МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

ДЬЯКОВ АЛЕКСЕЙ ПЕТРОВИЧ

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ В ЭЛЕКТРОННЫХ (КОМПЬЮТЕРНЫХ) СЕТЯХ

Направление подготовки 40.03.01 – «Юриспруденция»
юридического факультета СГУ им. Н.Г.Чернышевского

Автореферат бакалаврской работы

Научный руководитель
к.ю.н, доцент кафедры уголовного,
экологического права и криминологии Ф.А. Вестов

Зав. кафедрой уголовного, экологического
права и криминологии
д.ю.н, профессор Н.Т. Разгельдеев

Саратов 2020

Введение

Актуальность темы бакалаврской работы. Непрерывное и стремительное развитие компьютерных технологий и широкое использование электронно-вычислительных систем практически во всех сферах человеческой жизнедеятельности обозначили многочисленные проблемы в области правового регулирования отношений, связанных с компьютеризацией общества. Это не без основательно дает возможность обозначить вопрос о формировании отдельной отрасли компьютерного права, одним из основных аспектов которой являются «компьютерные преступления». Об актуальности проблемы свидетельствует их обширный перечень возможных способов.

За последние годы проведены многие работы, посвященные, в большинстве своем, криминологическим и криминалистическим аспектам компьютерных преступлений. Уголовно-правовые аспекты компьютерных преступлений в настоящее время выражены в научной литературе гораздо менее разобранными. В монографиях и статьях, в основном, затрагивается вопрос об объекте, предмете, орудиях совершения и их соотношение между собой. Некоторые работы содержат конструктивную критику главы 28 Уголовного кодекса РФ, как с уголовно-правовой, так и с информационной точки зрения.

Вышеизложенное является основанием для определения актуальности рассматриваемой темы исследования. Она заключается в массовом распространении компьютерных преступлений по всему миру, а особенно в странах с развитым информационным пространством. В связи с этим по всему миру в нормативную документацию вводятся составы преступлений, регулирующие данный аспект безопасности.

Цель бакалаврскойработы состоит в изучении и анализе положений, характеризующих понятие «компьютерного преступления» и уголовно-правовой состав неправомерного доступа к информации.

Для достижения цели была предпринята попытка решения следующих **задач:**

- ✓ рассмотреть понятие и дать общую характеристику преступлений в сфере компьютерной информации;
- ✓ исследовать Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации;
- ✓ рассмотреть основные нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Объектом исследования являются общественно-правовые отношения, складывающиеся в сфере охраны целостности компьютерной информации.

Предметом данногоисследования является уголовное законодательство, направленное на борьбу с преступностью в сфере высоких информационных технологий.

Степень научной разработанности. Тема исследования носит комплексный междисциплинарный характер.

Общетеоретической основой исследования послужили научные разработки и фундаментальные положения философии, общей теории права, уголовного права, криминологии, юридической психологии, социологии, ряда других дисциплин, а также работы таких ученых-юристов, как: Ю.М. Антонян, В.Н. Кудрявцев, Р.С. Белкин, В.М. Быков, А.Ю. Ларин, А.И. Бойцов, А.И. Рарог,В.В. Черников и др.

Методологическая основа исследования. Для решения поставленных задачи достижения цели исследования были использованы общенаучные методы: анализа и синтеза, индукции и дедукции,диалектико–материалистический.

Правовая основабакалаврской работы сформирована на основе норм Конституции Российской Федерации, федеральных законов, законов Российской Федерации, постановлений и распоряжений Правительства Российской Федерации, актов федеральных органов исполнительной власти,

законов и иных нормативных правовых актов субъектов Российской Федерации.

Эмпирическую основу работы составляют материалы уголовных дел о компьютерных преступлениях, материалы судебной практики по конкретным делам. Кроме того, в работе использованы статистические отчеты МВД, статистические и иные материалы, опубликованные в открытой печати.

Структура работыобусловлена ее темой, целями и задачами и состоит из введения, двух глав, в каждой из которой по 3 параграфа, заключения, списка использованных источников.

Основное содержание работы

Глава первая «Понятие и общая характеристика преступлений в сфере компьютерной информации» состоит из трех параграфов. В первом параграфе «Понятие преступлений в сфере компьютерной информации»проведен обзор теоретической базы исследования.В результате анализа научной литературы данного направления была выявлена неравнозначность таких двух понятий как «компьютерной преступление» и «преступления в сфере компьютерной информации». Было выявлено, что «преступление в сфере компьютерной информации» является частным в общем понятии «компьютерном преступлении».Данное утверждение можно обнаружить и на законодательном уровне. Согласно УК РФ законодатель объединяет все преступления по предмету преступного посягательства, то есть, в данном случае, охраняемой компьютерной информации, а также по непосредственному объекту состава преступления — общественным отношениям в сфере безопасного хранения, обработки и передачи компьютерной информации, в итоге обозначив их как «преступления в сфере компьютерной информации». Однако, понятие «компьютерные преступления», по своей сути является значительно шире. Это обусловлено тем, что вышеуказанное понятие включает множество противоправных действий в области компьютерной информации и информационно-телекоммуникационных сетей. Причем объект состава преступления может

включать в себя общественные отношения в различных сферах человеческой деятельности: общественный нравственности, экономической, здоровье населения[1].

Ученые Д.А. Зыков и М.С. Гаджиев к компьютерным преступлениям так же относят разного рода мошенничества: мошенничество с использованием платежных карт (ст. 159.3 УК РФ); мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), незаконные организация и проведение азартных игр (ст. 171.2 УК РФ); манипулирование рынком (ст. 185.3 УК РФ);незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов (ст. 228.1 УК РФ); изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242.1 УК РФ)[2].

Все вышеперечисленные преступные деяния совершаются с использованием информационно-телекоммуникационных сетей и сети Интернет, в связи с чем Д.А. Зыков относит эти составы преступлений к компьютерным.

Другого мнения придерживается Ю.М. Батурин. Он считает, что такой группы преступлений как компьютерные, в юридическом смысле нет. Развитие и распространение компьютерных средств стало поводом к изменению традиционных видов преступлений. Поэтому, по его мнению, правильнее было бы не выделять отдельную группу «компьютерных преступлений», а говорить лишь об отдельных компьютерных аспектах в составе преступлений[3].

---

[1] Попов, А. Н. Преступления в сфере компьютерной информации : учебное пособие / А. Н. Попов. — Санкт-Петербург : Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. — 68 с

[2] Сундуров Ф.Р., Тарханов И.А. Уголовное право России. Общая часть: Учебник / - 2-е изд., перераб. и доп. - М.: Статут, 2016

[3] Антонян, Ю. М. Криминология : учебник для академического бакалавриата / Ю. М. Антонян. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2018. — 388 с.

В параграфе 1.2 Общая характеристика преступлений в сфере компьютерной информациидана общая характеристика преступлений в сфере компьютерной информации. Более детально рассмотрен объект преступления, субъект, объективная и субъективная стороны. Анализ преступлений в сфере компьютерной информации позволяет определить тяжесть этих преступлений в соответствии со ст.15 УК РФ. Большинство из них относятся к преступлениям средней тяжести и предусматривают лишения свободы сроком до 5 лет. Это обусловлено в основном тем, что большинство опасных последствий наступают в виде вредя для пользователей ПК. Исключения составляют преступления, предусмотренные ч. 1 ст. 273 УК РФ создание, использование и распространение вредоносных компьютерных программ, повлекшие тяжкие последствия или создавшие угрозу их наступления. В данном случае наказания предусмотрены лишением свободы сроком до 7 лет[4].

В рамках проведенной работы было проведено анонимное анкетирование среди студентов второго курса юридического направления НИУ СГУ им. Чернышевского Научно-исследовательский университета«Саратовский государственный Университет им.Н.Г.Чернышевского» в котором приняло участие 37 человек. Целью проводимого анкетирования является мониторинг ситуации и знаний в данной сфере.

В параграфе 1.3 Законодательство РФ об уголовной ответственности за преступления в сфере компьютерной информациипроведен анализ законодательства РФ об уголовной ответственности за преступления в сфере компьютерной информации. По результатам вышерассмотренного можно говорить о том, что в настоящее время уголовное право охраняет не все элементы правоотношений в сфере

[4] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства РФ. - 2014. № 31. - Ст. 4398.

компьютерной информации. В связи с этим необходимо более детально разобрать определяемые в УК РФ составы преступлений.

Повторимся, что в УК РФ три статьи регулируют уголовное право в сфере компьютерной информации. Это ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ», ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети». Содержание каждой из статей УК РФ представлено в таблице в тексте работы.[5].

В **Главе 2. Уголовная ответственность за преступления в сфере компьютерной информации**проведен анализ уголовной ответственности за преступления в сфере компьютерной информации. Данная глава включает в себя 3 параграфа, каждый из которых посвящен отдельно взятой главе УК РФ[6], так или иначе касающийся сферы компьютерной информации.

В параграфе 2.1Неправомерный доступ к компьютерной информацииопределен объект, предмет, субъект, объективная и субъективная стороны преступления.

Для определения объекта данного типа преступления обратимся к статье 272 УК РФ. Во второй части данной статьи дается его четкое определение: «общественные отношения, обеспечивающие правомерный доступ, создание, обработку, преобразование, использование компьютерной информации самим создателем, потребление ее иными пользователями, а также правильное функционирование ЭВМ, системы ЭВМ или их сети»[7].

---

[5] Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 07.04.2020) (с изм. и доп., вступ. в силу с 12.04.2020)// URL http://www.consultant.ru/document/cons_doc_LAW_10699/

[6]Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 07.04.2020) (с изм. и доп., вступ. в силу с 12.04.2020)// URL http://www.consultant.ru/document/cons_doc_LAW_10699/

[7] Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 07.04.2020) (с изм. и доп., вступ. в силу с 12.04.2020)// URL http://www.consultant.ru/document/cons_doc_LAW_10699/

Предметом данного преступления является любая компьютерная информация ограниченного доступа. Для четкого понимания предмета преступления необходимо ясно представлять, что относится к информации ограниченного доступа.

Объективную сторону состава данного преступления оставляет неправомерный доступ к компьютерной информации охраняемой законом. В данном случае под доступом понимается возможность получения самой информации или ознакомления с ней. Он может быть выражен в проникновении в компьютерную систему с использованием специальных средств или получения доступа к системе под именем законного пользователя.

В качестве субъекта данного преступления выступает любое вменяемое лицо, в возрасте от шестнадцати лет.

Субъективная сторона рассматриваемого преступления характеризуется виной в форме умысла или неосторожности.

В параграфе 2.2Создание, использование и распространение вредоносных компьютерных программ определен объект, предмет, субъект, объективная и субъективная стороны преступления.

Объектом преступления в данной статье являются общественные отношения, обеспечивающие безопасность компьютерной информации и компьютеров.

С объективной стороны анализируемое преступление проявляется в совершении хотя бы одного из следующих действий: а) создание компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации; б) использование таких компьютерных программ или такой компьютерной информации; в) распространение таких компьютерных программ или такой компьютерной информации.

В качестве предмета преступления можно выделить аналогично статьи 272 УК РФ любую компьютерную информацию, охраняемую законом.

В качестве субъекта преступления выделяют лицо, достигшее 16-ти летнего возраста. Однако, необходимо иметь ввиду, что речь идет о преступлениях в сфере компьютерной информации, а в настоящее время участились случаи нарушения, регулирующего данный вопрос законодательства, «вундеркиндами», не достигшими шестнадцати лет. В данном случае необходимо руководствоваться уже ст. 20 УК РФ, ответственность за предусмотренные деяния в которой наступает с четырнадцати лет. Если же такая возможность отсутствует вопрос должен решаться с учетом предусмотренной законодательством комиссии по делам несовершеннолетних.

С субъективной стороны данное преступление совершается только с прямым умыслом. Виновный осознает, что создает такую программу либо компьютерную информацию, которая способна уничтожить, заблокировать, модифицировать либо копировать информацию, нарушить работу тех или иных устройств или их сети, либо использует или распространяет вредоносную программу и желает эти действия совершить.

В параграфе 2.3Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетейопределен объект, предмет, субъект, объективная и субъективная стороны преступления.

Объектом преступления можно считать отношения по поводу обеспечения безопасности информационных компьютерных технологий и средств их обеспечения, а также тесно связанных с ними процессов производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления компьютерной информации.

Предметом посягательства являются ЭВМ, система ЭВМ или их сеть.

Объективная сторона преступного нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной

информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям состоит из общественно опасного деяния в форме действия или бездействия, наступивших общественно опасных последствий и причинной связи между ними.

Субъектом является лицо, достигшее 16-летнего возраста, однако, необходимо отметить тот факт, что кроме шестнадцатилетнего возраста субъект данного преступления обладает, в силу своих должностных обязанностей, доступом к средствам хранения, обработки и передачи охраняемых данных, или информационно- телекоммуникационным сетям.

Субъективная сторона преступного нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям характеризуется виной в форме умысла или неосторожности.

Заключение. Изучив и проанализировав уголовную ответственность за преступления, совершаемые в электронных (компьютерных сетях) мы имеем возможность сделать ряд выводов касаемо данной сферы.

Во-первых, на основе статистических данных можно утверждать, что самыми совершаемыми преступлениями в данной сфере являются преступления, подразумевающие неправомерный доступ к компьютерной информации. Они составляют более половины всех преступлений, ответственность за которые предусмотренных главой 28 УК РФ, а именно статьей 272 УК РФ, имеющий в своем составе 4 части, больше чем в двух остальных, относящихся к данной главе. Этому способствует, озвученное выше непрерывное и стремительное развитие компьютерных технологий и широкое использование электронно-вычислительных систем практически во всех сферах человеческой жизнедеятельности.

Во-вторых, за последние годы проведены многие работы, посвященные, в большинстве своем, криминологическим и криминалистическим аспектам компьютерных преступлений. Уголовно-правовые аспекты компьютерных преступлений в настоящее время выражены в научной литературе гораздо менее разобранными. В монографиях и статьях, в основном, затрагивается вопрос об объекте, предмете, орудиях совершения и их соотношение между собой. Некоторые работы содержат конструктивную критику главы 28 Уголовного кодекса РФ, как с уголовно-правовой, так и с информационной точки зрения.

В-третьих, в связи с тем, что различного рода компьютерные «вирусы» и другие вредоносные программы, могут нарушить целостность информации, штатную работу ПК, сети ЭВМ, а также скомпрометировать скрытые различного рода данные остро стоит вопрос о противодействии созданию, использованию и распространению вредоносных компьютерных программ. Ответственность в данной сфере регулирует статья 273 УК РФ, однако, по нашему мнению, данные преступления являются уязвимым местом в УК РФ. Обуславливается это тем, что данные преступления могут нанести гораздо большей вред личности или государству, чем мы можем представить, однако, в этом случае дополнительная ответственность уже может быть дополнительно предусмотрена другими статьями УК РФ. А данный вопрос является еще более актуальным, если рассматривать данную сферу с точки зрения безопасности государства. Не для кого не секрет, что государственное управление и безопасность в развитых странах, в том числе и в России строится уже на основе компьютерных сетей. Проникновение в них разного рода вирусов может поставить под угрозу безопасность всего государства, как с военной точки зрения, так и с точки зрения дестабилизации общественной жизни. Конечно, при наступлении последствий такого масштаба, рассматриваемые выше статьи буду применяться к лицу лишь дополнительно, так как подобные составы преступления регулируются и в других статьях УК РФ, однако, ужесточение наказания в данной сфере,

разработка правильных методик и аппаратов выявления и предупреждения преступлений, а также совершенствования методов поиска нарушителей в компьютерном пространстве должны являться прерогативой работы в данном направлении.

В заключении можно сказать о том, что в настоящее время в России нет такого размаха компьютерной преступности, которая есть в некоторых странах Американского континента, Центральной и Восточной Европы. Но успокаиваться не следует. В Россию она обязательно придет, это связано прежде всего с тем, что наша страна динамично развивается в ногу со временем и уголовный закон наряду с другими мерами профилактического характера должен стать реальным превентивным средством, способствующим созданию условий для нормального развития телекоммуникационных систем и охраны их от преступных посягательств.