УК РФ), – 2,2 %;

3. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ) – 21,2 %;

4. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) – 8,1 %;

5. Нарушение правил эксплуатациисредств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей(ст. 274 УК РФ) – 0,02 %;

6. Нарушение авторских и смежныхправ, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 146 УК РФ), – 11,1 %;

7. Кража, совершенная с использованием компьютерных и телекоммуникационных технологий (ст. 158 УК РФ) –9,78 %;

8. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и мошенничество, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 159 УК РФ) –30,2 %;

9. Причинение имущественногоущерба путем обмана или злоупотребле-

[58] Яблоков, Е.А. Правовое регулирование борьбы с компьютерной преступностью в США / Е. А. Яблоков // Криминологический журнал. М. 2007. С.34 - 35.

ния доверием, совершенное с использованием компьютерных и телекоммуникационных технологий (ст. 165 УК РФ),– 0,2 %;

10. Незаконные организация и проведение азартных игр, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 171.2 УКРФ), – 0,2 %;

11. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 183 УК РФ), – 2,8 %;

12. Незаконное изготовление иоборот порнографических материалов или предметов, совершенные с использованием компьютерных и телекоммуникационных технологий (ст. 242 УК РФ),– 6,1 %;

13. Изготовление и оборот материалов или предметов с порнографическимиизображениями несовершеннолетних, совершенные с использованием компьютерных и телекоммуникационных технологий(ст. 242.1 УК РФ), – 5,3 %;

14. Использование несовершеннолетнего, в целях изготовления порнографических материалов или предметов, совершенное посредством компьютерныхи телекоммуникационных технологий (ст. 242.2 УК РФ), – 0,5 %[59].

При этом, согласно официальнойстатистике, динамика совершения преступлений в сфере компьютерной информации носит регрессивный характер, т.е. количество зарегистрированных, а следовательно, расследованных и направленных всуд уголовных дел из года в год неуклонно снижается.

По данным ГИАЦ МВД России, общееколичество преступлений в сфере компьютерной информации (зарегистрированныхв текущем периоде календарного года),предусмотренных ст. 272 и ст.ст. 273, 274 УК РФ составило: в 2009 г. 9 489 и 2097, 4; в 2010 г. – 6 132 и 1 010, 0;в 2011 г. – 2 005 и 693, 0; в 2012 г. – 1 930и 889, 1; в 2013 г. – 1 799 и 764, 0; в 2014 г.– 1 151 и 585, 3; в 2015 г. – 1396 и 974,12;в 2016 г. – 1456 и 1034,23[60].

[59] Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации. Сводный и сборник по России за январь-декабрь 2016 г. [Электронный ресурс]. URL: http://mvd.ru (дата обращения 26.05.2017).

[60] Главный информационный центр МВД РФ: официальный сайт.[Электронный ресурс]. URL: https://мвд.рф. (дата обращения 24.05.2017).

Таким образом, за последние восемь летколичество выявленных преступлений всфере компьютерной информации сократилось почти в 5 раз (количество уголовных дел уменьшилось с 11 590 до 2 382).

3.2 Характеристика личности компьютерного преступника

Под личностью компьютерного преступника в целом можно понимать совокупность значимых в социальном плане свойств, которые в сочетании с внешними условиями влияют н преступное поведение[61].

В общем анализе личности человека, совершающего преступлени , предусмотренные в гл. 28 УК РФ, необходим рассмотреть типовую классификацию преступников, дать общи портрет лиц, предпринимающих компьютерные правонарушения, выявить основные признаки, влияющие на преступно поведение и обусловливающие противоправный выбор.

Первыеотечественные работы, посвященны личности «компьютерных преступников» появились в конц 80-х - начале 90-х гг. и был , в основном, построены на основе анализ зарубежной статистики и правоприменительной практики. Та , например, Ю.М. Батурин выделял корыстны преступников: лиц, совершивших «компьютерные преступления» п небрежности или некомпетенции; «шпионов» и «хакеро », считая вторых «компьютерными хулиганами»[62].

Типовая классификаци лиц, совершающих правонарушения в сфере компьютерно информации, рассматривалась многими известными учеными . примеру, В.В. Крылов выделяет четыр основных типа преступников:

- нарушители правил пользовани компьютерной техникой;
- «белые воротнички» – респектабельные преступник ;
- компьютерные шпионы;
- лазутчики;
- хакеры, или «одержимые программист »[63].

В то же время зарубежные учены дают другую типовую квалификацию,

[61] Платонов, К. К. Проблема способностей. / К. К. Платонов // Кибепреступность. М.: Юрист, 2001. № 4. С. 34.
[62] Батурин, Ю. М. Право и политика в компьютерном округе: учебное пособие / Ю. М. Батурин и А. М. Жодзишский. М. 1991. С. 234.
[63] Крылов, В. В. Информационные компьютерные преступления. / В. В. Крылов // М.: Юрист, 1997. С. 64.

так, Д. Паркер выделяет сем категорий преступников в сфере компьютерной информаци :

- pranksters (шутник) – совершают преступления ради развлечения, бе корыстных мотивов;

- hucksters (торгаш) – лица с корыстными намерениями;

- malicious hacker (хакеры) – злоумышленники;

- personalsolvers (проблемные) – лица, решаютличные;

- careercriminals (профи) – преступники;

- extreme (защитники) – экстремалы, любители;

- irrationalpeople – «люди» [64].

При рассмотрении криминологического портрета преступник данной категории необходимо применять комплексны подход, учитывающий разные факторы развития человек : биофизиологические, социально-демографические, психологические, нравственные, социальн -ролевые, уголовно-правовые и криминологические.

современном мире преобладает виртуальное общение, в связи этим много людей старается реализоваться его пределах. Соответственно, способ самореализации може выйти за рамки уголовного законодательства Российско Федерации.

Человек, не обладающий привлекательной внешность , имеющий психологические проблемы при общении ил сталкивающийся с непониманием со стороны окружающи , пытается проявить себя в виртуальном пространств , добиваясь определенных достижений в программировании.

Данный индивид может самоутверждатьс , совершая компьютерные преступления, таким образом, пытаяс интеллектуально возвыситься, увеличить собственную значимость[65].

Примером этого может служит уголовное дело, возбужденное в Кемеровскойобласт . Гражданин А., работавший в отелег. Кемерово програм-

[64] Исследователи компьютерных преступлений. [Электронный ресурс]. URL: http://www.viruslab.ru. (дата обращения 27.05.2017).

[65] Керимов, В. Э., Профилактика и предупреждение преступлений в сфере компьютерной информации // В. Э. Керимов // Черные дыры в российском законодательстве. 2000. № 1. С. 34.

мистом, будучи уволенным, совершил и мести неправомерный доступ к компьютерной информации, скопировал конфиденциальную информаци о финансово-хозяйственной деятельности данного предприятия. Это повлекло з собой уничтожение его локальной компьютерной сет . Полученные сведения гражданин А. пытался продать конкурентам ООО «Логок», но был задержан. Указанные действия причинил ООО «Семья» ущерб в сумме 53 654 . 60 коп.[66].

Преступник может быть импульсивен ил прорабатывать свои действия до мелочей. Вполн возможно, что кто-то совершает преступлени в сфере компьютерной информации как вызо обществу, тем самым противопоставляя себя социальны отношениям.

Другой не будет бездумно эмоционально предпринимать противоправные действия, он може долго планировать преступление, ждать удобного момент или стечения обстоятельств, просчитывать все возможны последствия неправомерного поведения, способы сокрытия следо и только после этого совершать деяни . Можно предположить что такие правонарушения могу осуществляться в связи с личной заинтересованность либо из корыстных побуждений.

Однако корыстны мотивы порождаются гипертрофированными или извращенными потребностям , к примеру стремлением к легкой нажив . Молодым людям, которые составляют основную масс компьютерных преступников в Российской Федерации, свойственн также потребности социального характера, что веде к формированию мотивов агрессивной направленности.

Криминологически исследования личности преступника показывают, что сред ценностных ориентаций у данной категории ли преобладают индивидуально и кланово-эгоистические.

В данных случаях доминируют желание материального благополучи ,

[66] Уголовное дело № 1-158 (23.06.2014), Кемеровский районный суд // Архив Кемеровского районного суда Кемеровской области.

наиболее комфортных условий, проявления своего эг либо клановоэгоистический интерес[67]. В частност , ничем не ограниченная возможность совершения компьютерны преступлений и общедоступность компьютерных технологий, позволяющи получить любую информацию, приводят к объединени хакеров в преступные группировки, имеющие иногд транснациональный характер.

Нравственное и правовое сознани личности у компьютерных преступников обычно деформирован или ослаблено.

Еще И.И. Карпе и А. А. Ратинов более 30 лет назад отмечали, чт нарушенное правосознание может само по себ стать причиной выбора противоправного путиповедени [68]. В современном мире проявляется и противоположна тенденция. К примеру, группа хакеров «КиберБерку » совершает явные незаконные деяния, мотивируя сво деятельность высшими идеалами. Перечень мотивов, предложенны В.Б. Веховым, достаточно полно отражае мотивационную сферу деятельности компьютерных преступников[69].

1998 г, в Экспертно-криминалистическом центре МВ проведен классификационный анализ лиц, замеченных применении компьютеров для совершения противоправных деяни .

Обобщенный криминологический портрет преступника сильно изменился за это время и в основном не совпадает с реально существующим.

Это обусловлено рядом объективных факторов. Наприме , за последние 5–7лет значительно возросла доступност разнообразной компьютерной техники (включая коммуникаторы, планшетны компьютеры и смартфоны) и появилась возможност беспроводного доступа к сети Интернет высокимискоростями передачи данных[70].

Если говорить о зарубежном опыте, то сам факт появления компьютерной

---

[67] Долгова, А. И. Криминология: учебник / под ред. А. И. Долговой. М.: Издательство Закон, 1997. С. 292.

[68] Карпец, И. И. Правосознание как элемент правовой культуры // Правовая культура и вопросы правового воспитания. Сборник научных трудов / И. И. Карпец, А. Р. Ратинов. М.: Переиздание, 2005. С. 55.

[69] Вехов, В. Б. Компьютерные преступления: способы совершения, методики расследования: учебное пособие. / В. Б. Вехов. М. 2000. С. 10.

[70] Ушаков, С.И. Преступления в сфере обращения компьютерной информации (теория, законодательство, практика).дис… канд. юрид. наук. / С. И. Ушаков. Ростов н/Д., 2000. С. 144.

преступности в обществе многи исследователи отождествляют,с появлением так называемы «хакеров» (англ. «hack» - рубить, ломать) - пользовател вычислительной системы, занимающихся поиском незаконных способо получения несанкционированного доступа к средствам компьютерно техники (СКТ) и данным в совокупност с их несанкционированным использованием в корыстны целях[71].

Таким образом, можно сделать логичный вывод, что у условиях всеобщей глобализации и информатизаци прослеживается тенденция снжения возраста преступников в сфер компьютерной информации.

Это обусловлено как проблемам воспитания в сфере информационной культуры, том числе ввиду неграмотности родителей та и тем, что сами подростки, соверша преступления в указанной сфере, осознают сво безнаказанность в связи с тем, чт они не являются субъектами преступления силу возраста[72].

Знание рассмотренных свойств личност лиц, причастных к преступлениям в сфер компьютерной информации, позволит не только сформироват необходимую доказательственную базу по уголовным дела соответствующей категории. Это даст возможность следователя (суду) в процессе производства по уголовном делу выявлять обстоятельства, способствовавшие совершению преступлени .

3.3Меры по предупреждению компьютерной преступности

Система мер по предупреждению преступлений является одной из сфер социального управления, так как предполагает воздействиене только на детерминанты преступности, но и на причины их роста и развития. В теории криминологии меры по предупреждению преступности принято разделять на общесоциальные и специальные[73].

Данное разделение весьма условно, поскольку развитие преступности

---

[71] Букин, Д. С. Хакеры. О тех, кто делает это / Д. С. Букин // Рынок ценных бумаг. 1997. № 23. С. 45.
[72]Ходякова, Н. В. Личностный подход к формированию информационной культуры выпускников вузов.дис… канд. юрид. наук / Н. В. Ходяков. Волгоград, 2003. С. 34.
[73]Ценёв, О. П. Безопасность автоматизированных систем. / О. П. Ценёв. Российский следователь. М. 2006. №3. 2006. С. 4.

как социального явления требует от правоохранительных органов использования в своей работе более обширной совокупности мер, сочетающих особенности как общесоциальной, так и специальной профилактики. Такие «промежуточные» меры, с одной стороны, сходны с общесоцальными тем, что представляют собой понятие гораздо более широкое, чем просто борьба с преступностью.

С другой стороны, они имеют яркую направленность на профилактику преступности, хотя и не сводятся полностью к ней. Примером таких мер может служить «Доктрина об информационной безопасности РФ».

2013 год стал знаковым, положившим начало новому этапу в развитии Интернета на всей планете, расколов мир надвое. В 2013 году предполагалось найти компромисс относительно будущего Интернета, приняв новый регламент Международного союза электросвязи (МСЭ, англ. InternationalTelecommunicationUnion, ITU),в функции которого должен был войти контроль над инфраструктурой всемирной сети.

Это начинание поддержало большинство стран – 89, включая Россию и Китай.

Достаточно большое количество стран опасаются размножения кибер преступности, глобальных кибератак, а также самоорагнизации политических диссидентов через сети.

Новая интерпритация договора,по их мнению,должна была установить новые стандарты для решения этих проблем.

Впрочем, более 55 стран, выразили отказ подписать данное соглашение. Эксперты придержиались мнения, что США с самого начала были скептически настроены на упоминание Интернета в договоре и не хотели уступать «ни унции своих полномочий в сфере регулирования Интернета Международному союзу электросвязи»[74].

Результатом явилось то, что термин «Интерент» и «Сеть» не упонимались

[74] Намечается цифровая холодная война. [Электронный ресурс]. URL: http://www.letemps.ch/. (дата обращения: 27.05.2017).

в итоговом 26-страничном документе. Западноевропейские страны так же указали на то, что в статье 5В на странице 6 упоминаются меры, которые государства должны принять для предотвращения распространения нежелательной информации[75].

С одной стороны, это можно было интерпретировать как борьбу со спамом, но отдельные тоталитарные государства могут воспринять это как стимул к усилению контроля, за гражданами. Некоторые наблюдатели посчитали, что подобные меры приведут так же к увеличению контроля правительств над онлайн-контентом.Исходя из специфики преступлений, совершаемых с использованием компьютерных технологий,можно выделить три основные группы мер предупреждения преступлений, составляющие в совокупности систему борьбы с этим явлением:

— правовые;

— организационно-управленческие;

— технические[76];

К правовым мерам предупреждения компьютерных преступлений прежде всего относятнормы законодательства, устанавливающие уголовную ответственность за противоправные деянияв компьютерной сфере.Появление в 1996 г. в Уголовном кодексе РФГлавы 28 «Преступления в сфере информационных технологий» привело российское законодательство в соответствие с общепринятымимеждународными правовыми нормами, существовавшими в то время.

Однако после того, какданная глава была введена в УК РФ, прошло более 15 лет,и за это время существенных изменений законодателем внесено не было. Тристатьи, включенные в эту главу, уже не охватываютвсего многообразия преступлений, совершаемыхв современной компьютерной среде. Помимо этого,необходимо отметить не совсем удачную формулировку диспозиций статей данной главы.

Например,ст. 272 УК РФ «Неправомерный доступ к компьютерной ин-

[75] Комаров, А. А. Защита прав пользователей глобальной сети Интернет в процессе борьбы с компьютерными преступлениями. / А. А. Комаров. // Политика, государство и право. 2014. № 6. С. 43.

[76] Комаров, А. А. Стратегии наднациональных концепций предупреждения правонарушений в Интернет в их сравнительном выражении. / А. А. Комаров // Политика, государство и право. 2014. № 5. С. 32.

формации» в качестве оснований, влекущих уголовное преследование, предусматривает: уничтожение, блокирование, модификацию либокопирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Законодательдопустил серьезное упущение, забыв такое основание, как «ознакомление». А между тем чтение информации не менее опасно, чем ее копирование.

Иногда преступнику достаточно увидеть и прочитать информацию и она теряет свою ценность илиможет быть использована им в дальнейшем без всякого копирования.

Из-за несовершенства законодательства возникают и другие проблемы, затрудняющие предупреждение и расследование компьютерных преступлений.

Среди них можно выделить:

— неоднородность и бессистемность следственной и судебной практики по преступлениям даннойкатегории. В настоящее время Верховным судом непринято ни одного Постановления Пленума по вопросам применения статей о компьютерных преступлениях. Приговоры, вынесенные различнымисудами по однотипным уголовным делам, зачастуюрасходятся не только в вопросах квалификациидействий преступника, но и в определении размеров наказания;

Понятно, что одними правовыми мерами сдерживания не удастся достичь нужного результата в деле предупрежденияпреступлений. Из-за существующих проблем в уголовном законодательстве становится должной необходимость сугубого использования организационно-управленческих мер предупреждения компьютерной преступности:

- устранение утечки, хищения, утраты,искажения и подделки информации;

- предотвращение несанкционированных действий по уничтожению, модификации, искажению,копированию, блокированию информации и других форм незаконного вмешательства в информационные ресурсы и системы;

- гарантирование правового режима функционирования документированной информации как объекта собственности;

- сохранение государственной тайны и конфиденциальности документированной информации;

- обеспечение прав субъектов в информационных процессах и при разработке, производствеи применении информационных систем, технологий и средств их обеспечения.

Некоторые ученые (например, В.А. Бессонов), в системе предупреждения «компьютерной» преступности выделяют виктимологический элемент предупреждения как самостоятельноенаправление. Под виктимологическими факторами, воздействующими на совершение преступлений в сферекомпьютерной информации, автор понимает «совокупность условий, определяющих обращение субъекта в потенциальную или реальную жертву,а также личностные характеристики уже реальныхжертв преступления, участвующих в механизме совершения конкретного преступления», подразделяя данные факторы насоциальные, нравственно-психологические и поведенческие[77].

В действующей системе предупреждения преступлений в сфере компьютернойинформации существует серьезный пробел – плохоевнимание к изучению личности несовершеннолетнего преступника. С распространением глобальной компьютерной сети Интернетнесовершеннолетние правонарушители в РФ получили широкий спектр возможностей, поэтому должное внимание необходимо уделять профилактикепротивоправной деятельности среди подростков[78].

Также помимо организационно-управленческих мер, одну из главных ролей в борьбе с компьютерными преступлениями играют меры технического характера (аппаратные, программные).

Аппаратные методы предназначены для защиты компьютерной техники от нежелательных физических воздействий и закрытия возможных каналов утечки конфиденциальной информации. К ним относятся источники бесперебойного питания, устройства экранирования аппаратуры, шифрозамки и уст-

[77] Бессонов, В.А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации: автореф. дис… канд.юрид. наук. / В. А. Бессонов. Н. Новгород, 2000. С. 45.

[78]Копырюлин, А. Н. Преступления в сфере компьютерной информации: Уголовно - правовой и криминалогические аспекты. / А. Н. Копырюлин. Уголовное право. 2009. № 4. С. 102 - 103.

ройства идентификации личности.

Программные методы защиты предназначаются для непосредственной защиты информации. Для защиты информации при ее передаче обычно используют разнообразные методы шифрования данных. Как показывает практика, современные методы шифрования позволяют достаточно надежно скрыть смысл сообщения [79].

Возрастание компьютерной преступности, прежде всего, обусловлено следующими факторами:

- увеличением количества пользователей ЭВМ и пользователей глобальной сети.

- увеличением количества пользователей ЭВМ и пользователей глобальной сети Интернет вследствие уменьшения цен на соответствующую оргтехнику;

- неудовлетворительным отношением руководителей к вопросу обеспечения информационной безопасности и защиты информации;

- устаревающими средствами защиты программного обеспечения;

- устаревающими средствами, обеспечивающими информационную безопасность;

- возрастанием количества операций, осуществляемых безналичным путем с использованием различных международных финансовых платежных систем, а также расширением информационных сетей для обмена информацией, заключения контрактов и других операций без надлежащего контроля;

- учащением использования в преступной деятельности современных технических средств, в том числе и ЭВМ;

- непродуманной кадровой политикой приприеме на работу и увольнении;

- низким уровнем специальной подготовки должностных лиц правоохранительных органов.

[79]Цирлов, В. Л. Основы информационной безопасности автоматизированных систем. / В. Л. Цирлов // «Закон» М. 2008. С 28.

В связи с тем, что компьютерные преступления в силу своей специфики все больше приобретают транснациональный характер, усиливается и международное сотрудничество в области борьбы с этими преступлениями.

Международный опыт борьбы с преступностью свидетельствует о том, что одним из приоритетных направлений решения задачи эффективного противодействия современной преступной деятельности является активное использование правоохранительными органами различных мер профилактического характера[80].Для обемна опытом и консолидации усилий по борьбе с новым видом

преступности правоохранительными органами проводятся международные семинары, достижениями которых обычно становятся совместно разработанные и утвержденные планы мероприятий, направленных на профилактику компьютерной преступности. К примеру,Международная конференция «Информационные технологии и безопасность-2006», проходившая 19 – 23 октября 2007 г. в Крыму (Украина), или «Первая международная конференция по безопасности и правовым проблемам противодействия киберпреступности», состоявшаяся 2 – 4 июня 2008 г. в Каире (Египет).

Задачами подобных конференций являются обсуждение широкого круга актуальных проблем глобализации информационных систем и их влияния на формирование информационного общества, разработка совместных мероприятий по вопросам обеспечения информационной безопасности.

Среди таких мероприятий в качестве основныхможно выделить:

- разработку порядка взаимодействия правоохранительных и иных министерств и ведомств на международном уровне, а также обмена информацией в борьбе с использованием высоких технологий в преступных целях;

- проведение научно-практических конференций с участием практических работников по проблемам выявления, пресечения и расследования преступлений в сфере высоких технологий;

[80] Доклад Генерального Секретаря ООН «Воздействие организованной преступной деятельности на общество в целом» // Материалы комиссии ООН по предупреждению преступности и уголовному правосудию. Вена. 15.03. 1993. L7CN .

- подготовку методических рекомендацийпо выявлению, предупреждению, раскрытию преступлений в сфере высоких технологий;

- создание в составе экспертно-криминалистических учреждений подразделения для производства экспертиз по делам о преступлениях в сфере высоких технологий;

- разработку прогрмм подготовки кадров, специализирующихся для работы в сфере высоких технологий.

Само собой проведение данных мероприятий потребует достаточно большого количества времени и больших затрат но именно это должно стать первостепенной задачей правоохранительных органов в борьбе с компьютерной преступностью.

И в заключении, хотелось бы отметить, что практика борьбы с преступлениями в сфере компьютерной информации показывает, что положительный результат можно получить только при использовании комплекса правовых, организационных и технических мер предупреждения неправомерного доступа к компьютерной информации, причем все они одинаково важны и лишь дополняя друг друга образуют целенаправленную систему предупреждения и профилактики преступлений исследуемого направления.

ЗАКЛЮЧЕНИЕ

Преступления в сфере компьютерной информации,являются высоколатентными преступлениями и это является идеальной возможностью для претсупника совершать деяния и остоваться безнаказанным. По мнению специалистов, только 10-15% компьютерных преступлений становятся достоянием гласности, т.к. организации, пострадавшие вследствие совершения подобного рода преступлений, весьма неохотно предоставляют информацию, поскольку это может привести к потере их репутации или к совершению повторных преступлений[81].

Парадокс преступлений в сфере компьютерной информации состоит в том, что после их совершения потерпевший не особо заинтресован в поимке злоумышленника, а сам преступник, в случае его поимки разнообразными способами пытается прорекламировать свою противоправную деятельность на «арене» компьютерного взлома.

Объяснение этому феномену достаточно простое, как уже отмечалось выше, пострадавшая сторона не стремиться афишировать факт несанкционированного проникновенияю, ведь это может способстововать потере клиентской базы. А вторая причина заключается в том, что получивший даже максимальный срок преступник, приобретает широкую известность в деловых и криминальных кругах[82].

Так же основной проблемой явялется невыработка четких и эффективных методик по проведению комьютерных экспертиз, и конечно же нехватка квалифицированных специалистов.

Без грамотного экспертного заключения привлечени лица к уголовной ответственности, даже пр наличии признаков состава преступления, становится проблематичны .

Поэтому процент прекращенных дел по данной категории преступлений достаточно высок.

Мы придерживаемся мнения, от том что в гаве 28 УК РФ, лучше было бы

[81]Мелик. Э. В. Компьютерные преступления. / Э.В.Мелик. М.: Юрид. Лит., 2010. С. 40.
[82]Парога, А.И. Преступления в сфере компьютерной информации//Российское уголовное право: Особенная часть. /А. И. Парога. М. 2001. С. 671.

применять термин «информационная преступность». И для того чтобы повысить эффективность главы 28 необходимо ужесточение наказания. Данное ужесточение, может изменить уже сложившуюся ситуацию.

Необходимо расширитькруг криминализованныхдеяний в Главе 28 УК РФ, включив в нее:

-компьютерный шпионаж,

-компьютерный терроризм,

-компьютерное мошенничество,

-причинение имущественного вреда путем изменения компьютерной информации и т.д.

Такая возможность не исключена, так как законодательная база, регулирующая отношенияв сфере компьютерной информации и информационной безопасности, находится на этапе становления и совершенствования. Особенно это касается отношений, возникших в результате появления сети Интернет, а также в силу таких особенностей этой технологии, как глобальность, анонимность, широкая распространенность и т.д.

Вцелях повышения эффективности работ , направленной на обеспечение гарантий государственной защит прав и законных интересов граждан, целесообразны было бы включить в квалифицированные состав , регламентируемые главой 28 УК РФ, еще одног дополнительного непосредственного объекта отношений собственности о признании в связи с эти потерпевшего обязательным элементом этого объекта путе дополнения статей предусмотренных данной главой, новы квалифицирующим признаком «с причинением значительного материальног ущерба потерпевшему».

На момент 2017 года в нашей стране не особо развиты методы и меры организации борьбы с компьютерными преступлениями и чтобы исправить данную ситуацию необходимо сделать следующее:

-Выработать приемы и методы их выявления, раскрытия и доказывания;

-Изучить зарубежную практику борьбы с компьютерными преступлениями;

-Решить задачу криминологической оценки компьютерных преступлений проблем обеспечения информационной безопасности;

-Разработать меры прогнозирования и профилактики компьютерныхпреступлений;

-Проследить технологию и технику соверешния компьютерных преступлений;

-Закрепить терминн «ознакомление» в диспозиции статьи 272 УК РФ;

-Снизить возраст лица для привлечения к уголовной ответственности за компьютерные престпуления;

-Создание центров подготовки выскоквалифицированных специалистов в области компьютеризации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

I Правовые акты:

1 Уголовный кодекс Российской Федерации 13.06.1996 г. № 63-ФЗ (ред. от 17.04.2017) // Собрание законодательства РФ – 1996. - № 25. - Ст. 2954.

2 Федеральный закон от 07.07.2003 № 126-ФЗ"О связи" (ред. от 17.04.2017) //Собрание законодательства Российской Федерации. – 1995. – № 8. – Ст.20.

3 Федеральный закон от 27 июля 2006 г. № 149-ФЗ"Об информации, информационных технологиях и защите информации" (ред. от 19.12.2016) // Собрание Законодательства РФ. – 2006. – № 31 (ч. I). – Ст. 2.

4 Федеральный закон от 07.12.2011 № 419-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации" // Парламентская газета. - 2011. - 16-22 дек. - № 55-56. - С. 37-43.

5 Указ Президента РФ от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"//Собрание законодательства РФ12.12.2016. № 50. ст. 7074.

6 Конвенция о преступности в сфере компьютерной информации (ETS № 185) (Заключена в г. Будапеште 23 нояб. 2001 г.) // документ официально опубликованнебыл. Доступ из справ.- правовой системы «КонсультантПлюс».

7 Свод законов США 1989 г. § 1030 Титул 18. (ред. от 08.02 1997). - СПб: Юридический центр Пресс, 2012.

8 Уголовный кодекс Японии от 12.05.1995. (ред. от 02.03.2002). - СПб: Юридический центр Пресс, 2012.

9 Закон Японии «О несанкционированном проникновении в компьютерные сети».от 03.02.2000. (ред. от 08.09. 2004). - СПб: Юридичесикй центр Пресс, 2012.

II Специальная литература

10 Батурин, Ю.М. Право и политика в компьютерном округе: учебное пособие / Ю. М. Батурин, А.М. Жодзишский. – М. - 1991. - С. 234.

11 Бессонов, В.А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации.автореферат. дис. канд.юрид.наук. / В. А. Бессонов. Н. Новгород. 2000г. - С. 45.

12 Бражник, С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники.дис. канд.юрид. наук. / С. Д Бражник. Ижевск. 2009г. - С. 65.

13 Букин, Д.С. Хакеры. О тех, кто делает это /Д.С. Букин // Рынок ценных бумаг. 1997. - № 23.–С. 40.

14 Васильев, К. К.,Теория электрической связи: учебное пособие / К. К. Васильев, В. А. Глушков, А. В. Дормидонтов – М. - 2008. - С. 30.

15 Вехов, В.Б. Компьютерные преступления: способы совершения, методики расследования: учебное пособие. / В.Б. Вехов. – М. 2000. - С 10.

16 Дворецкий, М.Ю., Копырюлин А.Н. Правоприменение статьи 274 Уголовного Кодекса РФ: учебное пособие. / М.Ю. Дворецкий. М. - 2012. – С. 45- 46.

17 Доклад Генерального Секретаря ООН «Воздействие организованной преступной деятельности на общество в целом» // Материалы комиссии ООН по предупреждению преступности и уголовному правосудию.–Вена.- 1993. - L7CN.

18 Долгова, А.И. Криминология: учебник / под ред. А.И. Долговой.- М.: Издательство Закон, 1997. - С. 292.

19 Дорохов, Р.В. Уголовный кодекс изменили в помощь хакерам. / Р.В. Дорохов // «Хакер». – Санкт-Петербург. - 2013 год. - № 45 – С. 34.

20 Дорохов, Р.В. Компьютерная преступность. / Р.В. Дорохов // «ComputerLawandSecurity». – М. 2011.- № 32– С. 2.

21 Здравомыслов, Б.В. Уголовное право РФ. Особенная часть: учебник / под ред. проф. Б. В.Здравомыслова. — 2-е изд., перераб. и доп. — М.: Юристъ, - 2012. - С. 22.

22 Карпец, И. И. Правосознание как элемент правовой культуры // Правовая культура и вопросы правового воспитания / И.И. Карпец, А. Р. Ратинов // сборник научных трудов. М.: Переиздание 2005. С. 55–57.

23 Керимов, В.Э., Профилактика и предупреждение преступлений в сфере компьютерной информации // В.Э. Керимов // Черные дыры в российском законодательстве. 2000. № 1. С. 34.

24 Коликов, Н.Л. Причины и условия профессиональной компьютерной преступности. / Н.Л. Коликов // Вестник ЮУрГУ. – 2011. – № 19. – С.30.

25 Котов, Н.И. Комментарий к Уголовному кодексу Российской Федерации: научно-практический (постатейный). / Н.И. Котов, Г. ВДайшутов.-М.: Юрайт-Издат, 2012.

26 Колымин, В.И. Коллектив авторов – Хакер. / В.И. Колымин // «Хакер». – Санкт-Петербург. - 2014. - № 18 – С. 43.

27 Коликов, Н.Л. Причины и условия профессиональной компьютерной преступности. / Н.Л. Коликов. Вестник ЮУрГУ. – 2011. – № 19. – С. 30.

28 Копырюлин А.Н. Преступления в сфере компьютерной информации: Уголовно-правовой и криминалогические аспекты. / А.Н. Копырюлин // Уголовное право.- 2009. - № 4.- С. 102 - 103.

29 Комаров А.А. Стратегии наднациональных концепций предупреждения правонарушений в Интернет в их сравнительном выражении. / А.А. Комаров // Политика, государство и право. - 2014. - № 5. – С. 32.

30 Комаров, А.А. Защита прав пользователей глобальной сети Интернет в процессе борьбы с компьютерными преступлениями. / А.А. Комаров. // Политика, государство и право. - 2014. - № 6. – С. 43.

31 Крылов, В.В. Информационные компьютерные преступления. / В.В. Крылов // М.: Юрист, - 1997. - С. 64.

32 Кузнецова, Н.Ф. Курс уголовного права. Общая часть. Том 1: Учение о преступлении / Н.Ф. Кузнецовой // М.: Юрист, - 2012. – 340с.

33 Курушин, В.Д. Компьютерные преступления и информационная безопасность. / В.Д. Куршин // Справочник. – М.: Новый юрист, - 2004. - С 65.

34 Логинов, А.Б. Компьютерные преступления: способы совершения, методики расследования. / А.Б. Логинов. М.: Юрид. Лит. - 2000. - С 10.

35 Мелик, Э.В. Компьютерные преступления. / Э.В. Мелик. – М.: Юрид. Лит., - 2010. - С 40.

36 Мерзогитова, Ю.А. Понятие компьютерной преступности. / Ю.А. Мерзогитова // Вестник МВД России. - 2001. – № 5-6. – С. 84.

37 Наумов, А.В. Практика применения Уголовного кодекса Российской Федерации: Коментарий судебной практики и доктринальное толкование / А.В. Наумов // ВолтерсКлувер. - 2009. - С. 1024.

38 Платонов, К.К. Проблема способностей. / К.К. Платонов // Кибепреступность. - М.: Юрист. – 2001. - № 4. - С. 34.

39 Парога, А.И.Преступления в сфере компьютерной информации//Российское уголовное право: Особенная часть. /А.И. Парога// ред. проф.М.: - 2001. - С.671.

40 Скоромников, К.С. Компьютерное право Российской Федерации. / К.С. Скоромников.– М.: Проспект, - 2000. – С.200.

41 Степанов-Егиянц, В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ: автореф. дис. … канд. юрид. наук. / В.Г. Степанов-Егиняц. - М. - 2008. – С. 56.

42 Степанов-Егиянц, В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями. / В.Г. Степанов-Егиняц // Российскийследователь. - 2012. - № 24. - С.34.

43 Тропина, Т.В, Самоурегулирование исорегулирования в борьбе с Киберпреступностью и обеспечения Кибербезопасности. / Т.В.Тропина// В: JahnkeAl. (ред.), Дункер&Humblot, - Берлин, - 2012. – С. 56-57.

44 Ушаков, С.И. Преступления в сфере обращения компьютерной информации (теория, законодательство, практика).дис… канд. юрид. наук. / С. И. Ушаков. Ростов н/Д. - 2000. - С. 144.

45 Ходякова, Н. В. Личностный подход к формированию информационной культуры выпускников вузов:дис… канд.юрид. наук. / Н. В. Ходя-

ков.Волгоград. - 2003. - С. 34.

46 Цирлов, В.Л. Основы информационной безопасности автоматизированных систем. / В.Л. Цирлов // Закон. - М. - 2008.– С. 28.

47 Ценёв, О.П. Безопасность автоматизированных систем. / О.П. Ценёв // Российский следователь. - М. - 2006. - №3. - 2006.– С. 4.

48 Чирков, Д.К. Следственно-судебные действия: проблемы регламентации / Д. К. Чириков, А. Ж. Саркисян // Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны. «Networkingcomputer». - М.– № 3(27). – 2009. С. 219–226.

49 Широков, В. А.Компьютерные преступления: основные тенденции развития. / В.А. Широков, Е. В. Беспалов // Юрист. - 2006. - № 10. - С. 18.

50 Ягудин, А.Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработкиили передачи компьютерной информации и информационно-телекоммуникационных сетей:дис… канд. юр наук./ А.Н. Ягудин. Казань. - 2012. - С.218.

51 Яров, Д. А. Правовые, социальные и психологические основы производства по уголовным. / Д.А. Яров. - М. 2006. – С. 65.

52 Яблоков, Е.А. Правовое регулирование борьбы с компьютерной преступностью в США / Е.А. Яблоков //Криминологический журнал. – М. - 2002. - С. 52-55.

III Электронные ресурсы

53 Главный информационный центр МВД РФ: официальный сайт. [Электронный ресурс]. - Режим доступа: https://мвд.рф (дата обращения24.05.2017).

54 Методическиерекомендациипоосуществлениюнадзоразаисполнением законов при расследовании в сфере компьютерной информации. [Электронный ресурс].– Режим доступа: http://www.advodom.ru/practice/ (дата обращения 02.03.2015).

55 Определение пиринговых сетей. [Электронный ресурс]. – Режим доступа: http:// wiki.rnet.ru (дата обращения 25.05.2017).

56 TexasComputerCrimesLaw 1985 г. [Электронный ресурс].– Режим доступа: http://ruponia.livejournal.com(дата обращения 25.05.2017).

57 Определение сетевого протокола BitTorrent. [Электронный ресурс].– Режим доступа: http://ru.wikipedia.org(дата обращения 25.05.2017).

58 Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации. Сводный и сборник по России за январь-декабрь 2016 г. Ф-615 кн. 1. [Электронный ресурс]. – Режим доступа: http://mvd.ru(дата обращения 26.05.2017).

59 ЭкспертноесообществоGroup-IB.[Электронный ресурс].– Режим доступа: http://report2013.group-ib.ru(дата обращения 26.05.2017).

60 Лаборатория Касперского. [Электронный ресурс]. – Режим доступа: http://securelist.ru (дата обращения 26.05.2017).

61 Компютерные преступления в США.[Электронный ресурс].– Режим доступа: http://www/securitylab/ru(дата обращения 26.05.2017).

62 Исследователи компьютерных преступлений. [Электронныйресурс]. – Режим доступа: http://www.viruslab.ru(дата обращения 27.05.2017).

63 Рынок киберпреступности. [Электронныйресурс]. –Режим доступа:http://lawlibrary.ru(дата обращения 27.05.2017).

64 Мосин О.В. Компьютерная преступность в России. Как с ней бороться./ О.В Мосин. -[Электронный ресурс]. – Режим доступа: http://samlib.ru/ (дата обращения 27.05.2014).

65 Намечается цифровая холодная война. [Электронный ресурс]. – Режим доступа: http://www.letemps.ch/(дата обращения: 27.05.2017).

IV Правоприменительные акты

66 Постановление Пленума Верховного Суда РФ от 26 апреля 2007 г. № 14 «О практике рассмотрения судами уголовных дел о нарушении авторских, смежных, изобретательских и патентных прав, а также о незаконном использовании товарного знака» // Российская газета: Федеральный выпуск. - 2007. - 5 мая. - № 4358.

67 Уголовное дело № 1-158 (23.06.2014), Кемеровский районный суд// Архив Кемеровского районного суда Кемеровской области.

68 Решение по делу 2-64/ 2017 ~ М-49/2017(22.03.2017), Кобяйский районный суд (Республика Саха (Якутия) // Архив Кобяйского районного суда.

69 Решение Кемеровского районного суда по делу 1-771/2016 от 12.05.16. // Архив Кемеровского районного суда.