Министерство внутренних дел Российской Федерации

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

Кафедра Уголовного права

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему «Ответственность за неправомерный доступ к компьютерной информации по УК РФ»

Выполнил: Мась Дмитрий Владимирович

40.05.01 ПОНБ 2013 год набора, 131 учебная группа

Руководитель:
д.ю.н., профессор, профессор кафедры уголовного права
Талан Мария Вячеславовна

Рецензент:
Начальник СО ОП №12 «Гвардейский» СУ МВД России по г. Казани
Ахметзянов Ильдар Радикович

К защите _____
(допущена, дата)
Начальник кафедры _____

Дата защиты: "___" _____20___г. Оценка _____

Казань 2018

Содержание

Введение

Актуальность выбранной темы исследования определяется теоретической и практической важностью аспектов функционирования государства, которые имеют прямую зависимость от создания и развития в новейшей истории Российской Федерации адекватных, отвечающих вызовам времени систем и способов обеспечения безопасности в информационном поле как страны в целом так и в мире. Прогресс и научные достижения во многих областях, совершенствование в сфере информационно-коммуникационных технологий, рост доли компьютеризации и автоматизации в промышленной сфере повлияли на современное общество и мир, поспособствовали переходу его к постиндустриальному, а в частности и к информационному обществу. Которое предполагает производство, хранение и переработку, реализацию информации, пронизывающее все области жизнедеятельности человека. Таким образом на сегодняшний день информация и знания возведены в разряд одних из важных ресурсов, а в некоторых областях и стратегических.

В процессе отношений, которые возникали в информационном поле, появилась необходимость в решении правовых проблем, так или иначе связанных с изучением и развитием информационных технологий и накопленных знаний. Этим вопросам посвятили свои труды множество ученых, среди которых И.Л. Бачило, В.С. Беляева, И.Ю. Жукова, О.В. Щербакова, А.Б. Венгерова, В.А. Копылова, И.С. Мелюхина, М.М. Рассолова и другие.

Информатизация общества, возникновение и развитие новых сфер в науке и жизни — это очередной виток нынешней эпохи научно-технического прогресса. Однако с появлением целой новой отрасли, которая проникла буквально во все сфера жизни и деятельности людей, в разы увеличившая продуктивность и безопасность, побочным продуктом данного прогресса стали появляться новые виды правонарушений, а именно в сфере компьютерной информации и безопасности. Изначальной сложность системы, и

многогранность принципов и реализаций, такие преступления характеризуются низким уровнем раскрываемости и идентификации преступников.

Так как для совершения преступлений в сфере информационных технологий требуются определенные знания и навыки, а зачастую и достаточно высокие и узкие, то мировое сообщество оказалось неготовым к его появлению. Правоохранительные органы столкнулись с доныне неизвестным в практике видом преступлений, для которых просто не существовало механизмов регулирования таких отношений, таким образом затруднительным становилась даже соотношение с правонарушением в сфере компьютерной информации.

Правонарушения в сфере информационных технологий уступают в количестве в общей массе отступлений от букв закона, однако в отличии от остальных несут в себе реальную, неконтролируемую угрозу. И эта угроза направлена не только на отдельно взятых личностей, пользующихся персональными компьютерами, но и на целые сектора экономики, производства, а также национальной безопасности страны. Систематизация, разного рода объединения злоумышленников, зачастую раскиданных по всему земному шару, создает потребность в отлаженной системе предупреждения атак как на целые государства, так и на отдельные сектора жизнедеятельности. Помимо преступников, многим странам необходима защита в инфопространстве и от специально созданных подразделений других государств, ведущих сбор, систематизацию и подрывную деятельность.

Обращаясь к статистическим данным по совершенным преступлениями в сфере компьютерной информации, информационных технологий можно выявить определенную тенденцию роста. Это связано с все большей интеграцией в различные сферы деятельности человека новых технологий, а соответственно и появлению новых форм, начиная от мошенничества, до более серьезных отступлений от закона. А именно за период 2007 года было зарегистрировано свыше семи тысяч преступлений в сфере высоких технологий, из них раскрыто 91,4%. По данным за 2008 год было 9010 преступлений закона, закрыто порядка 93,44%, а конкретнее 8419. За 2009 год

было выявлено 10575, из которых раскрыто 9991, что составило 94,47%. Начало 2010 года началось с резкой активизации преступлений в сфере высоких технологий, а именно уже в первом квартале составило около 12 тысяч, из которых было раскрыто порядка 88%. Нетрудно проследить наметившиеся тенденции, и ситуация будет развиваться, не сколько в росте количества совершенных преступлений, но и в их качестве.

В настоящее время ущерб от хакерских атак по данным за вторую половину 2016 и первую половину 2017 год составил порядка 4,7 млрд. рублей в Российской Федерации. А урон за 2015 год в мире насчитывает примерно 3 трлн. долларов. Безусловно статистика понятие гибкое, однако и данных цифры впечатляют. Не стоит оставлять без внимания и те преступления которые не смогли по тем или иным причинам выявить, так же о тех преступлениях о которых граждане не сообщили. Таким образом картинка складывается удручающая. Однако с ростом преступлений в области высоких технологий развиваются и средства защиты от первых.

На сегодняшний день состояние информационной безопасности Российской Федерации не отвечает реалиям и потенциальным угрозам, вызовам современного мира. Ведется большая работа по укреплению защиты и обеспечению информационной безопасности. Так 12 мая 2017 года была зафиксирована хакерская атака, которая нарушила работу многих серверов находящихся на территории порядка 74 стран. Однако больше всего пострадали серверы, которые находились на территории Российской Федерации и Тайваня. Так же целями атак были Сбербанк, серверы МВД, МТС, Мегафон.

Конечно в общей картине доля преступлений в сфере высоких технологий мала, однако она неукоснительно растет.

Вступление УК РФ ставило ряд задач решением которой занялись теоретики уголовно-правовой науки, а именно: определение объекта преступлений в сфере информационных технологий, выразить понятия и обличить в систему; разработать критерии выявления схожих по составу видов преступных посягательств, отделение от иных составов преступлений;

определить квалификации, и соответствующие ответственности и наказания за них.

Бланкетный характер диспозиций, который соответствует уголовно-правовым нормам обязывает обращению к различным правовым актам, которые регулируют появляющиеся правоотношения, и к знаниям специфики и терминологии.

За ушедшее время с момента вступления в силу Уголовного кодекса Российской Федерации, в теоретическом и практическом поле применения норм о преступлении законов в сфере высоких технологий наметился вектор задач, которые на данный момент не стали предметом системного исследования.

Недостаток в Российской судебной практике значительно усложняет выполнение более детального анализа данного вида преступной деятельности, исполнение криминологической экспертизы норм о преступления гл. 28 Уголовного кодекса Российской Федерации.

Затруднения в определенных обстоятельствах спровоцированы сложностью, а порой и непродуманностью части законодательных актов. В юридической литературе не раз подчеркивалась недоработка, несоответствие, различные туманности и неопределенности положений главы 28 Уголовного кодекса Российской Федерации, что еще больше усложняло работу.

Однако независимо от степени важности как теоретической, так и практической стороны изучением, направленным на систематизацию уголовно-правовых и криминологических аспектов по сути не осуществлялось.

На сегодняшний день подавляющее большинство исследований и трудов носят более узкий характер. Плоды трудов облечены преимущественно в статьи, или краткие работы, направленные в основе своей или только на уголовно-правовую или же только затрагивающие криминологические аспекты.

Наряду с этим появляется потребность в осуществлении разработок в данной области, в которой бы учитывалось современное законодательство Российской Федерации.

Относительно вопросов, связанных с предупреждением неправомерного доступа к компьютерной информации, то они так требуют более конструктивной проработки. Ожидаемый результат несомненно должен привести к стимулированию увеличения показателей эффективности борьбы с преступлениями данного характера.

Дефицит исследования криминологической характеристики незаконного доступа к компьютерной информации, отсутствие системы мер, направленных на предупреждение, а также вопросов касательно виктимологической профилактики, требования к развитию уголовного законодательства, системный анализ правовых и организационно-технических мер, препятствующих незаконному доступу к компьютерной информации, обусловили выбор темы дипломной работы. Относительно актуальности, то сомнений в значимости и особой важности данной сферы нет.

Объектом изучения дипломной работы выступают общественные отношения, которые подвержены посягательствам извне, в итоге незаконного доступа к компьютерной информации.

Говоря о предмете исследования, то он заключает в себе следующее: преступная деятельность в сфере информационных технологий, как новообразованный объект уголовно-правового регулирования, ее текущее состояние, состав и динамику; криминологические стороны правонарушений в сфере информационных технологий; комплекс превентивных мер направленных на снижение преступлений в данной сфере; правовые, организационно-технические приемы защиты от преступных посягательств в сфере информационных технологий.

Цель дипломной работы состоит в системно уголовно-правовом и криминологическом научном исследовании происхождения, текущего положения, различных тенденций и их сменяемости, специфических свойств, превентивных мер по противодействию преступления закона в сфере информационных технологий в Российской Федерации. Посредством данной цели ставятся более определенные задачи данного исследования, а именно:

- анализ норм права, которые устанавливают уголовную ответственность за преступные деяния в сфере информационных технологий;
- изучение задач связанных с квалификацией преступных деяний и вопросов, связанных с привлечением к уголовной ответственности;
- систематизировать доминирующие отличительные черты лиц компьютерных преступников, которые совершают преступления в сфере информационных технологий;
- обозначить существенные факторы и условия, содействующие совершению преступлений в сфере информационных технологий;
- разработать общий регламент, направленный на защиту компьютерных данных на объектах информатизации и предписания по защите компьютерной информации;
- установка превентивных организационно-правовых мер для минимизации незаконного доступа к компьютерным данным;
- разработка плана по дальнейшему развитию комплекса мер превентивного характера – уголовно-правовых и организационно-технических, которые будут направлены на повышение эффективности их реализации в противовесе с преступлениями закона в сфере информационных технологий.

Содержание представленной дипломной работы не ставит перед собой задачу тщательного описания всех аспектов правонарушений, ввиду недостаточной степени разработанности данного вопроса на сегодняшний день. Потребность в скорой подготовке юридических принципов, регулирующих взаимодействия в информационном поле, привела к непроработанному и в отдельных случаях к неточной разработке некоторых основных правовых понятий в данной сфере, с последующей корректировкой, иными словами уточнениями в будущих нормативных актах. Сегодня, после разработки и вступления некоторых базовых нормативных актов в области информационных отношений, настало время для их реализации на практике. Источником теоретической стороны представленной дипломной работы выступают результаты исследований отечественных ученых-правоведов, а также

специалистов в области уголовного права, криминологии, и информационных технологий таких как: В.В. Крылова, М.Ю. Дворецкого, М.М. Карелиной, Ю.М. Батурина, О.Я. Баева, Д.А. Ястребова, С.И. Ушакова, А.П. Кузнецова, В.Е. Козлова, Г.Н. Борзенкова, В.С. Комиссарова, Д.В. Ведеева, В.С. Беляева и др., а также работы зарубежных специалистов: Д. Айкова, Дж. Вейценбаума, Н. Винера, Д. Керра, Д. Макнамара, С. Мэдника, и др.

Нормативной базой служит Конституция Российской Федерации, действующее уголовное законодательство Российской Федерации, закона РФ, указы Президента РФ, Правительства РФ. В основе статистических и иных данных, отражающих текущее положение, при разработке применялись данные полученные на официальном сайте статистики ГИЦ МВД России, а также результаты работы CyberCrimeCon, лаборатории Касперского и др.

В качестве методологической базы были приняты общенаучные способы изучения, а также эмпирические методы:

- историко-правовой – касается исследования исторической практики по определению уголовной ответственности за свершение преступлений в сфере информационных технологий;
- формально-правовой – суть которой в более тщательном анализе уголовно-правовых и организационно-технических мер, направленных на противопоставление незаконному доступу к компьютерным данным.

Состав дипломной работы содержит введение, 2 главы и заключение. Каждая глава направлена на изучение компьютерной информации, как предмета уголовно-правовой защиты, детальному уголовно-правовому и криминологическому анализу правонарушений в сфере информационных технологий, так и международной и отечественной практике противодействия с нарушениями закона в области информационных технологий.

1. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА СОСТАВОВ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ПРОБЛЕМЫ ИХ КВАЛИФИКАЦИИ

1.1 Компьютерная информация, как объект уголовно-правовой охраны

Динамический процесс развития информационных и коммуникационных технологий, как и тотальная информатизация современного общества стали предпосылками, которые подтолкнули к необходимости ввода в правовую систему Российской Федерации юридических норм, регулирующих общественные отношения, ввиду посягательств в сфере информационных технологий преступных и иных элементов. Свое начало Российская практика регулирования отношений в информационном поле берет с начала 90-х годов и содержало некоторые ведущие законы, такие как: Закон «О средствах массовой информации», Закон «О Федеральных органах правительственной связи и информации», Закон «О правовой охране программ для электронных вычислительных машин и баз данных», который в последствии утратил силу с 1 января 2008 г., Закон «Об информации, информатизации и защите информации» (утратил силу с 09.08.06), Закон «Об участии в международном обмене», Закон «О правовой охране программ для электронно-вычислительных машин и баз данных», так же утративший силу с 1 января 2008 г.

От начала 2008 года, а именно с 1 января все правовые отношения, формирующиеся в сфере сбора, обработки, накопления, хранения, реализации, передачи информации и данных, как и применение компьютерной техники, средств хранения, обработки информации и данных, каналов связи, различных телекоммуникаций в т.ч. регулируются частью четвертой Гражданского кодекса Российской Федерации. Последняя в свою очередь включает в себя один раздел VII «Права на результаты интеллектуальной деятельности и средства индивидуализации». Раздел, направлен на правовое регулирование отношений в сфере интеллектуальной собственности, является комплексом всех действующих норм, федеральных законов в единый законодательный акт.

При всем этом в сферу интеллектуальной собственности включается серия принципиально новых субъектов отношений и конкретизация их прав, это распространяется и к правам изготовителя без данных.

В приведенных законодательных актах были введены базовые термины и понятия, относящиеся к сфере информационных технологий, решались аспекты ее распространения, защиты авторских прав, имущественные и неимущественные отношения, которые возникали в результате создания, правовой охраной и применением программного обеспечения, а также новых информационных технологий.

К тому же было введено и описано в законе понятий и терминов касательно информационной безопасности и транснациального обмена информацией.

Однако при некоторых обстоятельствах сторона право применения наталкивается на определенные преграды при осуществлении правовых регламентов. Исходя из этого анализ законодательства, который направлен на регулирование информационных отношений, можно сделать вывод, что требуется более тщательное изучение правового содержания и принципов понятий, затрагивающих, как и содержание сути элементов информационных отношений, так и отношений регулирующийся с помощью уголовного закона.

Отечественное законодательство устанавливает и включает в понятие информация «данные о лицах, предметах, фактах, событиях, явлениях и процессах вне зависимости от формы их представления».[1] Однако, казалось бы, элементарное содержание понятия, не в полной мере отражает всю глубину понимания термина «информация», что делает трудоемкой задачу по ее применению как в законодательстве, литературе, так и в разговорной речи, ввиду широты и ее емкости.

---

[1]Модельный Уголовный Кодекс. Рекомендательный законодательный акт для Содружества Независимых Государств. Принят на 7-м пленарном заседании Межпарламентской ассамблеи государств-участником СНГ 17 февраля 1996г.//Приложение к информационному бюллетеню».1996.№10

В частности, в специализированном курсе «Информатики» приводятся такие понятия как «сообщение» и «информация» основными в информатике, но суть данных понятий нельзя раскрыть с помощью определений в законах, ввиду того что это привело бы к включению других не определенных им базовых понятий.[2]

Толковый словарь вычислительной техники и программирования приводит следующее описания понятия информация, как одной из начальных, не поддающихся определению в рамках кибернетики понятий.[3]

Стоит заметить, что применением данного термина как правило предполагает под собой образование материально-энергетического сигнала, который может быть зафиксирован сенсорно или на техническом уровне. В данных ситуациях по обыкновению информация трансформируется в сообщение. Для реализации системы приема-передачи требуется устройства соответственно приема и передачи, или иное средство связи. Касательно происхождения информации различают несколько мнений и точек зрения в кругу специалистов как информационной, так и юридической сферы. По нашему мнению, законодатель решает данный вопрос удовлетворительно, а если быть колее конкретным, то: разграничивает более четкие правовые рамки и формы, касательно того что подлежит защите в принятом законодательном порядке.

Подводя итог, можно сделать следующий вывод о том, что анализ принятого законодательства формирует порядок, по которому правовая охрана распространяется в первую очередь применительно к задокументированной информации, которая определена на физическом носителе с определенными атрибутами, другими словами та информация которая выражена к какой-либо форме и которую возможно распознать.

---

[2]Бауэр Ф.Л., Гооз Г. Информатика: Вводный курс./ Ф.Л.Бауэр, Г.С. Гооз. - М.: 1990. - С. 18.
[3]Заморин А.П., Марков А.С. Толковый словарь по вычислительной технике и программированию. Основные термин.// А.П. Заморин, А.С. Марков. - М., 1988. С. 68.

Под документированным данными понимают системную форму, которая идентифицируется как единая система: а) содержание информации; б) атрибуты, способствующие идентификации источника данных, целостности информации, степень ее точности, свойства и иные параметры; в) физический носитель информации, несущий в себе ее содержание, атрибуты, и реквизиты.

В.А. Копылов утверждает о том, что термин «документированная информация» базируется на двойственности, т.е. информация и одновременно материальный носитель, содержащий в себе набор символов, знаков, волн или иных методов отображения. В процессе документирования возникает своего рода материализация и овеществление данных. Таким образом напрашивается вывод о том, что информация переходит в разряд объектов Гражданского законодательства.

Стоит отметить, что Российское уголовное законодательство реализует правовую охрану как документированной информации, так и представлении ее в других видах, таким образом распространяет представление о предмете криминальной деятельности в более широком смысле. Изучение принятого Уголовного кодекса Российской Федерации демонстрирует придание особо статуса определенным информационным отношениям, на которые распространяются более тщательная механизмы защиты. Глава о правонарушениях в сфере информационных технологий пополнилась новыми терминами и понятиями, которых доныне не существовало как в уголовно-правовой терминологии, так и в законодательстве в целом, которое распространялось на регулирование отношений в информационном поле. Это связывается со стремительным развитием в науке и техническом прогрессе в данной области. Таким образом, ввиду сложности подобные термины и понятия сопровождаются дополнительными комментариями и пояснениями, для донесения полноты, которые они охватывают. Все это направлено на понимание особенностей технических параметров ново созданных средств обработки данных как новой составляющей уголовной-правовой и

криминалистической категории.[4] Безусловно, изучение терминов и понятий, используемых при описании правонарушений в сфере информационных технологий носит полезный характер, однако вне сомнений и то, что акцент смещен в сторону таких основных терминов как «информация» и «компьютерная информация».

В ходе анализа норм из разных отраслей права открывается возможность для подведения следующих следствий:

1. Информационные данные представляют собой систему направленных на передачу формализованных знаний и сведений о лицах, предметах, фактах, событиях, явлениях и процессах вне зависимости от их исходной формы представления.
2. Правовая охрана распространяется на любые виды документированной информации, другими словами на данные, которые материализованы в определенную форму, по которой ее можно идентифицировать.
3. Материализованная информация выступает объектом уголовно-правовой охраны.
4. Информационные данные подразделяются на конфиденциальную и массовую. Первая означает, что ознакомление и в целом доступ к оной ограничен автором или текущим собственником, иначе в рамках законодательства, вторая же распространяется свободно для всех соответственно.
5. Уровень допуска, или иными словами установление порядка использования данных определяется законом или правообладателем информации, которые в свою очередь устанавливают категорию доступности информации, либо ее частичную или полную конфиденциальность.

---

[4]Батурин Ю.М., Жодзинский А.М. / Компьютерная преступность и компьютерная безопасность// Ю. М. Батурин, А.М. Жодзинский. - М.: Юридическая литература, 1998. - С.52-54.

Под конфиденциальными данными с точки зрения закона являются следующие виды информации:

данные содержащие государственную тайну (охраняются Законом Российской Федерации «О государственной тайне» ст. ст. 275, 276, 283, 284 УК РФ);

данные передающиеся посредством переписки, телефонных переговоров, почтовых, телеграфных и других сообщений (гарантируется ч.2. ст.23 Конституцией РФ, ст. 138 УК РФ);

данные относительно тайны усыновления (ст. 155 УК РФ);

данные содержащие служебную тайну (ст. 139 ГК РФ), коммерческую тайну (ст. 139 ГК РФ и ст. 183 УК РФ), банковскую тайну (ст. 183 УК РФ), личную тайну (ст. 137 УК РФ), семейную тайну (ст. 137 УК РФ), информация, представляющая собой объект авторских и смежных прав (ст. 1255 ч. 4 ГК РФ);

6. Разнообразные формы незаконного завладения и использования конфиденциальных документированных данных без прямо выраженного согласия со стороны ее собственника (кроме особых случаев, прописанных в законодательстве) подпадают под нарушение прав, т.е. являются в этом случае неправомерными.
7. Незаконное использование документированной информации является наказуемым деянием.

Современное отечественное уголовное законодательство состоит в том числе из перечня прежде неизвестных составов преступлений, в число которых включены нормы, которые направлены на защиту компьютерных данных. Потребность определения уголовной ответственности за нанесение вреда, посредством применения компьютерных данных (в т.ч. данных на переносных и облачных хранилищах, хранящейся непосредственно на ЭВМ, или принадлежащих какой-либо сети) определяется ростом значимости и важности и более широкой интеграции ЭВМ практически во все значимые сферы деятельности человека.

Составы преступлений изложены в 28 главк Уголовного кодекса Российской Федерации, под названием «Преступления в сфере компьютерной

информации», состоящая из трех статей: «Неправомерный доступ к компьютерной информации» (ст. 272), «Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273) и «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» (ст. 274).

Обосновано то, что правонарушения данного вида размещены в разделе IX «Преступления против общественной безопасности и общественного порядка», ввиду того, что итоги незаконного использования информации и данных могут привести зачастую к непредсказуемым результатам, не говоря уже о базовом нарушении неприкосновенности интеллектуальной собственности, разглашении информации о частной жизни граждан, имущественный ущерб в виде прямых убытков и упущенной выгоды, нанесение вреда, порой непоправимого, для репутации компании, разнообразные виды нарушений штатной деятельности организаций, отрасли и др. Некоторые понятия и термины, применяемые в данной главе УК РФ, необходимо уточнить дополнительными комментариями. Труд М.М. Карелиной[5] в определенной степени облегчит усвоение перечисленных понятий, таких как:

- ЭВМ (компьютер) - устройство или система (несколько объединенных устройств) предназначенное для ввода, обработки и вывода информации;
- Сеть ЭВМ - совокупность компьютеров, средств и каналов связи, позволяющая использовать информационные и вычислительные ресурсы каждого компьютера, включенного в сеть независимо от его места нахождения;
- Компьютерная информация - в дополнение к определению, данном в ст. 2 закона "Об информации, информатизации и защите информации", необходимо заметить, что применительно к комментируемым статьям под компьютерной информацией понимаются не сами сведения, а форма их представления в машинном (компьютерном) виде, т.е. совокупность

[5]Карелина М.М. Преступления в сфере компьютерной информации / М.М. Карелина. - М., 1998.

символов, зафиксированная в памяти компьютера, либо на машинном носителе (дискете, оптическом, магнитооптическом диске, магнитной ленте либо ином материальном носителе). При рассмотрении дел следует учитывать, что при определенных условиях и физические поля могут являться носителями информации.

- Программа для ЭВМ (компьютера) - объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения;
- База данных - это объективная форма представления и организации совокупности данных (например, статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Одно из наиболее удачных формулировок понятия компьютерной информации, сформулировано доцентом кафедры криминалистики МГУ им. М.В. Ломоносова В. Крыловом, которое выделяет криминалистическое определение компьютерной информации как особого объекта незаконного покушения.

Компьютерная информация представляет собой сведения, знания иначе набор команд, если это программа, направленные на реализацию на ЭВМ, или управляющие ей, которые непосредственно хранятся на ЭВМ или на физических носителях, которые в свою очередь могут быть идентифицированы, как составная часть информационной системы, при наличии правообладателя, или распорядителя, которым и созданы правила ее использования.

Иначе говоря, система общественных отношений, подлежащих защите со стороны уголовного законодательства являются общим объектом для свершения компьютерных правонарушений; родовым является общественная безопасность и общественный порядок; видовым – система общественных

отношений по законному и надежному применению информационных данных; сам же объект рассматривается исходя из названий и содержаний конкретных статей. Должен разграничиться тот факт, что компьютерные данные могут представлять собой не только лишь объект посягательств, но и быть инструментом правонарушений, в случаях, когда электронно-вычислительная техника применяется для реализации иного незаконного покушения на третий объект. У данного утверждения имеется немало сторонников.[6]

Введение ее привело бы к обобщению границ ответственности понятия «компьютерное преступление» и созданию дополнительных препятствий в реализации функций как законодателя, так и правоприменителя. Создатели УК РФ избрали первый вариант, по которому определили содержание главы 28 в том смысле, что компьютерная информация в каждом отдельно взятом случае выступает только лишь предметом свершения незаконных действий в сфере информационных технологий. Однако, верным будет и тот факт, когда при реализации одного правонарушения, инструментом выступает другая компьютерная информация, то возникшие ранее отношения касательно последней непременно страдают, иными словами, она сама выступает в роли общественно опасного деяния. Не представляется возможным использование компьютерной информации в иных преступлениях закона, без начального нарушения охраны этих данных. Иначе говоря, не совершив действий, которые классифицируются в ст. 20 Федерального закона «Об информации, информатизации и защите информации», а именно: утечка, утрата, модификация, подлог, ликвидация, копирования, блокирования и иные действия противоправного характера на информационных ресурсах и системах.

Можно допустить, что данные на отдельно взятом компьютере могут и не пострадать, при использовании его только авторизованным пользователем, однако атаке могут подвергнуться те устройства, которые находятся с ней в одной сети. Как следствие, за реализацию банального хищения средств

---

[6]Ответственность за неправомерный доступ к компьютерной информации/ Кочои С., Савельев Д., //Российская юстиция. - 1999 - № 1

посредством электронных инструментов наступает ответственность по правилу идеальной совокупности преступлений.

Описывая существенную сторону приведенных составов, стоит отметить для начала, что подавляющее большинство из них изложены как материальные, из этого следует что предполагается как совершение общественно опасного деяния, так и наступление общественно опасных последствий, и установление в любом случае причинно-следственной связи между перечисленными признаками. Тем не менее в ввиду ч. 2 ст. 9 УК РФ, временем свершения всех этих преступлений будет считаться время завершения именно незаконной деятельности вне зависимости от времени наступления последствий. Конкретно сами общественно опасные деяния выражаются чаще в виде каких-либо действий, нежели бездействий. В итоге из всех отличительных черт субъективной стороны весомым будет только лишь вина. Наряду с этим, по ч. 2 ст. 24, для всех правонарушений представленного типа обязательно засвидетельствование вины в форме умысла. Предполагается, что особо трудоемким будет задача, связанная с различением неосторожного и невиновного причинения вреда, что в разы увеличивает сложность и замаскированность процессов, протекающих в объединенных сетях, системах ЭВМ и кластерах.

Позициистатей, представленных в 28 главе по большей части, носят описательный и чаще бланкетный характер, иначе отсылочный. Так для их реализации часто приходится обращаться к ст. 35 УК РФ, к нормативно-правовому акту о защите компьютерной информации, регламенту эксплуатации ЭВМ и другим. Санкции – альтернативные, кроме двух квалифицированных составов, где они ввиду особой тяжести последствий правонарушений ограничены до относительно-определенных. Так же в глава 28 «Преступления в сфере компьютерной информации» включается в себя нормы, не имеющие обратной силы, иными словами такие, которые устанавливают незаконные деяния, увеличивают ответственность, или другим способом ухудшают положение лица, в отношении которого выдвинута данная статья.

1.2Неправомерный доступ к компьютерной информации: состав преступления, проблемы квалификации

Статьей 272 УК РФ предусмотрена ответственность за незаконный доступ к компьютерным данным, следствием которой стало ликвидация, блокирование, модификация, хищение, посредством копирования, или нарушение работы вычислительных систем.[7]

Приведенная статья направлена на охрану права лиц на неприкосновенность информации в системе. Владельцем информационной вычислительной системы, а также информационных данных в ней, выступает любое лицо, законно пользующееся сервисом по переработке информации как собственник отдельно взятой вычислительной системы, сети, или как лицо, которое приобрело право на пользование системы, данных, согласно ст. 1280 ч. 4 ГК РФ. Эта статься охраняет компьютерную информацию всех организаций, учреждений и частных лиц. Диспозиция соответствующей нормы состоит в незаконном доступе к охраняемым законом компьютерным данным. Незаконная деятельность, ответственность за которое предусмотрено ст. 272, заключается в незаконном доступе к защищенным законом компьютерным данным, сопровождающийся определенным алгоритмом действий, и проявляется посредством проникновения, взлома, несанкционированного доступа в компьютерную систему, посредством специальных технических или программных средств, предоставляющих возможность обойти штатную систему безопасности; неправомерного использования действующих идентификационных данных, маскировка под авторизованного пользователя для получения доступа в компьютерную систему, кража носителей данных, находившихся под защитой, которое в конечном результате привело к ликвидации или блокированию информационных данных.

---

[7]Комиссаров В.С. Преступления в сфере компьютерной безопасности: понятие и ответственность/ В.С. Комисаров // Юридический мир. 2003. -№2. -С.13

Под защитой законом информационными данными подпадают те из них, к которым применим особый режим ее правовой охраны, т.е. это государственная, служебная, коммерческая тайна, персональные и иные данные. Под незаконным доступом понимают неправомерные действия, которые регулируются правовыми нормами, отдельными законами, актами управления, приказами, распоряжениями и другими, нарушающие режим доступа к информационным данным. Вдобавок к этому, незаконным доступом считается неправомерное использование со стороны какого-либо лица технических средств для обхода системы защиты на ЭВМ или ее сети. Это может быть, например, использование чужого пароля, подмены пароля, или ее снятия, модификации программы и т.п. Аналогично и касается ситуаций самовольного получения информации без разрешения на это ее собственника или автора.

Данная статья, состоит из 2 частей, и включает в себя довольно много признаков, являющихся обязательными для объекта, объективной и субъективной стороны состава преступления. Опираясь на диспозицию ст. 272 УК РФ, стоит отметить такие обязательные признаки объективной стороны незаконного доступа к охраняемой законом компьютерным данным.

Общественно опасные последствия, проявляющиеся в уничтожении, блокировании, изменении при копировании компьютерных данных, нарушении работоспособности ЭВМ или их сетей. Просматриваемой причинно-следственных связей между совершенным деянием и наступившими в результате последствиями. Недостаток одного из перечисленных ранее признаков исключает уголовную ответственность за преступление по 272 статье УК РФ. При практической деятельности возникают затруднения с трактовкой термина «неправомерный доступ к компьютерной информации», но четкое понимание данного понятия необходимое условие для дачи верной квалификации рассматриваемых общественно опасных деяний. Бытует мнение, что доступ считается незаконным при условии несанкционированного обращения к ресурсам ЭВМ и их сети лица, у которого в принципе отсутствуют

права доступа. Более четким в понимании данного понятия можно привести вариант предложенный Ю.А. Красиковым, которое гласит, что незаконным доступом считается не только при отсутствии такого права, но и при отсутствии правил защиты компьютерной информации.

Стоит также акцентировать внимание на том, что сегодня тот уровень технического прогресса в области компьютерных технологий, вдобавок степень сложности компьютерных программ дошли до такого высокого уровня, что появляется вероятность сбоя в работе ЭВМ, их систем, или их сети. Поводом для нештатной работы могут явиться и другие факторы, таки как несовместимость аппаратного железа и программного обеспечения.

По мнению В.В. Воробьева «если выполнение компьютером такой функции, как охрана информации от несанкционированного доступа, считать нарушением защиты информированных ресурсов становиться решаемой». Предполагается, что в складывающейся ситуации привлечение лица к уголовной ответственности является недопустимым, а различие преступного деяния от непреступного, по нашему мнению, возможно по наличию или отсутствию причинно-следственных связей между действиями лица, которым был совершен незаконный доступ к охраняемым законом данным и наступившие в следствии этого сбои в работе ЭВМ, их систем, кластеров, или их сети.

По нашему мнению, незаконный обход системы защиты данных в этом случае можно трактовать как оконченное преступление, квалифицирующееся по ст. 272 УК РФ. Действия, направленные на несанкционированное получение доступа к защищаемым законом данным, признается покушением на неправомерный доступ. Иными словами, деятельность лица, формально относящиеся к осуществлению незаконного доступа к компьютерным данным, в результате которых не было выявлено нарушений работы ЭВМ или их сети по независящим от лица обстоятельствам квалифицируется по ст. 272 УК РФ со ссылкой на ч. 3 ст. 30 УК РФ.

Как ранее упоминалось, состав преступного деяния изложен как материальный, к тому же деяние определено в форме действия и подразумевает обязательное наступление одного из перечисленных далее итогов:

- уничтожение данных, иными словами безвозвратное удаление информационных данных на физическом носителе, что подразумевает невозможность ее воссоздания на нем;
- блокировка информационных данных, или действия, повлекшие к ограничению или закрытию доступа к компьютерной системе и соответственно данным находящимся внутри нее;
- изменение информационных данных, замена исходных кодов программ, баз данных, текстовых данных, которые хранятся на физическом носителе;
- заимствование информационных данных, путем копирования и переноса информации на другой физический носитель, при неизменяемости исходных данных;
- нарушение работы ЭВМ, их объединений, или их сети, которое влечет за собой сбои в работе начиная от отдельно взятых программ и приложений, баз данных, выдача искаженных данных, заканчивая внештатной работой аппаратных средств, периферийных устройств, или же сбой в нормальной работе сети.[8]

Одним из главных задач является соотнесения причин и следствий в результате незаконного доступа. При использовании сложных компьютерных архитектур появляется вероятность уничтожения, блокирования или сбоя работы ЭВМ, в следствии технических ошибок в программном обеспечении или неисправностей. В данной ситуации, лицо которым был совершен незаконный доступ к компьютерным данным не может быть привлечено к ответственности ввиду отсутствия причинной связи между действиями и наступившими последствиями.

---

[8]Ответственность за неправомерный доступ к компьютерной информации/ Кочои С., Савельев Д., //Российская юстиция. - 1999 - № 1

Представленное преступление можно назвать оконченным именно в то мгновение, когда таковое предусмотрено данной статьей, а именно наличие определенных последствий. Иными словами, все манипуляции до запуска конечной команды или иной операции со стороны лица, совершающего незаконный доступ, носят характер неоконченного преступления.

Причины и преследуемые задачи данного правонарушения могут быть разнообразными. Как например, корыстными, месть, зависть, ставящих перед собой задачу добычи какой-либо информации, желание причинить вред, или спортивный интерес, чтобы проверить свои профессиональные способности и самоутвердиться.

Предметом преступления выступают компьютерные данные. Диспозиция статьи относительно этого, требует четкого представления рассмотренных ранее дефиниций – ЭВМ (компьютер), Сеть, Система компьютеров, Носитель информации (физический носитель) и прочие.

Объектом являются общественные отношения, относящиеся к безопасности использования компьютерных данных.

Объективная сторона данного преступления составляет незаконный доступ к защищенным законом компьютерным данным, который абсолютно всегда определяется как совершение определенных манипуляций, и сводится к проникновению в компьютерную систему с помощью следующего ряда атрибутов:

- применением специализированных технических или программных средств, предоставляющие возможность нарушения и обхода действующей системы безопасности данных;
- неправомерное обращение к действующим паролям, кодам доступа, для получения доступа к компьютерным данным, или иные способы и методы направление на получение доступа в закрытую ранее сеть, под видом авторизованного пользователя;

– кража носителей информации, в процессе которой были преодолены меры по их защите, конечный результат – это уничтожение или блокирование данных.

Несмотря на диспозицию ст. 272 УК РФ, в которой нет четких установок касательной субъективной стороны незаконного доступа к компьютерным данным, однако при реализации данного общественно опасного деяния безусловно речь ведется об умышленной форме вины в виде прямого или косвенного умысла. При таком положении дел виновное лицо дает себе отчет, что осуществляемые действия носят незаконный характер, а именно неправомерный доступ к компьютерной информации, которая в свою очередь находится под протекцией закона, тем самым понимает какие возможны последствия для данных, это как уничтожение или блокирование информации, копирование, модификация, изменения данных, нарушение работы ЭВМ, их системы, или их сети и желает наступления указанных преступных последствий, или же умышлено их допускает, иначе имеет к ним безразличное отношение. А.А. Толкаченко выделяет, что субъективная сторона подобного правонарушения носит только умышленный характер, иными словами лицо, которое тем или иным способом осуществляет незаконный доступ к данным, принимает во внимание факт возможности уничтожения, блокирования и иных изменений, если начальной его задачей это не является, иначе может добиваться других установок.

Не все авторы разделают подобный подход, например, С.А. Пашин допускает, что данное правонарушение может быть результатом действий, совершенных по неосторожности, причем степень вины в этом случае может проявляться при оценке лицом законности своего доступа к компьютерным данным, аналогично и касательно неблагоприятных результатов доступа, которые предписаны диспозицией данной нормы уголовного закона.

В процессе квалификации подобных правонарушений затруднительным и емким становится установление в действиях лица вины в виде умысла, а не действий по неосторожности, это связывают с тем что при разных состояниях

вычислительной системы одни и же манипуляции могут к конечному итогу приводить к разным и порою неожиданным результатам. Стоит подчеркнуть, что это в любом случае, было ли деяние совершено по неосторожности или же с каким бы то ни было умыслом.

Тем не менее подобный подход вступает в противоречие с нормой ст. 24 УК РФ, которое гласит, что деяние, которое было совершено только по неосторожности, считается правонарушением только в тех случаях, когда это специально учтено соответствующей статьей Особенной части УК. Из этого можно сделать вывод, о том, что незаконный доступ к защищаемым законом компьютерным данным, который характеризуется свойствами неосторожной формы вины преступлением не является. Диспозиция ст. 272 УК РФ четко устанавливает характер действия, связанный с доступом, в связи с компьютерными данными, находящихся под защитой закона, что он обязан иметь неправомерный характер, т.е. если у лица нет прав доступа к данной информации; если у лица есть определенные права доступа к данной информации, однако осуществляются они вразрез установленному порядку, с несоблюдением правил ее защиты. Приведенная выше ситуация носит характер общественно опасного, а таком случае перечисленные действий виновного можно классифицировать как деяния имеющий прямой или косвенный умысел. Данное лицо осознает к тому же возможное наступление указанных в законе общественно опасных последствий, в случае если таковое является целью, то здесь имеет место прямой умысле, иначе если такие последствия допускаются, либо в отношении них проявляется безразличие то это является косвенным умыслом.

Совершенно другой вариант развития событий при признании возможности совершения лицом таких действий по неосторожности. Тогда, при осознании лицом факта незаконности доступа по отношению к компьютерным данным, которые находятся под защитой закона, то данное лицо изначально действует умышленно, и ни о какой неосторожной форме вины идти речи не может, кроме случаев легкомыслия и небрежности. Первое имеется ввиду,

когда лицо совершающее неправомерный доступа предполагало предотвращение последствий, второе же ввиду не проявления достаточной внимательности и предусмотрительности. Аналогичные ситуации рассматриваются и в ст. 274 УК РФ, который состоит в умышленном представлении характера рассматриваемого события, а также в диспозиции ст. 272 УК не определено обратное. Итак, при незаконном доступе к компьютерным данным законодатель не сообщает совершение умышленных действий с неосторожным наступлением последствий, из этого следует что субъективная сторона этого состава проявляется только лишь в форме умысла.

Можно подвезти итог, о том, что в приведенном общественно опасном деянии, при котором виновный всецело осознает факт незаконного доступа к защищаемым законом компьютерным данным, так же осознает характер, а именно, как общественно опасный, предполагается вероятность или неизбежность наступления преступных последствий, нарушения работы ЭВМ, их системы, или их сети, преследует цели их наступления или проявляет безразличное отношение.

В составе преступления, согласно ст. 272 УК РФ, конструктивной составляющей прямого умысла составляет предвидение вероятности или неизбежности наступления общественно опасных последствий; волевой стороной умысла есть желание, выявляемое в отношении наступления общественно опасных последствий.

С точки зрения субъективности правонарушения, то ее отличительной чертой является факт прямого умысла (под этим подразумевается осознанность незаконного доступа, предположение вероятности наступления опасных последствий, или желания их наступления), иначе косвенного (осознанность незаконного доступа, предположение вероятности наступления опасных последствий, и допущение их наступления, или характер безразличного к ним отношения). Незаконный доступ к компьютерным данным – умышленное

деяние, так как в диспозиции ст. 272 УК не указано обратное.[9] Лицо, которое стремится получить доступ к данным, в первую очередь должно осознавать, что пытается получить доступ к данным которые не распространяются в свободном доступе, а значит к ним применены методы защиты, и соответственно права на доступ к подобным данным у него отсутствуют. О наличия определенных умыслов будут сигнализировать системы защиты данных от несанкционированного доступа (шифрование, коды доступа, ключи и др.), которые необходимо нарушить, для открытия доступа к данным, вывод на интерфейс устройств предостерегающих уведомлений, устные предупреждения о запрете доступа к данным и т.п.

В качестве субъекта подобного правонарушения чаще выступают лица, имеющие определенный опыт взаимодействия с компьютеризированными системами, и обладают навыками в информационной сфере, так же ввиду профессиональных знаний и наличия некоторого опыта они должны предвидеть вероятные последствия уничтожения, блокирования, модификации данных, либо нарушение работы ЭВМ, их системы, их сети, в результате вмешательства со стороны. Общее правило для субъектов, правонарушений, которые классифицируются по ст. 272 это достижение 16-летнего возраста, за исключением ч. 2 ст. 272, которая предполагает наличие специального субъекта, совершившего данное правонарушение.

В правонарушении, согласно ст. 272 УК РФ, незаконный доступ к компьютерным данным может производиться следующими категориями лиц:

А. не имеющими права на доступ к компьютерной информации в данных условиях места и времени, но осуществляющими "неправомерный доступ к охраняемой законом компьютерной информации" (ч. 1 ст.272);

Б. совершающими неправомерный доступ группой по предварительному сговору или организованной группой (ч.2ст.272);

---

[9]Научно-практический комментарий к УК РФ в двух томах. Т.2.Новгород: - НОМОС,1996г.С.134

В. совершающими неправомерный доступ, используя для этого свое служебное положение (ч.2ст.272);

Г. имеющими право доступа к ЭВМ, системы ЭВМ или их сети, но использующими это право в целях достижения преступного результата (уничтожение, блокирование, модификации либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети).

В соответствии с частью 1 статьи санкция основного состава подразделяется на три вида наказаний: штраф, исправительные работы и лишение свободы. Штраф также подразделяется на два вида: первый до двухсот тысяч рублей или кратный размеру заработной платы или иного дохода, осужденного за период до восемнадцати месяцев). Исправительные работы варьируются промежутком времени от шести месяцев до одного года, и наконец лишение свободы сроком до двух лет.

В соответствии с частью 2 статьи санкция была ужесточена. В ее состав был включен новый вид наказания - это арест на срок от трех до шести месяцев, размеры же прежних наказаний увеличены. Штраф от ста тысяч до восьмисот тысяч или зарплаты за период от одного года до двух лет; исправительные работы на срок от одного года до двух лет; лишение свободы до пяти лет. Все формы наказаний прописанных в ч.1 и ч.2 являются основными и не исключают вероятности присоединения какого-либо из дополнительных видов, предусмотренных в п. п. 2 и 3 ст. 45, исключая штрафа и конфискации имущества.

Для установления аспектов незаконного доступа к компьютерным данным и различия его от смежных правонарушений сотрудникам правоохранительных органов следует прибегнуть к методу юридического анализа, который позволит изучить отдельно взятое преступление с разнообразных сторон и выявить его конструктивные признаки. При всем этом важно отметить на что конкретно направлено противоправное действие, чему она угрожает, и чему наносит вред, либо создает угрозу причинения вреда; рассмотреть внешнюю объективную сторону правонарушения, которая

характеризует само деяние, установить факт действия или же бездействия, наступившие последствия и причинно-следственную связь между ними; внутреннюю субъективную сторону правонарушения, которая определяет представление о психическом отношении лица к содеянному и его последствия, речь идет об умысле (прямой или косвенный), неосторожности (небрежность, либо легкомыслие), мотив поведенческого акта субъекта и его конечная цель; характеристику самого субъекта преступного посягательства.

Для правонарушений, относящихся к ст. 272 УК РФ, главным аспектом общественно опасного деяния является незаконный доступ к компьютерным данным. При этом состав незаконного доступа к компьютерным данным отличается от создания, реализации и распространения вредоносных программных обеспечений для ЭВМ построен как материальный. Это правонарушение будет считаться оконченным именно в тот момент, когда проявятся вредные последствия, лежащие в причинной связи с поведенческим актом виновного.

1.3 Создание, использование и распространение вредоносных программ для ЭВМ, состав преступления, проблемы квалификации.

Статья 273 предусматривает ответственность, которая наступает за создание и распространения разнообразных компьютерных «червей» и других программ и приложений, которая наносят вред целостности данных, нарушают нормальную работу компьютера, или сети ЭВМ. Использование, или распространение вредоносного программного обеспечения подразумевает под собой инсталляция их в компьютер, систему ЭВМ или их сеть, как и продажа, обмен, дарение или безвозмездная передача третьим лицам.[10] Статься призвана охранять права владельца компьютерной системы на неприкосновенность и целостность хранящихся на ней данных. Прежде всего, компьютерный вирус

[10]Кузнецов А. П. Ответственность за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (ст. 274 УК РФ) / А. П. Кузнецов // Правовые вопросы связи. -- 2007. -- № 2.

или червьможет и не оказывать влияние на информацию, которой необходимо гарантировать целостность. Во-вторых, есть огромное количество типов программ, установка и использование которых, в особенности в неумелых руках может привести к плачевным результатам, однако они не подпадают под устоявшееся понятие компьютерного червя.

Вредоносными программным обеспечениями с точки зрения ст. 273 УК РФ считаются программы, изначально написанные для нарушения нормального функционирования компьютерных программ и приложений. Нормальное функционирование имеет ввиду исполнение операций исходных программ, для которых эти программы и писались, определения приводятся обычно в документации или в лицензионном соглашении. Из самых распространенных типов вредоносных программ стоит отметить такие как «компьютерные вирусы» и «логические бомбы».[11]

Компьютерный вирус – программа, способная к самораспространению на зараженной машине, модификации других программ с целью внедрения собственного кода в них, последнее приводит к нарушению работоспособности.

Логическая бомба –намеренное изменение части кода, или дополнение его какой-либо программы, системы ЭВМ, в результате чего она перестает частично или полностью функционировать. Может сопровождаться определенными алгоритмами, и запускаться только при выполнении определенных условий. Главным различием «логической бомбой» от «компьютерного вируса» является то, что с самого начала первая является частью программы и не распространяется на другие, а вторые же по своей сути являются более динамичными программами и способны распространяться как по самой зараженной машине, так и по сети, к которой она принадлежит. Правонарушение, предусмотренное ст. 273, является наиболее опасным из перечня в 28 главы, что и прослеживается в санкциях за его совершение.

---

[11]Безруков Н.А.Введение в компьютерную вирусологию. Общие принципы функционирования, классификация и каталог наиболее распространенных вирусов в MS DOS / Н.А. Безруков. - Киев, 2006. - С.86

Состав преступления по ч. 1 ст. 273 УК РФ, считается урезанным именно по такому фактору как «создания программ для ЭВМ или внесение изменений в существующие программы».

Объектом данного правонарушения являются общественные отношения по безопасному применению ЭВМ, ее программного обеспечения и информационного содержания.

Состав части 1 в сущности формальный и предполагает осуществление одного из следующих действий:

1. написание программ для ЭВМ, изначальной целью которых является несанкционированное уничтожение, блокирование, модификация, изменение, копирование информации, нарушение работы аппаратного «железа»;
2. внесение в существующие программы изменений, обладающих аналогичными свойствами п.1;
3. использование двух перечисленных видов программ;
4. распространение;
5. использование физических носителей с таким программным обеспечением.
6. распространение таких носителей.

Конечно, данный состав является формальным и не требует наступления каких-либо последствий, уголовная ответственность наступает уже на стадии написания, т.е. создания программы, вне зависимости была ли данная программа использована или же нет.[12] Создание вредоносных программ для ЭВМ в технологическом смысле сопоставимо с пунктами создания любых других программ и подразумевает под собой целенаправленную деятельность, которая состоит из следующих частей:

1. постановка задачи, решение вопроса связанного со средой распространения и конечного назначения программы;

---

[12]Комментарий к уголовному кодексу РФ. Научно-практический комментарий/Отв.ред.В.М.Лебедев.-М.Юрайт-М,2004.С.560

2. отбор средств и языка программирования;
3. написание программы;
4. тестирование жизнеспособности такой программы и соответствие поставленным задачам;
5. подготовка программы к реализации.

В трудах В.В. Крылова отличительной чертой является конечный пункт в стадиях создания вредоносных программ для ЭВМ, а именно фаза непосредственного запуска и действия программы, предоставление информации. Кажется, что действия такого характера не имеют отношения к процессу создания и распространения вредоносных программ.

На наш взгляд, всякое из упомянутого ранее этапа характеризуется признаками создания вредоносной программы, и таким образом может быть определено как правонарушение, которое предусматривается ч. 2 ст. 273 УК РФ, хоть даже в том случае, если вредоносная программа не завершена, или находится в стадии планирования. Наша позиция, касательно таких действий не рассматривать их как подготовительные, так как понятие «создание» программы сформулировано законодателем как процесс, а не конечный результат, а подобные действия в этом русле составляют признак объективной стороны состава данного правонарушения. Тем не менее, стоит подчеркнуть, что при ряде обстоятельств создаются исключения, которые не подпадают под уголовное преследование при использовании таких программ. В первую очередь это имеет отношения к организациям, которые занимаются разработкой антивирусных программ и иных средств защиты, и которые к тому же имеют лицензию на подобный род занятий, предоставленную Государственной технической комиссией при Президенте.

Если прибегнуть к анализу состава преступления, которая классифицируется ст. 273 УК РФ, то можно отметить несколько подходов в установлении объективной стороны. К слову, Ю.А. Красиков отмечает что «субъективная сторона этого преступления характеризуется прямым умыслом, законодатель в ч. 1 ст. 273 УК указывает на заведомый характер деятельности

виновного; при производстве новой программы или модификации уже имеющейся, виновное лицо осознает характер своих действий, и предполагает вероятность уничтожения, модификации, блокирования или копирования каких-либо данных, и желает совершить эти действия». На взгляд С.А. Пашина же, производства, реализация и распространений вредоносных программ для ЭВМ – это правонарушение, которое совершается только с прямым умыслом; лицо осознает тот факт, что программа характеризуется как вредоносная, и очевидно знает, какие последствия она в состоянии вызвать.

Как следствие, создание программ для ЭВМ, или модификация существующих, которые в результате поспособствуют к незаконному уничтожению, блокированию, изменению, копированию данных, вмешательству в работу ЭВИ, их системы, или их сети, иначе применению подобных программ классифицируется как оконченное правонарушение, вне зависимости от наступления последствий, перечисленных в Уголовном законе. Элементарным условием совершение факта правонарушения признается наличие хотя бы одного действия, альтернативно приведенного в диспозиции ч. 1 ст. 273 УК РФ. В плане интеллектуального прямого умысла в приведенных составах правонарушений является такое состояние сознания подозреваемого, когда он осознавал, иначе допускал возможности, о том, что создаваемые или применяемые им программные обсечения обладают свойствами вредоносного характера, предполагал вероятность наступления общественно опасных последствий в виде уничтожения, блокирования, изменения или копирования данных, вмешательство в нормальную работу ЭВМ, их системы, или их сети, и тем не менее желал реализации данных программ.

Как видно из анализа ч. 1 ст. 273 УК РФ, на законодательном уровне определения данного состава правонарушения как умышленного мы не наблюдаем. В данных ситуация, для классификации вины лица, требуется обращение к ч. 2 ст. 24 УК РФ, которая предусматривает, что действия, носящие характер неосторожного, считаются правонарушением при условии, если таковое предусмотрено соответствующей статьей Особенной части УК РФ

присутствует только в квалификационных составах. Поэтому по смыслу ст. 27 УК РФ, если в итоге совершения умышленного правонарушения нанесены тяжкие последствия, влекущие по закону более строгое наказание и которое не охватывалось умыслом лица, то уголовная ответственность за такие последствия наступает только в случае, если лицо предполагало вероятность их возникновения, однако без достаточных к тому оснований самонадеянно полагало их предотвратить, или в случае, если лицо предвидело, но должно было и могло предвидеть вероятность наступления этих последствий; в конечном итоге такое правонарушение считается совершенным умышленно.

Необходимыми признаками объективной стороны ч. 1 ст. 273 являются два аспекта, которые характеризуют способ и средство совершения правонарушения. Прежде всего это, то, что результаты деяния должны носить характер незаконного, а далее наличие самой вредоносной программы или модификации отдельных программ.

Крайним, помимо описанного компьютерного вируса, являются такие явления в сфере информационных технологий как «логическая бомба», «люк», «асинхронная атака» и иные.

С субъективной стороны состав данного правонарушения характеризуется виной в форме прямого умысла: в случае если виновный представлял общественную опасность результатов своих деяний, предполагал вероятность наступления таких последствий, однако несмотря на этом желал эти действия совершить, иными словами создание вредоносных программ конечной своей целью имело бы незаконное уничтожение, блокирование, изменение, копирование данных, или вмешательство в работу ЭВМ. Реализация подобных вредоносных программ аналогично может происходить умышленно.

При определении факта прямого умысла в действиях подозреваемого правонарушение подлежит квалификации исходя из изначальных целей и задач, которые были поставлены подозреваемым, иначе если последствия настали, то исходя от их тяжести и опасности. В данном случае деяния, которые подпадают по статью являются лишь способом достижения поставленной цели, а

совершенное деяние подлежит квалификации по классической совокупности совершенных правонарушений.[13] Требуется к тому же учесть, что правонарушение могло быть совершено по неосторожности в виде легкомыслия, как и в случае с косвенным умыслом в виде безразличного отношения к вероятным последствиям.

Субъект правонарушения – общий, иными словами субъектом этого правонарушения может приходиться любой гражданин, который достиг шестнадцатилетнего возраста. Объективной стороной правонарушения, предусмотренной ст. 273 УК РФ, являются следующие неправомерные действия:

1. Написание программ для ЭВМ, изначально приводящие к общественно опасным последствиям.
2. Модификация существующих отдельно взятых программ для ЭВМ, в конечно результате приводящие к общественно опасным последствиям.
3. Реализация таких программ или физических носителей с подобными программами.
4. Распространение подобных программных обеспечений или физических носителей с оными приложениями.

Такого рода действия подозреваемого изначально приводят к незаконному уничтожению, блокированию, изменению или копированию данных, вмешательству в нормальную работу ЭВМ, их системы или их сети. Довольно серьезная степень общественной опасности, которую несет создание, реализация, распространение вредоносных программ для ЭВМ содействует развитию законодателем данного состава преступления как формального, когда достаточным является сам факт создания компьютерного вируса либо совершение иного из перечисленных в ч. 1 ст. 273 УК РФ деяний, которые составляют объективную сторону этого состава, для привлечения лица к

[13]Батурин Ю.М.Проблемы компьютерного права / Ю.М. Батурин.- М.: Юридическая литература, 1998. - С.14.

уголовной ответственности. Наступление общественно опасных последствий в подобное случае значения для квалификации не имеют.

Санкцией ч. 1 предусмотрен один основной вид наказания – это лишение свободы сроком до трех лет, и один дополнительный, который заключается в назначении штрафа в размере до двухсот тысяч рублей или заработной платы, или иного дохода лица за период до восемнадцати месяцев.

Часть 2 ст. 273 относится у более опасным видам правонарушений, а именно: те же деяния, однако повлекшие более тяжкие последствия. Тяжкие последствия относится к разряду оценочных, установкой которой занимается суд. Суду не следует ограничиваться ссылкой на соответствующий признак, а в обязательном порядке привести в описательной части приговора обстоятельства, которые в конечном итоге стали основанием для вывода о наличии в содеянном указанного признака.

Санкция второй части приведенной статьи является относительно-определенной: лишение свободы на срок от трех до семи лет. Иными словами, конкретно такое преступление из всей главы имеет отношение к категории тяжких.

Отдельно стоит обратить внимание на вопрос касательно различения незаконного доступа к компьютерным данным от процессов, связанных с написанием, реализацией и распространением вредоносных программных обеспечений для ЭВМ. Затруднения в связи с этим заключаются в том, что как незаконный доступ к компьютерным данным, так и написание, реализация, распространение вредоносного ПО для ЭВМ являются прямой дорогой к незаконному уничтожению, блокированию, изменению, копированию данных, вмешательству в нормальное функционирование ЭВМ или их сети. К тому же, создание программ для ЭВМ или модификация существующих программ, приводящие в конечно итоге к перечисленным ранее последствиям, вполне могут сопровождаться незаконным доступом к компьютерным данным, что в очередной раз подтверждает прикладной характер разграничения данных правонарушений. В первую очередь, как было замечено ранее, предмет

преступления, по ст. 272 УК РФ, выступает исключительно те информационные данные, которые находятся под защитой законодательства. А предметом написания, реализация, распространения вредоносного программного обеспечения для ЭВМ может быть любая информация, вне зависимости находится она под защитой закона или же нет, которая содержится на физическом носителе, ЭВМ, их системе, или их сети.

Для примера, согласно ст. 273 УК РФ необходимо квалифицировать деяния виновного, который совершил незаконный доступ к программе для ЭВМ, которая в свою очередь не подпадала под защиту со стороны закона, и когда действия относительно нее были связаны с ее изменением, результатом которого настали бы перечисленные вредные последствия, то руководствоваться необходимо исходя их диспозиции статьи УК. Признаки состава незаконного доступа к компьютерным данным в данном случае отсутствуют. Следующим аспектом, который позволит различить незаконный доступ к компьютерным данным от создания, реализации, распространения вредоносных программных обеспечений для ЭВМ, приходится содержание общественно опасного деяния.[14] Оно подразумевает наступления хотя бы одного из ниже перечисленных действий:

А. написание вредоносного программного обеспечения для ЭВМ;

Б. внесение модификаций в уже существующие программы для ЭВМ, подводя их под категорию вредоносных программ;

В. реализация вредоносных программ для ЭВМ;

Г. использование машинных носителей, которые содержат в себе вредоносные программы;

Д. распространение машинных носителей, которые содержат в себе вредоносные программы.

К тому же необходимо учесть тот факт, что согласно предписанным законам, состав преступления, по ч. 1 ст. 273 УК РФ, построен как формальный.

---

[14]Кириченко А.Н. Вирусы научились размножаться по своим законам / А.Н. Кириченко // МН Коллекция. -2003. -№2. - С.12

Таким образом, для признания правонарушения оконченным нет необходимости наступления вредных последствий в виде уничтожения, блокирования, изменения, копирования информационных данных, вмешательства в нормальную работу ЭВМ, системы, или их сети. Вполне достаточно установление самого факта совершения общественно опасного деяния, если оно обеспечивало реальную угрозу наступления перечисленных ранее вредных последствий. Аналогично, когда виновный намерено создает вредоносную программу для ЭВМ или модифицирует уже существующую программу, сводя ее до вредоносной, иначе реализует или распространяет подобные программы или физические носители с такими программами, и вдобавок не совершает действий, направленных на незаконный доступ к защищенном законом информационным данным, в таком случае подобные деяния классифицируются согласно ст. 273 УК РФ.

В целом на практике вероятна ситуация, при которой виновный преследуя цель создания вредоносного программного обеспечения для ЭВМ, незаконно прибегает к модификации существующей программы, которая в свою очередь является объектом авторского права, а соответственно, которая находится под защитой закона. К этому можно отнести внесение или удаление отдельных фрагментов кода, программы, переработка данных посредством их обновления и тому подобное. Иначе говоря, модифицирует компьютерные данные. В таком случае, подобные действия подпадают под ст. 272 и ст. 273 УК РФ. Для разъяснения, диспозиция ст. 273 УК гласит, что относительно создания программ для ЭВМ, модификация уже существующих программ, реализация или распространение подобных программ или физических носителей, не охватывает своим содержанием факт незаконного доступа к защищаемым законом компьютерным данным.

Из всего этого можно сделать вывод о том, что деяния виновного подпадают под дополнительную квалификацию по ст. 272 УК. Оконченный состав незаконного доступа к компьютерным данным стоит оценивать относительно поведения лица, которое незаконным образом воспользовалось

программой для ЭВМ или модифицировала ее, однако в силу обстоятельств, которые выходят за рамки сознания и воли виновного, закончить эту программу до состояния вредоносной. Однако если действия виновного были пресечены на более ранней стадии, например, при попытке незаконного доступа к данным, и не связывались с модификацией последних, в таком случае рассматривается подготовка к созданию, реализации и распространению вредоносного программного обеспечения для ЭВМ и покушение на незаконный доступ к компьютерным данным.

В русле изложенного стоит акцентировать внимание на том факте, что согласно ч. 2 ст. 30 УК, уголовная ответственность наступает за подготовку только лишь к тяжкому преступлению. Таким образом, различия незаконного доступа к компьютерным данным от создания, реализации, распространения вредоносного программного обеспечения для ЭВМ можно отыскать в юридической характеристике предмета преступного посягательства, сути общественно опасных действий, которые приводят к вредным последствиям, в субъективной стороне, дающей представление об отношении субъекта к содеянному.

1.4 Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети: состав преступления, проблемы привлечения к ответственности.

Интеграция компьютерных технологий сегодня все в большей мере оказывают влияние на жизнедеятельность человека, а элементарный выход из строя ЭВМ, их системы, или их сети может в перспективе привести к катастрофическим последствиям, исходя из этого аспекта законодатель счет требуемым установления уголовной ответственности за нарушение регламента эксплуатации ЭВМ, их системы или их сети. И конкретно ст. 274 УК РФ призвана установить такую ответственность, при условии, что подобные деяния должны причинить существенный вред. Целью действия ст. 274 является предупреждение невыполнения пользователями своих профессиональных

обязанностей, которые оказывают прямое влияние на сохранность хранимых и обрабатываемых данных. Приведенная уголовная норм, разумеется не содержит конкретизированных технических требований и ссылается к ведомственным инструкциям, регламентам, правилам, которые призваны определять порядок работы, и которые устанавливаются лицом, специально наделенным таким правом и доводятся до конечных пользователей. Использование этой статьи не представляется возможным для систем публичного доступа, в основе своей имеется ввиду мировая паутина; ее действие имеет отношение только на компьютеры и локальные сети предприятий.

Приведенная статья также придерживается линии, что под защищаемыми законом информационными данными подразумевается информация, для которой в специальных законах предусмотрен особый режим ее правовой защиты. К таким данным относятся государственная, служебная, коммерческая, банковская тайны, персональные данные и другие.

Согласной данной статьи необходимо установление причинной связи между фактом нарушения и наступившими существенными вредными последствиями, и в полной мере доказано, что эти самые последствия являются прямым результатом нарушений правил эксплуатации, а не программным сбоем, иначе действиями, согласованными в ст. 272, 273 УК РФ.

Непосредственным объектом правонарушения, согласно этой статьи являются отношения по соблюдению правил и регламентов эксплуатации ЭВМ, их системы, или их сети, иными словами аппаратно-техническая направленность. Под этими правилами подразумеваются:

1. Общероссийские санитарные нормы и правила для работников вычислительных центров;
2. Техническая документация на приобретаемые компьютеры;
3. Конкретные, принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка.

Несоблюдение перечисленных правил, халатность может произойти в результате как активных действий, так и бездействия.

Состав ч. 1 статьи сформулирован как материальный. Так общественно опасные последствия заключаются при соблюдении одновременно двух условий:

- уничтожение, блокирование, изменение компьютерных данных на ЭВМ, которые находятся под защитой закона;
- наличие факта нанесения существенного вреда этими действиями.

Требуется отметить, что так как разговор ведется о правилах, регламентах эксплуатации конкретно ЭВМ, иначе говоря программно-аппаратной части, то и соответствующее нарушение должно затрагивать только техническую сторону несоблюдения требований безопасности компьютерных данных, а никак не организационную или правовую.

Кажется, верным классификация к таковым следующего перечня: блокировка системы защиты от незаконного доступа, несоблюдение правила электро- и противопожарной безопасности, применение ЭВМ в условиях, не отвечающих тем, которые установлены документацией по ее применению, сюда можно включить температурно-влажностный режим, радиопомех, приведение в бездействие систем оповещения, длительное оставление без присмотра и тому подобное. Непременно все перечисленные действия должны рассматриваться не отдельно, а исключительно в связи с угрозой безопасности хранимым на ЭВМ данным, которые находятся под защитой закона.[15]

Правонарушение может быть классифицировано как преступление лишь в случае наступления существенного вреда.

Установка степени существенного вреда, согласно данной статьи определяется судебной практикой в каждом отдельном случае, руководствуясь обстоятельствами дела, но стоит отметить, что существенный вред не должен быть более значительным в сравнении с тяжкими последствиями.

---

[15]Курушин В.Д., Минаев В.А. Компьютерные преступления информационная безопасность / В.Д. Курушин, В.А. Минаев - М.: Новый юрист,1998. - С.58

Дефицит правоприменительной практики к сожалению, не предоставляет четкого разграничения природы последнего, однако же рациональнее под существенным вредом понимать в первую очередь тот вред, который наносится именно информационным данным в ее основной, существенной части. Примером может послужит уничтожение, блокирование, изменение ценных данных, касающихся важных объектов, или большого массива данных, трудно восстанавливаемых данных или не подлежащих воспроизводству и т.п.; ликвидация системы защиты, которая в перспективе нанесла ущерб информационным ресурсам; широкое распространение искаженных сведений и т.д.

Квалифицированный состав несоблюдения правил эксплуатации ЭВМ подразумевает наступления двух форм вины, ввиду того что конструкция приведенной статьи предполагает умысел в отношении деяния и неосторожность касательно наступивших последствий.

Первым неблагоприятным последствием приходится умышленное уничтожение, блокирование, изменение компьютерных данных, тем не менее правонарушение будет оконченным только при наступлении второго общественно опасного последствия – неосторожного причинения тяжкого вреда.

Непосредственно сами правила, регламенты эксплуатации ЭВМ, их системы, или их сети при совершении правонарушения, согласно ч. 2. ст. 274 УК РФ, виновным не соблюдаются умышленно. Виновное лица понимает общественную опасность нарушения правил, регламентов эксплуатации ЭВМ, их системы или их сети, предполагает вероятность или неизбежность наступления вредных последствий, которые могут проявиться в форме уничтожения, блокирования, изменения компьютерных данных, вмешательства в работу ЭВМ, их систему, или их сети, желает или сознательно допускает наступления подобных последствий, иначе имеет к ним безразличное отношение. Факультативные признаки как субъективной, так и объективной

стороны состава преступления могут быть учтены судом в качестве смягчающих, иначе отягчающих ответственность обстоятельств.

Объективная сторона приведенного правонарушения заключается в несоблюдении правил, регламентов эксплуатации ЭВМ и характеризуются следующим:

1. Общественно опасным деянием, в форме действия или бездействия, заключающееся в несоблюдении правил, регламентов эксплуатации ЭВМ, их системы, или их сети.
2. Наступление общественно опасных последствий, которые представляют собой уничтожение, блокирование, изменение компьютерных данных, которые причинили существенный вред, иначе повлекли по неосторожности тяжкие последствия.
3. Наличие причинной связи между действием и наступившими соответственно последствиями.

При раскрытии объективной стороны такого вида общественно опасных посягательств законодатель прибегает к бланкетному способу: указывается в диспозиции статьи, что действие, иначе бездействие носит общий характер, т.е. несоблюдение правил. Суть содержания таких правил отражено в нормативных актах других отраслей права. Правила, регламенты эксплуатации заключены в общих требованиях по технике безопасности и эксплуатации ЭВМ и периферийных устройств, в специальных правила, инструкциях, предписывающих отдельные условия применения ЭВМ, это для примера определенной алгоритм действия, условия эксплуатации.

Субъективная сторона согласно ч. 1 приведенной статьи описывает наличие умысла, который своей целью ставит несоблюдение правил, регламентов использования ЭВМ. В результате наступления тяжких последствий ответственность наступает лишь в случае неосторожных действий, предусмотренных ч. 2 ст. 274.

Умышленное несоблюдение правил, регламентов применения ЭВМ, их системы, или их сети предусматривает уголовную ответственность согласно

последующим последствиям, также несоблюдение правил эксплуатации в таком случае принимает характер способа совершения правонарушения.

Для примера можно привести следующую ситуацию: работник технического отдела медицинского учреждения произвел установку программу, полученную посредством сети, однако не произвел предварительную проверку ее, речь заходит о преступной неосторожности, на наличие в ней компьютерного вируса, в результате чего начались сбои в работе ЭВМ, что в конечном итоге привело к отказу работы жизнеобеспечения реанимационного отделения и к смерти больного. Подобное подпадает под ч. 2 ст. 274.[16] Такие действия характеризуйся они как умышленные действия квалифицируются как покушение на убийство.

Субъектом данного правонарушения – специальный, лицо исполняющее должностные обязанности, имело право на доступ к ЭВМ, их системе, и их сети должно действовать в рамках установленных порядков, правил и регламентов использования.

Санкции согласно ч. 1 ст. 274 состоят их трех различных видов наказаний, а именно: лишение права занимать определенную должность или заниматься такой деятельностью на срок до пяти лет, обязательные работы от ста восьмидесяти до двухсот сорока часов, и наконец ограничение свободы до двух лет.

Часть 2 – состав с двумя формами вины, согласно которой в качестве квалифицирующего признака выступает наступление по неосторожности тяжких последствий. Содержание последней аналогично таковому для ч. 2 ст. 273. Санкция нормы различается от предыдущей только лишением свободы на срок до 4 лет.

По данным которыми располагают правоохранительные органы, имеют место быть сведения о фактах несанкционированного доступа к ЭВМ вычислительного центра железных дорог России, а также к электронным

---

[16]Кузнецов А. П. Ответственность за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (ст. 274 УК РФ) / А. П. Кузнецов // Правовые вопросы связи. -- 2007. -- № 2.

данным систем учета жилых и нежилых помещений местных органов управления во многих городах, что на сегодняшний день подпадает под ответственность согласно ст. 272 УК РФ, иначе ст. 274 УК в зависимости от действий лица, который совершил посягательство и нарушение правил эксплуатации конкретной сети. Требуется различать правонарушение, предусмотренное ст. 274 УК РФ от незаконного доступа к компьютерным данным. Приведенная статья разграничивает ответственность за несоблюдение правил, регламентов использования ЭВМ, их системы или их сети лицом, которое имеет доступ к ЭВМ, их системы или их сети, в результате которого произошло уничтожение, блокирование, изменение данных ЭВМ, находящихся под защитой закона, при соблюдении условия что данные деяния причинили существенный вред, это ч.1 ст. 274 УК, иначе повлекло по неосторожности тяжкие последствия, что является ч. 2 ст. 274 УК. Отличительные стороны между этими правонарушениями состоят в следующем:

А. при незаконном доступе к компьютерным данным, виновный не имел права обращаться к информации, ознакомиться с ней, и каким-либо образом распоряжаться, иначе действовал не санкционированно.

Состав несоблюдения правил, регламентов эксплуатации ЭВМ, их системы, или их сети, напротив, подразумевает, что виновный, согласно занимаемого служебного положения, или выполнения функциональных обязанностей, обращается к данным правомерно, иными словами действуем в этом плане на законных основаниях.

Таким образом, в отличии, субъект преступного посягательства, предусмотренногост.274 УК РФ - законный пользователь информации;

Б. неправомерный доступ к компьютерной информации – преступление, совершаемое только путем активных действий, тогда как нарушение правил эксплуатации ЭВМ или их сети может быть совершенно и бездействием (например, виновный не включает систему защиты информации от несанкционированного доступа к ней, оставляет без присмотра свое рабочее место и т.д.);

В. необходимым признаком объективной стороны анализируемых преступлений выступают общественно опасные последствия, которые, однако, по своему содержанию и объему неравнозначны.

Ответственность по ст. 274 УК РФ наступает только в том случае, если уничтожение, блокирование или модификация охраняемой законом информации ЭВМ причинило существенный вред потерпевшему. Для привлечения к ответственности по ст. 272 УК РФ причинение существенного вреда не требуется. Достаточно установить сам факт уничтожения, блокирования, модификации или копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Кроме того, закон не предусматривает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, если это деяние повлекло копирование информации, даже причинившее существенный вред. Указанное положение свидетельствует о неравнозначном подходе законодателя к объему преступных последствий, выступающих в качестве обязательных признаков для составов преступлений, предусмотренных ст. ст. 272 и 274 УКРФ.

Как указывалось, выше, в уголовном кодексе предусмотрена также довольно большая группа преступлений, совершение которых может быть связано не только с воздействием на компьютерную информацию, но и повлечь вредные последствия на компьютерную информацию, но и повлечь вредные последствия в виде уничтожения, блокирования, модификации либо копирования информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

2. КРИМИНОЛОГИЧЕСКИЙ АСПЕКТ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

2.1 Криминологическая характеристика личности преступника

Собранные в процессе исследования сведения о личности преступления, о его криминальном поведении и виновности создают фактическую базу для принятия обоснованных решений по его уголовному преследованию.[17]

Заслуживает внимания классификация лиц, склонных к совершению преступления в сфере компьютерной информации, предложенная А.В.Кузнецовым.[18] К первой группе относятся лица, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами фанатизма, и изобретательности. Вторая включает лиц, страдающих новым видом психических заболеваний – информационными и компьютерными фобиями, и третью группу составляют профессиональные компьютерные преступники с ярко выраженными корыстными целями. Именно эта группа представляет собой основную угрозу для общества, являясь кадровым ядром компьютерной преступности. Особую категорию преступников составляют хакеры.Их определяют, как особую категорию специалистов в сфере вычислительной техники, осуществляющих негативные действия в области систем компьютерной связи и информационных технологий с целью получения доступа к защищенной компьютерной информации. На основе имеющихся публикаций и результатов анализа следственной практики можно предложить следующую классификацию лиц, совершающих преступления в сфере компьютерной информации, в зависимости от их специализации:

1. Кракеры – лица, деятельность которых направлена на "взлом" различного программного обеспечения. Их целями обычно являются: устранение

---

[17]Козлов В.Е.Теория и практика борьбы с компьютерной преступностью /В.Е. Козлов. - М.: Горячая линия, Телеком. - 2002. - С.161

[18]Кузнецов А.В. Некоторые вопросы расследования преступлений в сфере компьютерной информации//Информационный бюллетень следственного комитета МВД РФ;

защиты от несанкционированного копирования, бесплатная регистрация программных продуктов, устранение каких-либо ограничений или расширение возможностей программ.

2. Фрикеры – специализируются на неправомерном использовании коммуникационных услуг и средств связи. Их деятельность направлена на безвозмездное использование услуг междугородной телефонной связи (включая телефонные переговоры через сеть Интернет), услуг мобильной связи.
3. Кардеры (от англ. card-карта). Направленность их деятельности предполагает наличие глубоких знаний в области программирования микросхем и микропроцессов. Их целью становится неправомерная модификация информации на электронных банковских, телевизионных и других картах.
4. Хакеры (сетевые хакеры). Предметом посягательств являются различные сетевые ресурсы: серверы электронной почты, серверы, предоставляющие услуги по размещению веб-страниц, информационные ресурсы крупных компаний и т.п.

Важную роль в формировании антисоциальной направленности в сознании играют условия внутреннего (субъективного) характера. В отличие от внешних условий. Они охватывают явления. Связанные с особенностями личности правонарушителя.[19]К ним на наш взгляд относятся: недостаточный уровень правовой культуры; ослабленность волевых качеств личности; импульсивность, которая проявляется в сниженном контроле своего поведения; отсутствие правильных целей в жизни и умения их добиваться; неуверенность в себе, выражающаяся в предпочтительном выборе виртуального общения и т.п.

Особенности характера и темперамента лица, совершившего преступление в сфере компьютерной информации, необходимо принимать во внимание для выявления таких качеств личности, которые могут

---

[19]Антонян Ю.М., Еникеев М.И.Психология преступника и расследования преступлений / Ю.М. Антонян, М.И. Еникеев. - М.: Юрист,1996.- С.28

способствовать совершению данного преступления, это также может конкретизировать меры предупредительно-воспитательного воздействия на данное лицо с учетом его личностных особенностей.

Под способом совершения преступления понимается система объединенных единым замыслом действий преступника (и связанных с ним лиц) по подготовке, совершению и сокрытию преступления, детерминированных объективными и субъективными факторами и сопряженных и использование соответствующих орудий и средств.

На сегодняшний день существует несколько классификаций способов совершения преступлений в сфере компьютерной информации. Одна из классификации предложена А. Н. Родионовым и А. В. Кузнецовым. Согласно ей, способы совершения компьютерных преступлений можно подразделить на:

1. изъятие средств компьютерной техники;
2. неправомерный доступ к компьютерной информации преступления, совершенные в отношении компьютерной информации, находящееся в глобальных компьютерных сетях; преступления, совершенные в отношении компьютерной информации, находящееся в ЭВМ, не являющихся компьютером в классическом понимании этого слова (пейджер, сотовый телефон, кассовый аппарат, и т.п.);
3. изготовление или распространение вредоносных программ (вирусы, программы – взломщики и т.п.);
4. перехват информации.

На наш взгляд, способы совершения неправомерного доступа компьютерной информации можно объединить в три основные группы.

Первая группа- это способы непосредственного доступа. При их реализации информация уничтожается, блокируется, модифицируется, копируется, а также может нарушаться работа ЭВМ, системы ЭВМ или их сети путем отдачи соответствующих команд с компьютера, на котором информация находится. Непосредственный доступ может осуществляться как лицами, работающими с информацией (имеющими отношение к этой работе), так и

лицами, специально проникающими в закрытые зоны и помещения, где производится обработка информации.

Другой способ непосредственного доступа к компьютерной информации заключается в неправомерном использовании преступником технических отходов информационного процесса, оставленных пользователем после работы с компьютерной техникой. Он осуществляется в двух формах: физической и электронной.

Физический поиск отходов сводится к обследованию рабочих мест программистов, содержимого мусорных баков, емкостей для технологических отходов для сбора оставленных или выброшенных физических носителей информации, а также обследованию различной документации, оставленной на рабочем месте ежедневников.

Вторая группа способов совершения рассматриваемого преступления включает способы опосредованного (удаленного доступа к компьютерной информации). При этом неправомерный доступ к определенному компьютеру и находящееся на нем информации осуществляется с другого компьютера, находящегося на определенном расстояние через компьютерные сети. Способы опосредованного доступа к компьютерной информации, в свою очередь, можно разделить на две подгруппы: способы преодоления парольной, а также иной программой или технической защиты и последующего подключения к чужой системе; способы перехвата информации.

К способам первой подгруппы относятся:

1. Подключение к линии связи законного пользователя (например, к телефонной линии) и получение тем самым доступа к его системе. Подключившись, преступник дожидается сигнала, означающего окончание работы, перехватывает его на "себя", а потом, когда законный пользователь закончил сеанс работы, осуществляет доступ к его системе. Данный способ сравним с работой двух параллельных телефонных аппаратов, подключенных к одному абонентскому номеру: если один

телефон находиться в активном режиме (ведется разговор по первому закончен и трубка положена, он может быть продолжен по второму.

2. Проникновение в чужие информационные сети путем автоматического перебора абонентских номеров с последующим соединением с тем или иным компьютером (перебор осуществляется до тех пор, пока на другом конце линии не "отзовется чужой" компьютер). Поскольку в подобном случае один несанкционированный пользователь может быть легко обнаружен, подобный "электронный взлом" осуществляется в одновременно с несколькими рабочих мест: в заданное время несколько (более десяти)персональных компьютеров одновременно предпринимают попытку несанкционированного доступа.
3. Проникновение в компьютерную систему и использованием чужих паролей, выдавая себя за законного пользователя. При подобном способе незаконный пользователь осуществляет подбор пароля для доступа к чужому компьютеру. Подбор паролей может осуществляться двумя методами. Первый: подбор паролей путем простого перебора всех возможных сочетаний символов до тех пор, пока не будет установлена нужный код, что позволило преступнику получить исчерпывающий список личных кодов пользователь.

Ко второй подгруппе способов опосредованного (удаленного) доступа к компьютерной информации относятся способы ее непосредственного, электромагнитного и других видов перехвата.

Непосредственный перехват осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного "подслушивания" являются кабельные и проводные системы, наземные микроволновые системы, системы правительственной связи.

Электромагнитный перехват. Современные технические средства позволяют получить информацию без непосредственного подключения к

компьютерной системе: за счет перехвата излучений центрального процессора, дисплея, коммуникационных каналов, принтера ит.д. Все это можно осуществить, находясь на достаточном удалении от объекта перехвата. Например, используя специальную аппаратуру, можно "снимать" информацию с компьютера, расположенного в соседнем помещении, здании. Таким образом, при несанкционированном доступе в Интернет происходит обращение к "списку" имен и паролей на компьютере провайдера, который является коммерческой тайной. Что касается наступления общественно опасных последствий, их может быть несколько. В самом общем случае – это нарушение работы сети ЭВМ, под которым надо понимать следующие:

1. Выдачу искаженных информации, поскольку во всех протоколах фигурирует имя зарегистрированного пользователя.
2. Сбои в работе оборудования, поскольку оборудование провайдерской фирмы рассчитано на определенное количество пользователей и, разумеется, не учитывает нелегально подключившихся. Повышенная загрузка оборудования приводит к ошибкам при передачи данных и, как следствие, необоснованным задержкам при работе.

При этом обязательным условием является сохранение физической целостности ЭВМ, системы ЭВМ или их сети. Если наряду с названными нарушениями работы оборудования нарушается и физическая целостность компьютерной ЭВМ, системы ЭВМ или их сети. Если наряду с названными нарушениями работы оборудования нарушается и физическая целостность компьютерной системы как физической вещи, содеянное требует дополнительной квалификации по статьям о преступлениях против собственности. Помимо нарушения работы, в случае монопольного режима доступа(либо статического IP адреса), происходит блокирование информации, т.е.другой пользователь под этим же именем (адресом) лишается возможности входа. При этом нарушение работы по п.2 не будет, так как количество пользователь не меняется. Причинение материального ущерба наносимого в результате списания денежных средств со счетов зарегистрированных

пользователей должно быть квалифицирована как причинение имущественного ущерба путем обмана или злоупотребления доверием при отсутствии признаков хищения т.е. по ч.1 ст. 165; либо в случае неоднократности по ч.1, либо в случае крупного ущерба по ч.3. Однако неоднократность в данном случае следует разграничивать с длящимися преступлением. Так, неоднократным целесообразно считать вход различными сетевыми реквизитами, а длящимся – разделенный по времени вход под одним и тем же именем, и паролем.

2.2 Факторы, способствующие совершению преступлений в сфере компьютерной информации

За последнее годы предлагаются различные пути решения вопросов связанных с выявлением факторов совершения преступлений в сфере компьютерной информации и условий, способствующих его совершению. Однако указанные решения на наш взгляд, не являются исчерпывающими и нуждаются в дальнейшей разработке. К числу нерешенных относятся, в частности вопросы о составе совокупности явлений, подлежащих установлению в качестве причин и условий по каждому уголовному делу, а также о роли и значении для наступления события преступления отдельных обстоятельств, входящих в эту совокупность.

По мнению Г.Г. Зуйкова, совокупность причин и условий, вызывающих совершение какого-либо преступления, можно определить следующим образом.[20]

- непосредственная причина совершения преступления.
- условия, способствующие действию непосредственной причины и конкретному преступному посягательству.
- обстоятельства, сформировавшие непосредственную причину и являющиеся таким образом причинами непосредственной причины,

[20]Зуйков Г.Г. К вопросу о понятии причин преступления и условий, способствующих его совершению//Вопросы предупреждения преступности, вып.2 «Юрид.лит-ра»,1995г.-С.15

условия, способствующие действию факторов формирующих непосредственную причину и т.д.

Необходимо отметить, что в связи с многообразием факторов, объективно и субъективно влияющих на совершение преступлений в сфере компьютерной информации не всегда удается открыть их фактическое взаимодействие и установить какие из них привели непосредственно к совершению преступления, а какие служили более или менее отдаленными причинами этого явления.[21]

Непосредственной причиной совершения рассматриваемых деяний, как правило, выступает антисоциальная направленность, выразившаяся в формировании и сознательной реализации преступного умысла, так как с субъективной стороны преступления в сфере компьютерной информации могут быть совершены только умышленно.

Обстоятельства, формирующие антисоциальную направленность, то есть непосредственную причину, по мнению Ушакова С.И. можно разделить на объективные и субъективные.[22]

К числу объективных условий относятся такие как:

1. непродуманная кадровая политика в вопросах приема на работу сотрудников и их увольнения. Мировой опыт развития компьютерной техники свидетельствует, что специалисты высокой квалификации, неудовлетворенные условиями или оплатой труда, нередко уходят из компании для того, чтобы начать собственный бизнес. При этом, они "прихватывают" с собой различную информацию, являющуюся собственностью владельцев фирмы, включая технологию, список потребителей и т.д. Иными словами, всё, что имело какую-либо интеллектуальную ценность, покидало ворота предприятия в дипломатах, нанося при этом многомиллионные убытки;

---

[21]Козлов В.Е.Теория и практика борьбы с компьютерной преступностью /В.Е. Козлов. - М.: Горячая линия, Телеком. - 2002. - С.161

[22]Ушаков С.И. Преступления в сфере обращения компьютерной информации (теория, законодательство, практика) - Ростов-на-Дону,2001г.- С.169

2. нарушение должностными лицами организаторских хозяйственных и социальных функций, выразившихся в возникновении у сотрудников материальной незаинтересованности осуществления своих обязанностей, необоснованном ограничении трудовых прав и возможностей использования льгот и социальных гарантий, препятствовании учебе, повышению квалификации, осуществлении права на отдых и т.п.;
3. недостаточно серьезное отношение руководителей к вопросам обеспечения информационной безопасности и защиты информации. Нередко в крупных организациях, обрабатывающих значительный объем компьютерной информации, отсутствует не только служба или отдел информационной компьютерной безопасности. Но и отдельное лицо, в обязанности которого входило бы ее обеспечение. Это может спровоцировать совершение рассматриваемого преступления.

К внешним условиям можно отнести следующие:

1. недостаточная защита используемого программного обеспечения от несанкционированного доступа. Например, операционные системы MicroSoftотличается несовершенным алгоритмом шифрования сохраняемых паролей (в сети Интернет распространены программы расшифровки " PWL" файлов, содержащих пороли). Подобные программы были использованы в ходе совершения неправомерного доступа к компьютерной информации в 14, 7% изученных уголовных дел. В 8,8 % случаев при осуществлении такого доступа использовались программы, предназначенные для тестирования надежности сетевых программных и аппаратных средств защиты информации;
2. уязвимость защиты электронной почты (на пути к адресату сообщение проходит через многочисленные компьютеры. Причем часто новым маршрутом, к тому же при пересылке почты остается большое число копий, сильно снижающих уровень защиты). Электронное сообщение само по себе может нести существенную опасность, из-за возможности прикрепления к электронным письмам активных компонентов, среди

которых может оказаться и вредоносная программа так, при совершении 5,9 % изученных преступлений использовались вредоносных программы, типа "троянский конь", которые посылались будущей " жертве" прикрепленными к обычному электронному письму;

3. недостаточная надежность технических средств защиты компьютерной техники. Существующие сегодня методы эмуляции и перехвата позволяют обойти большинство аппаратных средств защиты, например, электронных "HASP" ключей, подключаемых к портам компьютера, через которые происходит соединение с периферийным оборудованием;
4. отсутствие контрольных проверок программным оборудованием соответствия и правильности вводимой информации.

К внутриорганизационным условиям можно отнести:

1. отсутствие должного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации и ее безопасности в части защиты средств компьютерной техники от несанкционированного доступа. Зарубежный опыт свидетельствует о том, что создание соответствующих подразделений или должностей в значительной степени снижает риск несанкционированного доступа к охраняемой компьютерной информации.;
2. неконтролируемый доступ сотрудников к элементам управления средств компьютерной технике (устройствам ввода информации), используемых как автономно, так и в качестве элементов автоматизированной сети;
3. несовершенство парольной системе защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;
4. неприменение категорийности допуска сотрудников к документации строгой финансовой отчетности, в том числе находящейся в электронном виде;

5. отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной компьютерной информации;
6. легкомыслие и небрежность собственников и пользователь компьютерной информации;
7. нарушение установленных сроков хранения копий программ и компьютерной информации, а иногда и полное их отсутствие.

Определяющее значение имеет деятельность государства в лице уполномоченных органов по разработке и регламентации общегосударственных вопросов защиты Российского информационного пространства, выявлению и устранению обстоятельств, способствующих посягательствам на компьютерную информацию. При этом необходимо учитывать влияние как внешних, так и внутренних факторов, способствующих количественному росту рассматриваемых преступлений.

Внешние общегосударственные факторы, на наш взгляд, следующие:

1. ускоренная интеграция Российской Федерации в международное информационное пространство. Объединение с локальными и глобальными сетями граничащих с Россией информационно развитых стран. Непрерывное увеличение количества и пропускной способности каналов связи с глобальной сетью Интернет;
2. рост числа ЭВМ, используемых в России, увеличение числа пользователей, объемов информации, хранимой и передаваемой ЭВМ;
3. возможность выхода российского пользователя в мировые информационные сети для обмена информацией. Заключения контрактов, осуществления платежей и покупок.

Подобный обмен в настоящее время производится абонентами самостоятельно, без контроля со стороны государственных органов, минуя государственные границы.

К внутренним общегосударственным факторам относятся:

1. недостаточный уровень специальной подготовки должностных лиц правоохранительных органов, в обязанности которых входит предупреждение, раскрытие и расследование компьютерных преступлений;
2. отсутствие скоординированности в работе государственных и общественных структур в сфере обеспечения информационной безопасности. Помимо правоохранительных органов (МВД, ФСБ и прокуратуры), вопросами информационной безопасности занимаются Комитет по политике информатизации при Президенте РФ, Палата по информационным спорам при Президенте РФ, Государственная техническая комиссия при Президенте РФ, Министерство связи РФ, Международная Академия информатизации;
3. ограничения на импорт в Россию защищенных от электронного шпионажа компьютеров и сетевого оборудования;
4. использование в преступной деятельности современных технических средств, в том числе ЭВМ. Во-первых, организованная преступность включена в крупномасштабный бизнес, выходящий за рамки отдельных государств, где без компьютеров невозможно руководить и организовать сферу незаконной деятельности. Во- вторых, из организаций, использующих ЭВМ, удобнее "вытягивать" деньги с помощью такой же техники, дающей возможность повысить прибыль и сократить риск.

Деятельность по выявлению и устранению обстоятельств, способствующих совершению неправомерного доступа к компьютерной информации, в конечном счете, направлена на создание таких условий, при которых совершение данного преступления будет максимально затруднено или невозможно, но, если оно совершено, первостепенное значение приобретает выявление всех эпизодов преступления.

2.3 Меры по предупреждению преступлений в сфере компьютерной информации.

К организационным мерам предупреждения преступлений в сфере компьютерной информации можно отнести следующую совокупность мероприятий.

- совершенствование научно-технических средств, тактических приемов и методов расследования неправомерного доступа к компьютерной информации;
- своевременное явление и пресечение как начавшихся преступлений, так и неправомерного доступа к компьютерной информации на стадии покушения или подготовки к нему;
- установление обстоятельств, способствовавших совершению каждого преступления, разработка и совершенствование методов и приемов выявления таких образов;
- создание подразделений в МВД, ФСБ и прокуратуре, специализирующихся на расследовании высокотехнологичных преступлений, в частности неправомерного доступа к компьютерной информации, а также экспертно – криминалистических подразделений, способных отвечать на все вопросы компьютерно-технических и компьютерно-информационных экспертиз;
- своевременная регистрация и надлежащий учет этих преступлений;
- переподготовка и повышение квалификации работников правоохранительных органов, расследующих неправомерный доступ к компьютерной информации;
- информационное обеспечение деятельности органов внутренних дел;
- разработка и внедрение политики безопасности компьютерной информации, включающий подбор, проверку и инструктаж персонала, участвующего во всех стадиях информационного процесса.

В настоящее время основными задачами отделов по борьбе с преступлениями в сфере высоких технологий (ОБПСВТ) являются:

1. Выявление преступлений в сфере компьютерной информации когда объектом преступного посягательства является ЭВМ, их системы м сети права собственника информации, в сфере телекоммуникаций ЭВМ их системы и сети являются орудием совершения преступления, а также посягательств на конституционные права граждан - неприкосновенность личной жизни, тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, совершенных путем неправомерного прослушивания сообщений и снятия информации с технических каналов связи.
2. Возбуждение уголовных дел и производство неотложных следственных действий, при необходимости пресечение указанных преступлений.
3. Выявление лиц, групп и сообществ, занимающихся противоправной деятельностью в данной области, документирование их преступной деятельности, проведение мероприятий по предупреждению таких преступлений.
4. Выполнение поручений следователей по расследованию указанных преступлений, производство оперативно - розыскных мероприятий, а также участие в расследовании в составе следственно - оперативных групп.

Аналогичные подразделения созданы и в других российских правоохранительных органах - Генеральной прокуратуре и Федеральной службе безопасности.

1. Аналитическую разведку совершенствование информационного - аналитического обеспечения деятельности подразделении криминальной полиции, изучение перспективных средств и методов поиска и сопоставительного анализа самой разнообразной, имеющей значение для борьбы с данным компьютерным преступлением информации от материалов средств массовой информации в электронных библиотеках

сети Интернет до конкретных оперативных данных. Целью такого анализа является формирование новых знаний о способах совершения неправомерного доступа к компьютерной информации, способах его сокрытия, выявления фактов несанкционированного доступа о которых не поступило заявлений в правоохранительные органы и т.п.

2. Компьютерную разведку - применение средств и методов организации гласного и негласного получения информации, хранимой и обрабатываемой компьютерными системами для получения сведений о готовящихся преступлениях. Деятельность по скрытому получению компьютерной информации может предусматривать как непосредственный доступ к интересующим информационным ресурсам, так и перехват электронных сообщений, передаваемых по компьютерным проводам и радиосетям.
3. Обеспечение информационной безопасности органов внутренних дел которое распространяется от защиты субъектов и интересов органов внутренних дел от недоброкачественной информации до защиты ведомственной информации ограниченного доступа, информационных технологий и средств их обеспечения. Информационная безопасность ОВД определяется надежностью систем ее обеспечения включая надежность аппаратных средств и программного обеспечения.

Международное сотрудничество при расследовании рассматриваемого преступления осуществляется в формах:

а. обмена информацией, в том числе:
   - о готовящемся или совершенном неправомерном доступе к компьютерной информации и причастных к нему физических и юридических лицах.
   - о формах и методах предупреждения, выявления, пресечения, раскрытия и расследования данного преступления.
   - о способах его совершения

- о национальном законодательстве и международных договорах, регулирующих вопросы предупреждения выявления пресечения, раскрытия и расследования как рассматриваемого преступления, так и других преступлений в сфере компьютерной информации.

б. исполнения запросов о провидении оперативно - розыскных мероприятий, а также процессуальных действий, в соответствии с международными договорами о правовой помощи.

в. планирования и проведения скоординированных мероприятий и операций по предупреждению, выявлению, пресечению, раскрытию и расследованию неправомерного доступа к компьютерной информации.

г. оказания содействия ив подготовке и повышении квалификации кадров, в том числе путем стажировки специалистов, организации конференций, семинаров, и учебных курсов.

д. создания информационных систем, обеспечивающих выполнение задач по предупреждению, выявлению, пресечению, раскрытию и расследованию данного преступления.

е. проведения совместных научных исследований по представляющим взаимный интерес проблемам борьбы с рассматриваемым преступлениями, а с другой стороны- увеличить объем информации, проходящей через государственные СМИ, направленной на повышение уровня правовой, информационной и компьютерной культуры общества.

Организационные мероприятия по предупреждению неправомерного доступа к компьютерной информации рассматриваются многими специалистами, занимающимися вопросами безопасности компьютерных систем как наиболее важные и эффективные. Это связано с тем что они являются фундаментом, на котором строится вся система защиты компьютерной информации от неправомерного доступа.

Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно- технических средств защиты информационных систем, обрабатывающих информацию с ограниченным

доступом в негосударственных структурах, осуществляются органами государственной власти. Правительство Российской Федерации определяет порядок осуществления такого контроля. В организациях обрабатывающих государственную информацию с ограниченным доступом создается специальные службы, обеспечивающие защиту такой информации.

Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации, в случае невыполнения этих требований. Он также вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах. Соответствующие органы определяет Правительство Российской Федерации. Эти органы соблюдают условия конфиденциальности самой информации и результатов проверки. Субъектами, осуществляющими профилактику неправомерного доступа к компьютерной информации являются правоохранительные органы, поскольку профилактическая деятельность составляет обязательную составную часть правоохранительной деятельности: органы межведомственного контроля, отраслевые органы управления, международные органы и общественные организации, а так же непосредственные руководители предприятий и организаций в которых обращается конфиденциальная компьютерная информация ответственные сотрудники по информационной безопасности. 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 исследуемого преступления.

2.4 Международное сотрудничество в борьбе с преступлениями в сфере компьютерной информации.

Исходя из изложенного, можно сделать выводы о том, что сложность компьютерной техники, неоднозначность квалификации, а также трудность сбора доказательственной информации не приведет в ближайшее время к появлению большого числа уголовных дел, возбужденных по статьям 272-274 УК. Кроме этого, нас ждет появление таких специфических форм компьютерных правонарушений, к которым не применимы составы преступлений, предусмотренные вышеуказанными статьями. Но все же попытка реализации уголовно-правовой политики России в новой для нее области - сфере компьютерных правоотношений, поможет снять накопившиеся здесь противоречия, защитить права заинтересованных лиц. Ее успех будет зависеть от многих факторов политического, экономического, научно-технического, организационного характера. Немаловажное значение будет играть понимание правоведами транснационального характера компьютерной преступности и, как следствие, установление международных контактов с правоохранительными структурами. Такими же значимыми факторами будут и контакты с частными охранными структурами и структурами информационной безопасности в кредитно-денежной сфере. Сегодняшние реалии заставляют двигаться в этих направлениях. По данным правоохранительных органов криминальное поле кредитно-банковской системы активно заполняется преступлениями, связанными с использованием электронных средств доступа к информации (компьютерные, телекоммуникационные системы, кредитные карточки и др.). Для правоохранительных органов эта проблема наиболее остро встает в связи с переходом абсолютного числа банковских и финансовых структур на расчеты с использованием компьютерных сетей.

Например, только по данным ГИЦ МВД России, в 2007-2009 гг. выявлено 26821 преступление преступлений с использованием электронных средств доступа. По данным Федеральной службы реагирования на ЧП в компьютерном пространстве, только в 2008г. было зарегистрировано 9010 преступлений, из

них раскрыто-8419, на 24% больше, чем в предыдущем году. За 2009г. раскрыто-9991 из 10575 (на 43,6% больше, чем в 2008г.) В первом квартале 2010г. преступлений в данной сфере было зарегистрировано 11918 (из них 1230 – в январе, 3634 – в феврале, 2541 – в марте и 4513 – в апреле), среди которых раскрыто 10488 (более 88 %). Обнаружить удается менее 15% всех преступлений этого рода и лишь 10% из них предаются огласке. Понятно, что без тщательно отработанных методик расследования, помогающих людям обрести чувство защищенности, под сомнением оказывается - ни больше ни меньше - стабильность сегодняшних военных и коммерческих предприятий, не говоря уже об электронной торговле на базе Internet. Результаты статистического анализа убытков и типов преступлений не могут считаться достаточно корректными, поскольку, во-первых, не все группы жертв смогли предоставить достоверные сведения о своих финансовых потерях, а во-вторых, чисто денежными потерями ущерб в данном случае далеко не ограничивается.

Подобная картина требует кардинальных решений на международном уровне. И первые попытки уже сделаны. Надо отметить, что российские правоохранительные органы в достаточной степени осознали угрозу, которую таит в себе информатизация общества и государства. В меру возможностей, отпущенных финансированием ведомства, пытаются делать упреждающие шаги. Создавать компьютерную сеть МВД у нас начали еще в 1991году, понимая, что с бумажными картотеками много преступников не наловишь. Программное обеспечение для управления базами данных, в которых МВД хранит миллионы записей, приобретено у не менее знаменитой американской фирмы Oracle. Создание милицейской компьютерной сети, которая в конце концов должна раскинуться от Калининграда до Южно-Сахалинска, - сегодня один из глобальных российских информационных проектов, который выполняется четко и в положенные сроки. Остается пожелать, чтобы подобная сеть сама не стала объектом посягательств преступников.

Заключение

В ходе проведенного исследования:

- выявлены недостатки законодательной техники при конструировании ст. 272 УК РФ, сформулированы и обоснованы рекомендации по решению ряда задач прикладного характера;
- дана общая характеристика составов преступлений в сфере компьютерной информации и проблемы их квалификации;
- рассмотрен состав преступления по ст. 272 "Неправомерный доступ к компьютерной информации" и проблемы квалификации данного преступления;
- исследованы проблемы квалификации преступления по ст.273 "Создание, использование и распространение вредоносных программ для ЭВМ";
- проанализированы проблемы привлечения к уголовной ответственности по ст.274 УК РФ "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети
- дана криминологическая характеристика особенностям преступлений в сфере компьютерной информации;
- установлены основные особенности личности компьютерных преступников, совершающих неправомерный доступ к компьютерной информации;
- указаны основные факторы, способствующие совершению преступлений;
- рассмотрены меры по предупреждению преступлений в сфере компьютерной информации и обобщен опыт международного сотрудничества в борьбе против преступлений данного вида.

Новизна работы определяется также теми результатами исследования:

1. Компьютерная сфера является основой для возникновения нового вида общественных отношений - компьютерных, которые, в свою очередь, стали одним из объектов уголовно-правовой охраны.

2. Применение компьютерных технологий для обработки информации повлекло появление новых преступлений — преступлений в сфере компьютерной информации.
3. Проанализировав терминологический аппарат, использованный законодателем при конструировании состава ст. 272 УК РФ, установлено следующее:

– в существующем понятийном аппарате гл. 28 УК РФ отсутствует качественная определенность, что несовместимо с требованиями законодательной техники;
– основным из недостатков в использовании названных признаков является то, что все они не имеют количественного выражения и не могут характеризоваться различной интенсивностью проявления;
– при конструировании уголовно-правовых норм законодателю необходимо отказаться от введения в уголовное законодательство узкопрофессиональных технических терминов без их легального толкования, а те из них, без которых невозможно обойтись в настоящее время, должны получить легальное толкование в базовом российском информационном законодательстве.

4. В рамках общей профилактики государство должно создавать и финансировать специальные научно-исследовательские центры в целях изучения и предупреждения неправомерного доступа к компьютерной информации и других преступлений в сфере компьютерной информации.
5. Содержащиеся в исследовании теоретические положения и выводы, направленные на развитие и совершенствование общей теории правового регулирования отношений в сфере компьютерной информации, могут использоваться для дальнейших исследований, связанных с проблемой уголовной ответственности за преступления в сфере компьютерной информации. В соответствии с поставленными целями и задачами все выводы и положения, составляющие теоретическую часть работы, подчинены идее использования их в практической деятельности. На

основе расчетов реальных данных, выполненных в ряде организаций и внедренных в их практику, показано, что проведение профилактических мероприятий существенно снижает риск неправомерного доступа к компьютерной информации.

Итак, попытка реализации уголовно-правовой политики в новой для нее области - сфере компьютерных правоотношений, сможет окажется успешной, если поможет снять накопившиеся здесь противоречия, защитить права заинтересованных лиц - будет зависеть от многих факторов политического, экономического, научно-технического, организационного характера.

Так же хотелось бы подчеркнуть, что абсолютную надёжность и безопасность в компьютерных сетях не смогут гарантировать никакие аппаратные, программные и любые другие решения. В то же время свести риск потерь возможно лишь при комплексном подходе к вопросам безопасности.

Список литературы

Нормативные правовые акты

1. Конституция Российской Федерации (принята на всенародном голосовании 12.12.1993 г.)// Справочная система «Гарант».
2. Уголовный кодекс Российской Федерации от 13 июня 1996г.№63-ФЗ. // Справочная система «Гарант».
3. Федеральный Закон «Об информации, информационных технологиях и защите информации» от 27 июля 2006г. №149-ФЗ (с изм. и доп. от 23.04.18) // Справочная система «Гарант».
4. Федеральный Закон «О коммерческой тайне» от 29 июля 2004г. №98-ФЗ. (с изм. и доп. от 18.04.18) // Справочная система «Консультант плюс».
5. Часть четвертая Гражданского кодекса РФ, принятая Государственной Думой ФС РФ (24.11.2006г.) (с изм. и доп. от 28.03.17) // Справочная система «Гарант».
6. Федеральный закон «О связи» от 07 июля 2003 г. №126-ФЗ (с изм. от 29.07.17) // Справочная система «Консультант плюс».
7. Доктрина информационной безопасности Российской Федерации 9 утв. Указом Президентом РФ от 17 декабря 1997г. №1300//СЗ РФ.2000.28 сентября»187.
8. Закон «О государственной тайне» от 21 июля 1993 г. № 5485-1 // Справочная система «Гарант».
9. Закон «Об обязательном экземпляре документов» от 29 декабря 1994 г. 77-ФЗ (с изм. и доп. от 03.07.16) // Справочная система «Гарант».
10. Модельный Уголовный Кодекс. Рекомендательный законодательный акт для Содружества Независимых Государств. Принят на 7-м пленарном заседании Межпарламентской ассамблеи государств-участником СНГ 17 февраля 1996г.//Приложение к информационному бюллетеню».1996.№10

11. Указ Президента РФ от 12 мая 2004 г.№611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена»// СЗ РФ.2000.№2.Ст.170
12. Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств - участников Содружества Независимых Государств в сфере информатизации (Москва, 24 декабря 1999 г.) // Бюллетень международных договоров,2002.№11.
13. Соглашение с сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации Минск, 1 июня 2001 г.) Текст Соглашения официально опубликован не был// СПС «Гарант».

Научная и учебная литература

14. Антонян Ю.М., Еникеев М.И.Психология преступника и расследования преступлений / Ю.М. Антонян, М.И. Еникеев. - М.: Юрист,1996.- С.28
15. Баев О.Я., Мещеряков В.А. Проблемы уголовно-правового регулирования в сфере компьютерной информации /О.Я. Баев, В.А. Мещеряков // Защита информации. - Конфидент. -1998.- № 5.
16. Барсуков В.С., Водолазский В.В. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский .- М.: Нолидж, 2000. - С.64
17. Батурин Ю.М., Жодзинский А.М. / Компьютерная преступность и компьютерная безопасность// Ю. М. Батурин, А.М. Жодзинский. - М.: Юридическая литература, 1998. - С.52-54.
18. Батурин Ю.М.Проблемы компьютерного права / Ю.М. Батурин.- М.: Юридическая литература, 1998. - С.14.
19. Безруков Н.А.Введение в компьютерную вирусологию. Общие принципы функционирования, классификация и каталог наиболее распространенных вирусов в MS DOS / Н.А. Безруков. - Киев, 2006. - С.86

20. Беляев В.С. Безопасность в распределительных системах / В.С. Беляев - М., 1995.
21. Борзенков Г.Н., Комиссаров В.С. Уголовное право Российской Федерации / Г.Н. Борзенков, В.С. Комисаров. - М.: Олимп, 1997.
22. Волеводз А.Г.Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. - М.: Изд-во Юрлитиформ, 2000.-С.495.
23. Вехов В.Б., Рогозин В.Ю. Методика расследования преступлений в сфере компьютерной информации // Криминалистическая методика расследования отдельных видов преступлений: Учеб. пособие в 2-х частях.
24. Горбатов В.С., Полянская О.Ю., Доказывание в судебных делах по компьютерным преступлениям В.С. Горбатов, О.Ю. Полянская. -М.: МИФИ, 1997.
25. Дворецкий М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания / М.Ю. Дворецкий. - Тамбов, 2003.
26. Дворецкий М.Ю. Преступления в сфере информации: Научно-практический комментарий к гл.28.Уголовного кодекса РФ/ М.Ю.Дворецкий. - М.,2005.
27. Дворецкий М., Копырюлин А. Проблемы квалификации преступлений, сопряженных с созданием, использованием и распространением вредоносных программ / М. Дворецкий, А. Копырюлин // Уголовное право. - 2007. - №4.
28. Дворецкий М.Ю. Преступления в сфере компьютерной информации (уголовно-правовое исследование) / М.Ю. Дворецкий. Волгоград, 2001 (Диссертация и автореферат)
29. Жуков Ю.И., Приманкин А.И., Щербаков О.В.Информационная безопасность и аппаратно-программная надежность компьютерных средств органов внутренних дел//Вестник МВД России,2000, - №3.-С.75-81

30. Информация как элемент криминальной деятельности /Крылов В.В./Вестник Московского университета, Серия 11, Право, 1998, № 4
31. Информационные вызовы национальной и международной безопасности/ под. общ. ред. А.В.Федорова, В.Н.Цыгиченко.М.,2001.
32. Как остановить компьютерное пиратство? / Симкин Л.// Российская юстиция, 1996, №10)
33. Карелина М.М. Преступления в сфере компьютерной информации / М.М. Карелина. - М., 1998.
34. Кириченко А.Н. Вирусы научились размножаться по своим законам / А.Н. Кириченко // МН Коллекция. -2003. - №2. - С.12
35. Козлов В.Е.Теория и практика борьбы с компьютерной преступностью /В.Е. Козлов. - М.: Горячая линия, Телеком. - 2002. - С.161
36. Комиссаров В.С. Преступления в сфере компьютерной безопасности: понятие и ответственность/ В.С. Комисаров // Юридический мир. 2003. - №2. -С.13
37. Комментарий к Гражданскому кодексу РФ части четвертой. Правовое регулирование отношений в сфере интеллектуальной собственности. Автор комментариев и составитель - А.Б.Борисов - М.: Книжный мир, 2008. - 288с.
38. Комментарий к Гражданскому кодексу РФ части 4.Правовое регулирование отношений в сфере интеллектуальной деятельности. С постатейными материалами и практическими разъяснениями. Автор комментариев и составитель- А.Б.Борисов - М.: Книжный мир, 2008- С.51
39. Комментарий к уголовному кодексу РФ. Научно-практический комментарий/Отв. ред. В.М. Лебедев. - М.Юрайт - М, 2004.С.560
40. Компьютерные технологии в юридической деятельности: Учебное и
41. Котухов М.М., Марков А.С. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем / М.М. Котухов, А.С.Марков - СПб.: ВУС, 2004. - 190 с.

42. Криминогенные аспекты глобальной сети Интернет /И.Н. Соловьев //Налоговый вестник, № 4, апрель 2001 г.
43. Копырюлин А. Н. Преступления в сфере компьютерной информации: Уголовно-правовой и криминологический аспекты: Автореф. дис. ... канд. юрид. наук. / А. Н. Копырюлин. - Тамбов, 2007.
44. Копырюлин А.Н. Квалификация преступлений в сфере компьютерной информации / А. Копырюлин // Законность. - 2007. - № 6.
45. Кузнецов А.В.Некоторые вопросы расследования преступлений в сфере компьютерной информации//Информационный бюллетень следственного комитета МВД РФ.
46. Кузнецов А. П. Ответственность за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (ст. 274 УК РФ) / А. П. Кузнецов // Правовые вопросы связи. - 2007. - № 2.
47. Кузнецов А. П. Ответственность за преступления в сфере компьютерной информации по зарубежному законодательству / А. П. Кузнецов // Международное публичное и частное право. - 2007. - N 3.
48. Маляров А. И. Объект преступления в сфере электронно-цифровой (компьютерной) информации и вопросы квалификации (российский и зарубежный опыт) / А. И. Маляров // Общество и право. - 2008. - N 2.
49. Маслакова Е. А. История правового регулирования уголовной ответственности за компьютерные преступления / Е. А. Маслакова // Информационное право. - 2006. - N 4.
50. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: ВГУ, 2002. - 408 с.
51. Наумов А. В. Практика применения Уголовного кодекса Российской Федерации: Комментарий судебной практики и доктринальное толкование / А. В. Наумов. - М.: Волтерс Клувер, 2005.
52. Расследование хищений, совершаемых в кредитно-финансовой сфере с использованием электронных средств /В.Г.Баяхчев, В.В. Улейчик, //Законодательство, № 6, июнь 2000 г.

53. Резвана А.П., Субботиной М.В. - М.: ИМЦ ГУК МВД России, 2002. - С. 84-108.
54. Состояние преступности в Российской Федерации: Статистика // Официальный сайт МВД РФ www.mvd.ru
55. Уголовное право РФ. Особенная часть: Учебник / Под ред. проф. Б. В. Здравомыслова. - 2-е изд., перераб. и доп. - М.: Юристъ, 2001.
56. Уголовное право Российской Федерации. Особенная часть: Учебник/ Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. - 2-е изд.,
57. Ушаков С.И. Преступления в сфере обращения компьютерной информации (теория, законодательство, практика) - Ростов-на-Дону, 2001г.- С.169
58. Ястребов Д. А. Вопрос о латентности неправомерного доступа к компьютерной информации в Российской Федерации / Д. А. Ястребов // Юридический мир. - 2008. - № 10.
59. Ястребов Д. А. Вопросы отграничения неправомерного доступа к компьютерной информации от смежных составов преступлений / Д. А. Ястребов // Российский следователь. - 2008. - № 17.
60. Ястребов Д. А. Законодательный опыт стран - участниц Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации / Д. А. Ястребов // Российский следователь. - 2008. - № 6.

Рецензия

на выпускную квалификационную работу на тему «Ответственность за неправомерный доступ к компьютерной информации по УК РФ», подготовленную слушателем учебной группы № 131 факультета очного обучения Казанского юридического института МВД России младшим лейтенантом полиции Мась Дмитрием Владимировичем.

Представленная на рецензирование рукопись выпускной квалификационной работы[1] на тему «Ответственность за неправомерный доступ к компьютерной информации по УК РФ», подготовленная слушателем факультета очного обучения[2] Казанского юридического института МВД России[3] младшим лейтенантом полиции Мась Дмитрием Владимировичем, представляется весьма актуальной для сотрудников территориальных и других органов МВД Российской Федерации[4], поскольку посвящена выработке практических знаний и умений по применению мер предупреждения и противодействия преступлениям в сфере компьютерной информации. С учетом постоянно развивающейся компьютерной техники, повышением важности информационной безопасности, а также быстрым обучением специальным познаниям лицами, занимающимся преступной деятельностью, вопросы по предупреждению и противодействию преступлениям в сфере компьютерной ифнормации будут появляться как в теории, так и в практике. Проведенное исследование, в рамках выпускной квалификационной работы по противодействию преступлениям в сфере компьютерной информации, раскрывает основные понятия и методы в организации и тактике противодействия преступлениям в сфере компьютерной информации, позволяет выявить имеющийся положительный опыт при документировании данных преступлений.

---

[1] Далее – «ВКР и (или) работа».
[2] Далее – «ФОО».
[3] Далее – «КЮИ МВД России и (или) институт».
[4] Далее – «Органы внутренних дел» и (или) «ОВД».

Содержание рукописи выпускной квалификационной работы составляют введение, две главы по четыре параграфа в каждом, заключение, список использованных нормативных правовых актов, учебной и учебно-методической литературы.

Как и всякая творческая работа, рецензируемый материал содержит ряд положений, которые, на взгляд рецензента, носят дискуссионный характер и могут быть изложены в несколько иной редакции. При написании своей работы дипломнику следовало бы как можно больше изучить и проанализировать имеющийся положительный опыт по противодействию преступлений в сфере компьютерной информации в других субъектах Российской Федерации, и в зарубежных государствах.

В целом рецензируемое ВКР, подготовленная слушателем КЮИ МВД России младшим лейтенантом полиции Мась Дмитрием Владимировичем, базируется на хорошем знании автором теоретических и практических материалов, нормативных документов, специфики работы правоохранительных органов, отвечает требованиям, предъявляемым к подобному рода работам, а при устранении отмеченных выше недостатков может заслуживать положительной оценки.

Руководитель следственного органа –
начальник отдела по расследованию преступлений на территории
обслуживаемой ОП №12 «Гвардейский»,
СУ УМВД России по г. Казани
подполковник юстиции И.Р. Ахметзянов

«23» 03 2018 г.

М.П.

ОТЗЫВ

о ходе выполнения выпускной квалификационной работы
слушателя 131 учебной группы Мась Дмитрия Владимировича
на тему «Ответственность за неправомерный доступ к компьютерной информации по УК РФ»

Представленная на рецензирование рукопись выпускной квалификационной работы на тему «Ответственность за неправомерный доступ к компьютерной информации по УК РФ», подготовленная слушателем факультета очного обучения Казанского юридического института МВД России Мась Дмитрием Владимировичем, выбрана из списка предложенного кафедрой и представляется весьма актуальной для сотрудников территориальных и других органов МВД Российской Федерации, поскольку посвящена выработке практических знаний и умений по применению мер предупреждения и противодействия преступлениям в сфере компьютерной информации.

С учетом постоянно развивающейся компьютерной техники, повышением важности информационной безопасности, а также быстрым обучением специальным познаниям лицами, занимающимся преступной деятельностью, вопросы по предупреждению и противодействию преступлениям в сфере компьютерной информации будут появляться как в теории, так и в практике. Проведенное исследование, в рамках выпускной квалификационной работы по противодействию преступлениям в сфере компьютерной информации, раскрывает основные понятия, виды юридической ответственности, личность злоумышленника и предложения в организации противодействия преступлениям в сфере компьютерной информации.

Согласно поставленным целям и задачам исследования с учетом ее актуальности содержание рукописи выпускной квалификационной работы составляют введение, две главы по четыре параграфа в каждом, заключение, список использованных нормативных правовых актов, учебной и учебно-методической литературы.

Как и всякая творческая работа, рецензируемый материал содержит ря положений, которые, на взгляд рецензента, носят дискуссионный характер могут быть изложены в несколько иной редакции. При написании своей работ слушателю следовало бы как можно больше изучить и проанализироват имеющийся положительный опыт по противодействию преступлений в сфер компьютерной информации в других субъектах Российской Федерации, и зарубежных государствах.

В целом рецензируемое ВКР, подготовленная слушателем КЮИ МВ России младшим лейтенантом полиции Мась Дмитрием Владимировичем базируется на хорошем знании автором теоретических и практически материалов, нормативных документов, специфики работы правоохранительны органов, отвечает требованиям, предъявляемым к подобному рода работам, при устранении отмеченных выше недостатков может заслуживат положительной оценки.

Научный руководитель:
доктор юридических наук
профессор кафедры уголовно права
М.В. Талан

«24» 05 2018 г.

Подпись М.В. Талан
УДОСТОВЕРЯЕТСЯ
ОД и Р КЮИ МВД России

АНТИПЛАГИАТ
ТВОРИТЕ СОБСТВЕННЫМ УМОМ

УВАЖАЕМЫЙ ПОЛЬЗОВАТЕЛЬ!

Обращаем ваше внимание, что система «Антиплагиат» отвечает на вопрос, является ли тот или иной фрагмент текста заимствованным или нет. Ответ на вопрос, является ли заимствованный фрагмент именно плагиатом, а не законной цитатой, система оставляет на ваше усмотрение. Данный отчет не подлежит использованию в коммерческих целях.

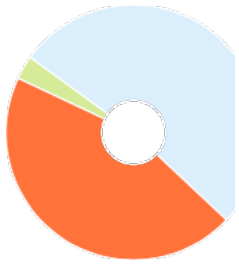
Отчет о проверке на заимствования №1

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 166
Начало загрузки: 07.06.2018 19:49:44
Длительность загрузки: 00:01:10
Имя исходного файла: Проект Дипломной_работы_0.011
Размер текста: 80 кБ
Символов в тексте: 121084
Слов в тексте: 14602
Число предложений: 768

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Последний готовый отчет (ред.)
Начало проверки: 07.06.2018 19:50:55
Длительность проверки: 00:00:09
Комментарии: не указано
Модули поиска: Модуль поиска ЭБС "БиблиоРоссика", Модуль поиска ЭБС "BOOK.ru", Коллекция РГБ, Цитирование, Модуль поиска ЭБС "Университетская библиотека онлайн", Коллекция eLIBRARY.RU, Коллекция ГАРАНТ, Модуль поиска ЭБС "Айбукс", Модуль поиска Интернет, Модуль поиска "КЮИ МВД РФ", Модуль поиска ЭБС "Лань", Сводная коллекция вузов МВД, Кольцо вузов



ЗАИМСТВОВАНИЯ	ЦИТИРОВАНИЯ	ОРИГИНАЛЬНОСТЬ
44,63%	3,37%	52%

№	Доля в отчете	Доля в тексте	Источник	Ссылка	Актуален на	Модуль поиска	Блоков в отчете	Блоков в тексте
[01]	7,06%	42,77%	Скачать/bestref-156914.doc	http://bestreferat.ru	08 Июн 2012	Модуль поиска Интернет	1	189
[02]	4,96%	37,32%	Борисов Сергей Преступлен...	http://dlib.rsl.ru	17 Фев 2014	Коллекция РГБ	116	379
[03]	13,96%	25,05%	Преступления в сфере комп...	http://knowledge.allbest.ru	раньше 2011	Модуль поиска Интернет	14	121
[04]	0,02%	17,6%	Егорышев, Александр Серге...	http://dlib.rsl.ru	раньше 2011	Коллекция РГБ	2	115
[05]	10,94%	12,42%	Преступления в сфере комп...	http://knowledge.allbest.ru	раньше 2011	Модуль поиска Интернет	4	29
[06]	3,07%	8,39%	Преступления в сфере комп...	http://knowledge.allbest.ru	раньше 2011	Модуль поиска Интернет	34	116
[07]	0,07%	7,45%	Юридический институт МВД...	http://lawdiss.org.ua	раньше 2011	Модуль поиска Интернет	2	87
[08]	0%	6,98%	ОСНОВНЫЕ ОБСТОЯТЕЛЬСТ...	http://elibrary.ru	28 Авг 2014	Коллекция eLIBRARY.RU	0	63
[09]	0,46%	6,97%	Ястребов, Дмитрий Андреев...	http://dlib.rsl.ru	02 Фев 2013	Коллекция РГБ	16	96
[10]	0,31%	6,73%	Шарков, Александр Евгенье...	http://dlib.rsl.ru	20 Янв 2010	Коллекция РГБ	8	80
[11]	0,12%	5,94%	Геллер, Артем Владимирови...	http://dlib.rsl.ru	20 Янв 2010	Коллекция РГБ	5	79
[12]	0,06%	5,63%	Гаврилин, Юрий Викторови...	http://dlib.rsl.ru	раньше 2011	Коллекция РГБ	2	64
[13]	1,19%	5,46%	Копырюлин, Алексей Никол...	http://dlib.rsl.ru	02 Фев 2013	Коллекция РГБ	31	115
[14]	0%	5,25%	Сизова баринов.doc	не указано	06 Мая 2013	Сводная коллекция вузов МВД	0	66
[15]	0,27%	4,91%	Гаврилин, Юрий Викторови...	http://dlib.rsl.ru	07 Мар 2012	Коллекция РГБ	12	90
[16]	0%	4,76%	Пожилых, Валерий Алексан...	http://dlib.rsl.ru	20 Янв 2010	Коллекция РГБ	0	51
[17]	0,23%	3,95%	диплом отредактированны...	не указано	06 Мая 2016	Кольцо вузов	5	74

[18]	0,08%	3,94%	2014.zip/Этибарян А.Г.doc	не указано	27 Апр 2017	Кольцо вузов	3	53
[19]	0%	3,92%	Лыткин, Николай Николаев...	http://dlib.rsl.ru	02 Фев 2013	Коллекция РГБ	0	81
[20]	0,05%	3,74%	Карпов, Виктор Сергеевич д...	http://dlib.rsl.ru	26 Дек 2011	Коллекция РГБ	2	73
[21]	0,21%	3,71%	2760Antiplagiat.zip/DSLH201...	не указано	27 Авг 2015	Кольцо вузов	5	63
[22]	0%	3,56%	Распопова, Анна Викторовн...	http://dlib.rsl.ru	раньше 2011	Коллекция РГБ	0	48
[23]	0%	3,5%	Экономические и правовые...	http://bibliorossica.com	25 Мая 2016	Модуль поиска ЭБС "БиблиоРоссика"	0	62
[24]	0%	3,5%	13770	http://e.lanbook.com	09 Мар 2016	Модуль поиска ЭБС "Лань"	0	62
[25]	0%	3,5%	Диплом комп.преступность ...	не указано	15 Мая 2013	Сводная коллекция вузов МВД	0	56
[26]	0%	3,44%	Оптимизация уголовной от...	http://elibrary.ru	19 Дек 2015	Коллекция eLIBRARY.RU	1	65
[27]	0,33%	3,4%	Евдокимов, Константин Ник...	http://dlib.rsl.ru	20 Янв 2010	Коллекция РГБ	8	59
[28]	0%	3,39%	Сударева, Лилия Александр...	http://dlib.rsl.ru	02 Фев 2013	Коллекция РГБ	0	62
[29]	0,14%	3,38%	Дворецкий, Михаил Юрьев...	http://dlib.rsl.ru	26 Дек 2011	Коллекция РГБ	4	58
[30]	0,03%	3,02%	Ковалев И.И..doc	не указано	07 Апр 2014	Сводная коллекция вузов МВД	2	81
[31]	0,05%	2,96%	Проблемы борьбы в сфере ...	не указано	24 Июл 2014	Сводная коллекция вузов МВД	2	50
[32]	0,06%	2,93%	Лопатина, Татьяна Михайло...	http://dlib.rsl.ru	20 Янв 2010	Коллекция РГБ	4	54
[33]	0,06%	2,89%	Евдокимов, Максим Валери...	http://dlib.rsl.ru	раньше 2011	Коллекция РГБ	2	50
[34]	0,04%	2,82%	Бессонов, Владимир Анатол...	http://dlib.rsl.ru	26 Дек 2011	Коллекция РГБ	2	49
[35]	0%	2,8%	Преступления в сфере комп...	http://elibrary.ru	23 Сен 2015	Коллекция eLIBRARY.RU	0	56
[36]	0,72%	2,69%	Комментарий к Уголовному ...	http://ivo.garant.ru	13 Янв 2017	Коллекция ГАРАНТ	13	55
[37]	0%	2,55%	253556	http://biblioclub.ru	19 Апр 2016	Модуль поиска ЭБС "Университетская библиотека онлайн"	0	58
[38]	0%	2,55%	Государственная информац...	http://ibooks.ru	09 Дек 2016	Модуль поиска ЭБС "Айбукс"	0	58
[39]	0%	2,55%	5175	http://e.lanbook.com	09 Мар 2016	Модуль поиска ЭБС "Лань"	0	58
[40]	0%	2,51%	Шмелева_Этап_3._Прохожде...	не указано	17 Ноя 2016	Кольцо вузов	0	53
[41]	0,07%	2,47%	ISBN9785913590381.txt	не указано	26 Окт 2017	Кольцо вузов	2	32
[42]	0%	2,44%	1 и 2 квартал.rar/Исаева. Ме...	не указано	24 Июл 2014	Сводная коллекция вузов МВД	0	40
[43]	0%	2,41%	Земсков Глухова.docx	не указано	23 Мая 2013	Сводная коллекция вузов МВД	0	40
[44]	0%	2,41%	Вопросы отграничения неп...	http://elibrary.ru	раньше 2011	Коллекция eLIBRARY.RU	0	35
[45]	0%	2,38%	2009_1(10).doc	не указано	17 Янв 2012	Сводная коллекция вузов МВД	0	39
[46]	0,34%	2,38%	Ямщикова, Надежда Владим...	http://dlib.rsl.ru	раньше 2011	Коллекция РГБ	14	52
[47]	0,07%	2,38%	2006.rar/Проблемы борьбы ...	не указано	24 Июл 2014	Сводная коллекция вузов МВД	3	39
[48]	0%	2,33%	Вестник_ЮНиП_2007_7.docx	не указано	08 Окт 2015	Сводная коллекция вузов МВД	0	57
[49]	0,04%	2,26%	2007_7.doc	не указано	17 Янв 2012	Сводная коллекция вузов МВД	2	55
[50]	0%	2,24%	45554	http://e.lanbook.com	09 Мар 2016	Модуль поиска ЭБС "Лань"	0	48
[51]	0,14%	2,24%	Москвитина_Этап_3._Прохо...	не указано	17 Ноя 2016	Кольцо вузов	3	39
[52]	0%	2,21%	Работа. ВКР 24.06.2017 _исп...	не указано	25 Июн 2017	Кольцо вузов	0	40
[53]	0,47%	2,16%	Комментарий к Уголовному ...	http://ivo.garant.ru	12 Янв 2017	Коллекция ГАРАНТ	12	43
[54]	0%	2,06%	Вестник_ЮНиП_2009_1(10).d...	не указано	08 Окт 2015	Сводная коллекция вузов МВД	0	30
[55]	0%	2,06%	61737	http://e.lanbook.com	09 Мар 2016	Модуль поиска ЭБС "Лань"	0	40

[56]	0%	1,99%	140255	http://biblioclub.ru	18 Апр 2016	Модуль поиска ЭБС "Университетская библиотека онлайн"	0	33
[57]	0,04%	1,99%	2006.rar/Раскрытие и рассле...	не указано	24 Июл 2014	Сводная коллекция вузов МВД	3	55
[58]	0%	1,86%	08_04_16_МХГильмутдинов_...	не указано	08 Апр 2016	Кольцо вузов	0	42
[59]	0%	1,84%	Информационная безопасн...	http://ibooks.ru	09 Дек 2016	Модуль поиска ЭБС "Айбукс"	0	49
[60]	0,13%	1,78%	Комментарий к Уголовному ...	http://ivo.garant.ru	13 Янв 2017	Коллекция ГАРАНТ	4	47
[61]	0%	1,78%	не указано	http://rulitru.ru	26 Ноя 2012	Модуль поиска Интернет	0	47
[62]	0%	1,78%	Егорышев, Александр Серге...	http://dlib.rsl.ru	21 Янв 2010	Коллекция РГБ	0	26
[63]	0%	1,76%	УГОЛОВНОЕ ПРАВО	http://lawdiss.org.ua	07 Ноя 2012	Модуль поиска Интернет	0	43
[64]	0,04%	1,75%	Шемякин Михаил Юрьевич ...	не указано	13 Мая 2017	Кольцо вузов	1	39
[65]	0,03%	1,75%	Юридическая техника №7 Ч...	не указано	29 Окт 2015	Сводная коллекция вузов МВД	1	45
[66]	0%	1,69%	70952	http://e.lanbook.com	09 Мар 2016	Модуль поиска ЭБС "Лань"	0	46
[67]	0%	1,6%	ИНФОРМАЦИОННАЯ БЕЗОП...	http://elibrary.ru	07 Ноя 2015	Коллекция eLIBRARY.RU	0	31
[68]	0%	1,55%	ПРАВОВАЯ ХАРАКТЕРИСТИК...	http://elibrary.ru	21 Фев 2018	Коллекция eLIBRARY.RU	0	14
[69]	0%	1,52%	Криминалистика	http://ibooks.ru	09 Дек 2016	Модуль поиска ЭБС "Айбукс"	0	28
[70]	0%	1,5%	не указано	http://uchebalegko.ru	10 Ноя 2012	Модуль поиска Интернет	0	30
[71]	0,01%	1,38%	Полный текст диссертации	http://istina.msu.ru	13 Янв 2017	Модуль поиска Интернет	1	51
[72]	0,49%	1,38%	Агешкина Н.А., Беляев М.А., ...	http://ivo.garant.ru	12 Янв 2017	Коллекция ГАРАНТ	12	37
[73]	0%	1,34%	61746	http://e.lanbook.com	09 Мар 2016	Модуль поиска ЭБС "Лань"	1	26
[74]	0,15%	1,34%	Комментарий к Уголовному ...	http://ivo.garant.ru	15 Янв 2017	Коллекция ГАРАНТ	3	30
[75]	0%	1,29%	Международно-правовое со...	http://elibrary.ru	28 Авг 2014	Коллекция eLIBRARY.RU	0	17
[76]	0%	1,29%	Соглашение о сотрудничест...	http://elibrary.ru	28 Авг 2014	Коллекция eLIBRARY.RU	0	17
[77]	0%	1,29%	Соглашение о сотрудничест...	http://ivo.garant.ru	13 Янв 2017	Коллекция ГАРАНТ	0	17
[78]	0,02%	1,26%	Трибуна молодых ученых 2...	не указано	05 Ноя 2015	Сводная коллекция вузов МВД	1	32
[79]	0%	1,25%	Основы информационной б...	http://ibooks.ru	09 Дек 2016	Модуль поиска ЭБС "Айбукс"	0	12
[80]	0%	1,23%	Российское уголовное прав...	http://bibliorossica.com	27 Мая 2016	Модуль поиска ЭБС "БиблиоРоссика"	0	28
[81]	0%	1,23%	Российское уголовное прав...	http://ibooks.ru	09 Дек 2016	Модуль поиска ЭБС "Айбукс"	0	28
[82]	0%	1,21%	Основы права интеллектуал...	https://book.ru	03 Июл 2017	Модуль поиска ЭБС "BOOK.ru"	0	29
[83]	0,07%	1,18%	Уголовное право России. Ос...	http://ivo.garant.ru	14 Янв 2017	Коллекция ГАРАНТ	4	31
[84]	0,01%	1,18%	254082	http://biblioclub.ru	19 Апр 2016	Модуль поиска ЭБС "Университетская библиотека онлайн"	1	32
[85]	0%	1,15%	Лопашенко Н.А. Посягатель...	http://ivo.garant.ru	15 Янв 2017	Коллекция ГАРАНТ	0	30
[86]	0%	1,15%	142535	http://biblioclub.ru	18 Апр 2016	Модуль поиска ЭБС "Университетская библиотека онлайн"	0	21
[87]	0%	1,11%	42324	http://e.lanbook.com	09 Мар 2016	Модуль поиска ЭБС "Лань"	0	12
[88]	0%	1,11%	Информационные технолог...	http://ibooks.ru	09 Дек 2016	Модуль поиска ЭБС "Айбукс"	0	25
[89]	0%	1,1%	Уголовное право России. Ос...	http://ibooks.ru	09 Дек 2016	Модуль поиска ЭБС "Айбукс"	0	29
[90]	0%	1,08%	54710	http://e.lanbook.com	09 Мар 2016	Модуль поиска ЭБС "Лань"	0	21
[91]	0%	1,04%	2013 ВНИИ2.rar/М Инф прот...	не указано	30 Июл 2014	Сводная коллекция вузов МВД	0	27
[92]	0,35%	0,99%	Крыжановская А.А. Граждан...	http://ivo.garant.ru	13 Янв 2017	Коллекция ГАРАНТ	6	19
			Вестник ЮНиП 2006 6.docx			Сводная коллекция		

[93]	0%	0,98%		не указано	08 Окт 2015	вузов МВД	0	22
[94]	0%	0,98%	Уголовное право России. Ча...	https://book.ru	03 Июл 2017	Модуль поиска ЭБС "BOOK.ru"	0	25
[95]	0%	0,98%	252382	http://biblioclub.ru	19 Апр 2016	Модуль поиска ЭБС "Университетская библиотека онлайн"	0	25
[96]	0%	0,98%	54714	http://e.lanbook.com	09 Мар 2016	Модуль поиска ЭБС "Лань"	0	25
[97]	0%	0,97%	Неправомерный доступ к ко...	http://elibrary.ru	27 Авг 2014	Коллекция eLIBRARY.RU	0	22
[98]	0,25%	0,95%	Комментарий к Уголовному ...	http://ivo.garant.ru	12 Янв 2017	Коллекция ГАРАНТ	4	19
[99]	0%	0,95%	Правовые основы противод...	http://elibrary.ru	раньше 2011	Коллекция eLIBRARY.RU	0	9
[100]	0%	0,94%	Теоретические основы пред...	https://book.ru	03 Июл 2017	Модуль поиска ЭБС "BOOK.ru"	0	12
[101]	0%	0,91%	Основы права интеллектуал...	http://bibliorossica.com	26 Мая 2016	Модуль поиска ЭБС "БиблиоРоссика"	0	17
[102]	0%	0,9%	Организация и технологии ...	http://bibliorossica.com	27 Дек 2016	Модуль поиска ЭБС "БиблиоРоссика"	0	20
[103]	0%	0,88%	ПРЕДУПРЕЖДЕНИЕ ПРЕСТУП...	http://elibrary.ru	25 Дек 2016	Коллекция eLIBRARY.RU	0	20
[104]	0%	0,86%	Комментарий к Уголовному ...	http://ivo.garant.ru	15 Янв 2017	Коллекция ГАРАНТ	0	18
[105]	0%	0,86%	Компьютерная информация...	http://elibrary.ru	11 Мая 2018	Коллекция eLIBRARY.RU	0	20
[106]	0%	0,82%	Закон Республики Хакасия о...	http://ivo.garant.ru	14 Янв 2017	Коллекция ГАРАНТ	0	9
[107]	0%	0,79%	Основы электронной комме...	http://bibliorossica.com	25 Мая 2016	Модуль поиска ЭБС "БиблиоРоссика"	0	14
[108]	0%	0,79%	НАРУШЕНИЕ ПРАВИЛ ЭКСП...	http://elibrary.ru	15 Янв 2017	Коллекция eLIBRARY.RU	0	7
[109]	0%	0,78%	227359	http://biblioclub.ru	19 Апр 2016	Модуль поиска ЭБС "Университетская библиотека онлайн"	0	19
[110]	0%	0,78%	Баранов, Мацкевич 2009 Пр...	не указано	30 Окт 2015	Сводная коллекция вузов МВД	0	27
[111]	0%	0,77%	Основы права интеллектуал...	http://bibliorossica.com	26 Мая 2016	Модуль поиска ЭБС "БиблиоРоссика"	0	13
[112]	0%	0,74%	Право и информатизация о...	http://elibrary.ru	30 Авг 2014	Коллекция eLIBRARY.RU	0	16
[113]	0%	0,73%	239102	http://biblioclub.ru	раньше 2011	Модуль поиска ЭБС "Университетская библиотека онлайн"	0	9
[114]	0,14%	0,69%	Гаврилов Э.П., Городов О.А.,...	http://ivo.garant.ru	15 Янв 2017	Коллекция ГАРАНТ	2	8
[115]	0%	0,69%	Политические причины как ...	http://elibrary.ru	раньше 2011	Коллекция eLIBRARY.RU	0	13
[116]	0%	0,66%	Комментарий к Уголовному ...	https://book.ru	03 Июл 2017	Модуль поиска ЭБС "BOOK.ru"	0	16
[117]	0%	0,65%	Платежные карты. Бизнес-э...	http://bibliorossica.com	26 Мая 2016	Модуль поиска ЭБС "БиблиоРоссика"	0	15
[118]	0%	0,65%	Уголовное законодательств...	http://ibooks.ru	09 Дек 2016	Модуль поиска ЭБС "Айбукс"	0	16
[119]	0%	0,63%	Политические причины как ...	http://ivo.garant.ru	14 Янв 2017	Коллекция ГАРАНТ	0	9
[120]	0%	0,6%	Выявление и расследовани...	http://ibooks.ru	09 Дек 2016	Модуль поиска ЭБС "Айбукс"	0	12
[121]	0%	0,6%	227364	http://biblioclub.ru	19 Апр 2016	Модуль поиска ЭБС "Университетская библиотека онлайн"	0	12
[122]	0%	0,6%	Литовченко Александра раб...	не указано	29 Дек 2016	Модуль поиска "КЮИ МВД РФ"	0	17
[123]	0%	0,59%	ISBN9785392165834.txt	не указано	26 Окт 2017	Кольцо вузов	0	14
[124]	0%	0,58%	Комментарий к Гражданско...	https://book.ru	03 Июл 2017	Модуль поиска ЭБС "BOOK.ru"	0	8
[125]	0,03%	0,58%	Колосков СЮ.doc	не указано	08 Дек 2016	Сводная коллекция вузов МВД	1	11
[126]	0%	0,57%	Актуальные проблемы инфо...	https://book.ru	03 Июл 2017	Модуль поиска ЭБС "BOOK.ru"	0	9
[127]	0%	0,56%	Руководство для следовател...	https://book.ru	03 Июл 2017	Модуль поиска ЭБС "BOOK.ru"	0	12
[128]	0%	0,53%	Толкование Особенной част...	http://bibliorossica.com	27 Мая 2016	Модуль поиска ЭБС "БиблиоРоссика"	0	15
[129]	0%	0,51%	Причины и условия соверш...	http://elibrary.ru	17 Дек 2016	Коллекция eLIBRARY.RU	0	4

[130]	0%	0,5%	Юридическая техника №9 2...	не указано	29 Окт 2015	Сводная коллекция вузов МВД	0	13
[131]	0%	0,5%	Политические факторы ком...	http://elibrary.ru	раньше 2011	Коллекция eLIBRARY.RU	0	4
[132]	0%	0,49%	ТЕОРЕТИКО-ПРАВОВЫЕ ОСН...	http://elibrary.ru	14 Сен 2015	Коллекция eLIBRARY.RU	0	15
[133]	0,04%	0,49%	Паутова Э.В. Квалифициров...	http://ivo.garant.ru	13 Янв 2017	Коллекция ГАРАНТ	2	16
[134]	0%	0,48%	252357	http://biblioclub.ru	19 Апр 2016	Модуль поиска ЭБС "Университетская библиотека онлайн"	0	10
[135]	0%	0,48%	Правовое обеспечение инн...	http://elibrary.ru	29 Авг 2014	Коллекция eLIBRARY.RU	0	5
[136]	0,02%	0,46%	Гражданское право: учебно...	http://ibooks.ru	09 Дек 2016	Модуль поиска ЭБС "Айбукс"	2	8
[137]	0%	0,45%	Доктринальные и законодат...	http://elibrary.ru	23 Сен 2015	Коллекция eLIBRARY.RU	0	14
[138]	0%	0,44%	Шутова Дисс без списка 020...	не указано	02 Июн 2017	Сводная коллекция вузов МВД	0	9
[139]	0%	0,42%	227360	http://biblioclub.ru	19 Апр 2016	Модуль поиска ЭБС "Университетская библиотека онлайн"	0	9
[140]	0%	0,42%	Russian	http://unodc.org	12 Янв 2017	Модуль поиска Интернет	0	9
[141]	0%	0,36%	Уголовное право России. Ча...	https://book.ru	03 Июл 2017	Модуль поиска ЭБС "BOOK.ru"	0	6
[142]	0%	0,36%	54713	http://e.lanbook.com	09 Мар 2016	Модуль поиска ЭБС "Лань"	0	6
[143]	0%	0,34%	Уголовное право России. О...	https://book.ru	03 Июл 2017	Модуль поиска ЭБС "BOOK.ru"	0	12
[144]	0%	0,34%	Уголовное право России. О...	http://ivo.garant.ru	15 Янв 2017	Коллекция ГАРАНТ	1	12
[145]	0%	0,31%	2 курс	http://kpfu.ru	29 Ноя 2016	Модуль поиска Интернет	0	6
[146]	0%	0,31%	Соблюдение законности и п...	http://ivo.garant.ru	13 Янв 2017	Коллекция ГАРАНТ	0	3
[147]	0%	0,31%	Ответственность за преступ...	http://bibliorossica.com	26 Мая 2016	Модуль поиска ЭБС "БиблиоРоссика"	0	9
[148]	0%	0,27%	Уголовное право. Общая ча...	https://book.ru	03 Июл 2017	Модуль поиска ЭБС "BOOK.ru"	0	6
[149]	0,05%	0,16%	Комментарий к Уголовно-п...	http://ivo.garant.ru	15 Янв 2017	Коллекция ГАРАНТ	1	3
[150]	0,02%	0,11%	Доктрина информационной...	http://ivo.garant.ru	12 Янв 2017	Коллекция ГАРАНТ	1	4
[151]	0%	0,05%	Гараева Дина Конкурсная р...	не указано	07 Фев 2018	Модуль поиска "КЮИ МВД РФ"	0	2
[152]	0%	0,04%	Тельканова Елена Олеговна...	не указано	22 Дек 2016	Модуль поиска "КЮИ МВД РФ"	0	2
[153]	0%	0,02%	Максуров А.А., Таланова М.В...	http://ivo.garant.ru	15 Янв 2017	Коллекция ГАРАНТ	0	2
[154]	0,48%	0%	не указано	не указано	раньше 2011	Цитирование	2	2