

**Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Пензенский государственный университет»**

Юридический институт

Кафедра «Уголовное право»
(наименование)

Направление подготовки

40.03.01 «Юриспруденция»
(код и наименование)

Профиль Правозащитная деятельность
(наименование)

БАКАЛАВРСКАЯ РАБОТА

**по теме: Уголовно-правовая характеристика преступлений в сфере
компьютерной информации**

Студент (ка) гр. 19ЮЮЮЗ
номер группы

подпись, дата

Букур Михаил Степанович
фамилия, имя, отчество

Научный руководитель К.Ю.Н., доцент
должность

каф. «Уголовное право» ФГБОУ ВО ПГУ
наименование организации

подпись, дата

Молев Г.И.
фамилия, инициалы

Консультанты:

ПО _____
наименование раздела, звание, должность

подпись, дата

фамилия, инициалы

ПО _____
наименование раздела, звание, должность

подпись, дата

фамилия, инициалы

ПО _____
наименование раздела, звание, должность

подпись, дата

фамилия, инициалы

Нормоконтролер: К.Ю.Н.,
доцент каф. «Уголовное право»
должность,

подпись, дата

Безрукова О.В.
фамилия, инициалы

Работа допущена к защите в (протокол заседания кафедры от _ 2023г. №__)

Заведующий кафедрой Уголовное право
название

подпись, дата

Романовский Г.Б.
фамилия, инициалы

Работа защищена с оценкой _____ (Протокол от _____ 2023г. №__)

Секретарь ГЭК

подпись, дата

Вдовина Т.Е.
фамилия, инициалы

Пенза 2023 г.

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Юридический институт

Направление «Юриспруденция»

УТВЕРЖДАЮ

Зав. кафедрой «Уголовное право»

название

_____/ Г.Б. Романовский /
(инициалы и фамилия)

_____ 2023 г.

ЗАДАНИЕ

на выпускную квалификационную работу студента (ки) гр. № 19ЮЮ3

Букура Михаила Степановича

1. Тема работы: Уголовно-правовая характеристика преступлений в сфере компьютерной информации

2. Научный руководитель: к.ю.н., доцент каф. УП Молев Г.И.

3. Дата выдачи задания: 14.04.2023 г.

4. Срок сдачи студентом законченной работы: 25.05.23 г.

5. Перечень подлежащих разработке вопросов:

5.1 Общая характеристика преступлений в сфере компьютерной информации

5.2 Уголовно-правовой анализ преступлений, совершаемых в сфере компьютерной информации

5.3 Проблемы квалификации преступлений в сфере компьютерной информации и пути их решения

6. Консультанты по работе, с указанием относящихся к ним разделов работы:

Раздел	Консультант	Подпись, дата	
		Задание выдал	Выполненное задание принял
Введение		14 апреля 2023 г. Молев Г.И.	22 апреля 2023 г. Молев Г.И.
Общая характеристика преступлений в сфере компьютерной информации		22 апреля 2023 г. Молев Г.И.	6 мая 2023 г. Молев Г.И.
Уголовно-правовой анализ преступлений, совершаемых в сфере компьютерной информации		2 мая 2023 г. Молев Г.И.	13 мая 2023 г. Молев Г.И.
Проблемы квалификации преступлений в сфере компьютерной информации и пути их решения		12 мая 2023 г. Молев Г.И.	20 мая 2023 г. Молев Г.И.
Заключение		20 мая 2023 г. Молев Г.И.	25 мая 2023 г. Молев Г.И.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	5
1 Общая характеристика преступлений в сфере компьютерной информации.....	8
1.1 История возникновения и развития компьютерных преступлений: отечественный и зарубежный анализ.....	8
1.2 Понятие и виды преступлений в сфере компьютерной информации.....	18
2 Уголовно-правовой анализ преступлений, совершаемых в сфере компьютерной информации	26
2.1 Неправомерный доступ к компьютерной информации (ст. 272 УК РФ)	26
2.2 Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)	36
2.3 Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).....	45
3 Проблемы квалификации преступлений в сфере компьютерной информации и пути их решения	50
ЗАКЛЮЧЕНИЕ	59
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	61

ВВЕДЕНИЕ

В современном мире информационные технологии занимают все более важное место в жизни общества. Компьютеры и другие устройства, подключенные к интернету, используются не только для работы и общения, но и для хранения и передачи конфиденциальной информации, в том числе персональных данных. Однако, с развитием цифровых технологий возросла и угроза нарушения прав и свобод граждан, а также нарушения конфиденциальности информации.

Актуальность данной темы выражается в том, что за последние годы, количество преступлений совершаемых в сфере компьютерной информации неуклонно растет. Так, за последние 5 лет количество таких преступлений увеличилось в 11 раз. По отчету Генеральной прокуратуры РФ только в 2021 году было зарегистрировано 518 тысяч преступлений в сфере компьютерной информации, а ущерб от них составил 165 миллиардов рублей. А в 2022 году каждое четвертое преступление в России было связано с использованием информационных технологий.¹

Научная проблема отражается главным образом в квалификации преступлений в сфере компьютерной информации. Зачастую правоприменитель сталкивается трудностям, связанными с определением объекта преступного посягательства связанного с компьютерной информацией и соотношением его с другими статьями Уголовного Кодекса.

Проблеме преступлений в сфере компьютерной информации уделено значительное внимание. Данные вопросы рассматривались в работах Ю.М. Батурина, А.М. Жодзишского, А.В. Венгерова, В.Б. Вехова, В.С. Комиссарова В.В. Крылова, В.Д. Курушина, Ю.И. Ляпунова, В.Ю. Максимова, В.А.

¹Генеральная прокуратура Российской Федерации [официальный сайт]. - URL: <https://epp.genproc.gov.ru/web/gprf> (дата обращения: 30.04.2023).

Минаева, И.В. Никифорова, А.С. Попова, Н.А. Селиванова, А.С. Черных и других.

Объектом исследования являются общественные отношения, возникающие при совершении преступлений в сфере компьютерной информации.

Предметом исследования выступают уголовно-правовые нормы, устанавливающие ответственность за преступления в сфере компьютерной информации.

Цель исследования состоит в проведении всестороннего анализа уголовно-правовых норм, устанавливающих ответственность за совершение преступлений в сфере компьютерной информации, а также в разработке рекомендаций по внесению изменений в действующий Уголовный Кодекс РФ.

Задачи исследования:

- анализ истории возникновения и развития уголовной ответственности за совершение компьютерных преступлений в отечественном и зарубежном праве;
- исследование понятия и видов преступлений в сфере компьютерной информации;
- проведение уголовно-правового анализа преступлений, совершаемых в сфере компьютерной информации;
- изучение проблем квалификации преступлений в сфере компьютерной информации и определение путей их решения.

В работе будут использованы различные источники, включая законодательство Российской Федерации, научные и практические работы российских и зарубежных специалистов, а также статистические данные о преступлениях в сфере компьютерной информации.

Методологической основой исследования послужат общенаучные и частно-научные методы. Историко-правовой метод будет использован для изучения истории компьютерных преступлений и возникновения уголовной

ответственности за них. Формально-логический метод позволит провести детальный анализ уголовно-правовых мер по противодействию преступлениям в сфере компьютерной информации. Статистический метод включает сбор и анализ статистических данных о преступности в сфере компьютерной информации.

Теоретическую основу исследования составили работы ведущих отечественных и зарубежных ученых, относящиеся к исследуемой проблеме: Т.Г. Смирновой, В.В. Воробьева, Л.А. Бутлеровой, С.Г. Спириной, М.Ю. Дворецкого, С.Ю. Бытко, А.В. Доронина, В.С. Степанова-Егиянца, Т.М. Лопатиной, Д.В. Добровольского, Д.А. Ястребова и других авторов.

Нормативно-правовая база исследования включает в себя Конституцию Российской Федерации, Уголовный кодекс РФ 1996 г., действующее отраслевое законодательство, законы и подзаконные нормативно-правовые акты, международное законодательство по проблемам компьютерной преступности.

Теоретическая значимость исследования заключается в том, что в нем осуществлен анализ уголовно-правовых аспектов составов преступлений в сфере компьютерной информации, освещаются спорные вопросы по квалификации преступлений, вносятся предложения по совершенствованию действующего законодательства.

Практическая значимость исследования определяется возможностью использовать полученные результаты в практической деятельности судебно-следственных органов при решении вопросов в квалификации преступлений в сфере компьютерной информации; в деятельности по совершенствованию уголовно-правовых норм, устанавливающих ответственность за преступления в рассматриваемой сфере.

Данная работа состоит из введения, трех глав, заключения, и списка использованных источников.

1 Общая характеристика преступлений в сфере компьютерной информации

1.1 История возникновения и развития компьютерных преступлений: отечественный и зарубежный анализ

С самого начала человеческой цивилизации люди старались найти эффективные способы сохранения и передачи информации. В древние времена это были глиняные таблички и грубые пергаменты, которые не были достаточно надежными и удобными. Впоследствии появились печатные станки, а затем радио и телевидение, которые значительно облегчили жизнь людей и способствовали развитию других областей науки, производства, организации работы и систематизации общественной жизни, позволяя людям связываться друг с другом на больших расстояниях.

Наиболее значимым достижением в развитии информационных технологий на данный момент является глобальная сеть интернет, которая соединила вместе весь мир, открывая новые возможности для людей, имеющих доступ к современным устройствам.

Однако, несмотря на все преимущества, которые предоставили нам компьютерные технологии, их все более глубокое внедрение в повседневную жизнь привело к появлению новых видов преступлений, которые не были ранее известны законодательству и представляют теперь большую угрозу не только для отдельных лиц, но и для общественной безопасности в целом.

Перед тем как перейти к анализу компьютерной преступности, необходимо исследовать историю ее зарождения.

Первые шаги в создании электронно-вычислительных машин (ЭВМ) были предприняты еще в 20 и 30 годы прошлого века. Тогда основной целью с которой они создавались было проведение сложных арифметических расчетов и составление таблиц. Однако, настоящий бум в создании ЭВМ

произошел во время Второй мировой войны, когда государства начали создавать машины, способные расшифровывать коды и шифры вражеских сообщений. В США и Великобритании были созданы первые цифровые ЭВМ, а в СССР - первые аналоговые машины. Все они были огромными, медленными и сложными в использовании.

Первая программно-управляемая ЭВМ, названная «Манчестерский марк I», была создана в 1949 году в Великобритании. Она была быстрой, компактной и имела возможность программного управления, что стало ключевым моментом в развитии компьютеров.

С 1950-х годов создание ЭВМ стало предметом конкуренции между различными странами и компаниями. Были созданы такие ЭВМ, как IBM 701, UNIVAC I и Burroughs E101, которые были первыми коммерчески успешными компьютерами. В СССР в это время были созданы машины под названием «Урал», «Ереван» и «Минск».¹

В 1960-х годах Соединенные штаты достигли значительных успехов в создании компьютерной сети. Исследователи из Массачусетского технологического института (MIT) предложили теории передачи данных от одного компьютера к другому в 1962 году, а уже в 1965 году было установлено первое соединение между компьютерами из Массачусетса и Калифорнии, что создало первую локальную компьютерную сеть. На дальнейшее развитие компьютерной сети повлияло Управление перспективных исследовательских проектов Министерства обороны США (DARPA), которое начало активно заниматься исследованиями в этом направлении для военных нужд.

В 1980-х годах большая часть военной сети была превращена в общедоступный канал связи, который был открыт для гражданских лиц и

¹ Попов А.Н. Преступления в сфере компьютерной информации: учебное пособие. - СПб.: Санкт-Петербургский юридический институт Академии Генеральной прокуратуры РФ, 2018. - С. 56.

частных компаний. Это и привело к появлению всемирной компьютерной сети - интернета, с которой мы имеем дело сегодня.¹

Соединенные Штаты не только были первыми, кто создал компьютерную сеть, но и первыми, кто столкнулся с преступлениями, связанными с компьютерами.

В 1960-х годах термин «компьютерная преступность» впервые появился в американских СМИ, и самыми громкими случаями стали дело Альфонса Конфессоре, первого человека, осужденного в 1969 году за использование компьютера для совершения налогового мошенничества на сумму 620 тысяч долларов, а также дело о краже 10,2 миллионов долларов при помощи компьютерной техники из «Секьюрити Пасифик Бэнк».²

В 1979 году в Вильнюсе было зафиксировано первый случай компьютерной преступности в Советском Союзе. Работница почтовой связи была задержана за использование бреши в автоматизированной системе «Онега» в течение двух лет для кражи денежных средств из посылаемых пособий и пенсий гражданам. Общая сумма ущерба была оценена в 78 тысяч рублей.³

К сожалению, количество подобных преступлений с каждым годом только росло, и вместе с ним и размер наносимого ущерба.

Например, в 1988 году, молодой аспирант Корнельского университета - Роберт Моррис, от скуки в свободное время написал вредоносную компьютерную программу, позже известную как «Червь». Из личного интереса он отправил своего «Червя» в свободное плавание в локальную сеть Корнельского университета, даже не ожидая к каким результатам в конечном

¹ Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff Brief History of the Internet // Internet Society. - 1997. - URL: <https://www.internetsociety.org/internet/history-internet/brief-history-internet/> (дата обращения: 30.04.2023).

² Бессонов С.А. История и зарубежный опыт правовой регламентации компьютерной преступности // Теория науки. - 2013. - № 2. - С. 233.

³ Китайкина О.О. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации: история и современность // Научный формат. - 2020. - №7. - С. 122.

итоге приведет его маленькая шалость. Буквально за считанные дни «Червь» заразил всю локальную сеть, остановив работу почти всех компьютеров на территории института, а затем, оттуда он отправился и в глобальную сеть, выведя из строя более 6 тысяч компьютеров, что составляло на тот момент 10% от всех компьютерных устройств на планете. И по сей день данный инцидент остается одной из самых крупных кибератак в мировой истории, которая нанесла ущерба в общем итоге на 98 миллионов долларов США.

Но не смотря на весь причиненный урон, данный инцидент стал сильным толчком в развитии законодательства, касающегося компьютерной преступности и наглядно показал необходимость обеспечения безопасности компьютерного информационного пространства, и даже создания специальных групп реагирования на киберпреступления.¹

В 1991 году в нашей стране были сделаны первые шаги по созданию правовых норм, регулирующих область компьютерной безопасности. Это произошло после кражи с использованием ЭВМ 125,5 тысяч долларов из Внешэкономбанка СССР. Законодательству необходимо было реагировать на новую угрозу до того, как ущерб станет еще больше в будущем.

В связи с этим 23 сентября 1992 года были приняты важные законы: Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных»² и Закон РФ «О правовой охране топологий интегральных микросхем»³. Эти законы определили объекты правовой охраны и условия ее предоставления, установили определения для таких терминов, как «программы ЭВМ» и «базы данных». В сути своей, эти законы

¹ Morris Worm // FBI. - 2019. - URL: <https://www.fbi.gov/history/famous-cases/morris-worm> (дата обращения: 30.04.2023).

² О правовой охране программ для электронных вычислительных машин и баз данных: Федеральный закон от 23.09.1992 № 3523-1 (ред. от 18.12.2006) // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. - 1992. - № 42. - Ст. 2325. (утратил силу).

³ О правовой охране топологий интегральных микросхем: Федеральный закон от 23.09.1992 № 3526-1 (ред. от 02.02.2006) // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. - 1992. - № 42. - Ст. 2328. (утратил силу).

положили начало формированию законодательного аппарата в области компьютерной безопасности в России.

В это же время Верховный совет Российской Федерации принял постановление № 3524-1, которое регулировало процедуру введения в силу Закона Российской Федерации «О правовой охране программ для ЭВМ и баз данных». Это постановление внесло изменения в Уголовный и Гражданский кодексы Российской Федерации. Позднее также произошли изменения в других законах, связанных с правовой охраной компьютерных программ и баз данных.¹

Указ Президента РФ № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации», который был опубликован 3 апреля 1995 года, стал значимым событием в истории противодействия компьютерной преступности в России. Благодаря этому указу, вопросы, связанные с информатизацией и информационным сотрудничеством России со странами СНГ, а также организация мер по обеспечению защиты информации, стали решаться на уровне указов президента и актов правительства Российской Федерации.²

4 июля 1996 года был принят Федеральный закон № 85-ФЗ «Об участии в международном информационном обмене», который содержал определения таких понятий, как «массовая информация», «информационные ресурсы», «информационные продукты», «информационные услуги» и т.д. Этот закон был одним из важных документов, направленных на более эффективное

¹ О правовой охране программ для ЭВМ и баз данных: Федеральный закон от 23.09.1992 № 3524-1 (ред. от 18.12.2006) // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. - 1992. - № 42. - Ст. 2326. (утратил силу).

² О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации: Указ президента от 03.04.1995 № 334 (ред. от 25.07.2000) // Собрание законодательства Российской Федерации. - 1995. - № 15. - Ст. 1285.

участие России в обмене международной информацией в рамках единого международного пространства.¹

1 января 1997 г. вступил в силу новый Уголовный кодекс Российской Федерации, который за время претерпел значительные изменения, действующие до сих пор. Так, в нем появилась 28 глава, которая окончательно ввела и утвердила уголовную ответственность за такие преступления как; неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных программ; и за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Путем включения главы 28 в раздел IX Уголовного кодекса «Преступления против общественной безопасности и общественного порядка», законодательство РФ окончательно закрепило компьютерную преступность как опасное явление для общества, за которое необходимо нести уголовную ответственность.²

Позднее в 28 главу были внесены изменения, которые добавили статьи 274.1 и 274.2, устанавливающие уголовную ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Появление таких статей было обусловлено высокой степенью общественной опасности, связанной с возможным причинением вреда критической информационной инфраструктуре РФ и созданием угрозы ее безопасности.

7 июля 2003 года был принят Федеральный закон № 126-ФЗ «О связи» с целью определения полномочий органов государственной власти в области телекоммуникаций, установления принципов регулирования

¹ Об участии в международном информационном обмене: Федеральный закон от 04.07.1996 № 85-ФЗ (ред. от 27.07.2006) // Собрание законодательства Российской Федерации. - 1996. - № 28. - Ст. 3347. (утратил силу).

² Уголовный кодекс Российской Федерации от 13.06.1996 (ред. от 28.04.2023) // Собрание законодательства Российской Федерации. - 1996. - № 25. - Ст. 2954.

соответствующей деятельности и фиксации прав и обязанностей физических и юридических лиц, участвующих в этой сфере.¹

Несмотря на общий прогресс в развитии законодательства в области противодействия компьютерным преступлениям, к сожалению их количество только росло. Уже на конец 2009 года, правоохранительными органами регистрировалось более 11 тысяч преступлений.²

Это происходит по нескольким причинам:

- Во-первых, компьютерные преступления обладают высокой степенью латентности, что позволяет потенциальным преступникам чувствовать себя безнаказанными.

- Во-вторых, с расширением доступа к цифровым устройствам и интернету среди населения естественным образом увеличивается количество таких преступлений.

- В-третьих, компьютеризация предприятий и организаций создает возможности для сотрудников, осведомленных об уязвимостях компьютерных систем на рабочих местах, злоупотреблять ими в своих корыстных целях.

Следует отметить, что заметное повышение квалификации сотрудников подразделений, занимающихся борьбой с преступностью в сфере компьютерной информации, способствовало регистрации новых случаев преступлений в этой сфере и формированию объективной статистики.

Согласно отчету управления «К» МВД РФ, в 2012 году ущерб от компьютерных преступлений в России составил 2,3 миллиарда долларов, что почти в два раза больше, чем в 2010 году, когда ущерб оценивался в 1,3 миллиарда долларов. В этом же году, Алексей Мошков - тогдашний глава

¹ О связи: Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 18.00.2023) // Собрание законодательства Российской Федерации. - 2003. - № 28. - Ст. 2895.

² Никеров Д.М. Хохлова О.М. Преступления в сфере высоких технологий в современной России // Вестник Восточно-Сибирского института МВД России. - 2019. - №2. - С. 212.

управления «К», отмечал что наиболее распространенными преступлениями в сфере компьютерной преступности являются мошенничества и кражи со счетов граждан и юридических лиц.¹

Исходя из вышесказанного, можно с уверенностью заключить, что компьютерная преступность представляет серьезную угрозу, требующую незамедлительных мер и эффективных стратегий противодействия. Однако разработка таких мер и стратегий без учета международного опыта может быть затруднительной.

Другие страны могли сталкиваться с преступлениями, которые до сих пор могут быть незнакомы отечественному законодателю, и в целом они обладают обширным опытом в борьбе с этой формой преступности, благодаря более раннему внедрению компьютерных технологий в различные сферы своей жизни.

В 1970 году, в штате Гессен, Германия, был принят первый закон о защите персональных данных, который регулировал обработку электронных данных, связанных с налоговым сбором, жилищно-коммунальным хозяйством и другими муниципальными услугами. Однако этот закон применялся только на территории штата Гессен и не распространялся на другие регионы Федеративной Республики Германия.

А первой страной, которая национально ввела законодательную ответственность за компьютерные преступления, стала Швеция. 2 апреля 1973 года был издан закон о данных (Data Act), в котором устанавливалась ответственность за такие преступления, как незаконное проникновение в компьютерные системы и введение ложных данных в базы данных с целью

¹ МВД Российской Федерации [официальный сайт]. - URL: <http://www.mvd.ru> (дата обращения: 30.04.2023).

хищения денежных средств, ценных бумаг, имущества и конфиденциальной информации.¹

В 1977 году правительство США выразило беспокойство по поводу компьютерных преступлений, так как на тот момент они преследовались в соответствии с законом «О мошенничестве с использованием почты и телеграмм». Это создавало проблемы в квалификации таких преступлений, и многие из них могли остаться безнаказанными и не раскрытыми. В связи с этим, в 1977 году законодательная власть США приняла федеральный закон, который устанавливал уголовную ответственность за компьютерные преступления. В 1984 году этот закон претерпел значительные изменения и получил новое название - «О компьютерном мошенничестве и злоупотреблениях» (Computer Fraud and Abuse Act). В последующие годы, с 1989 по 2008 год, этот закон был подвергнут множеству поправок, чтобы отразить изменяющиеся условия борьбы с компьютерной преступностью.²

В настоящее время конгресс США рассматривает возможность ужесточения наказания за преступления, совершенные в области компьютерной информации. Например, предлагается увеличение срока лишения свободы до 20 лет за «экономический шпионаж» и до 30 лет за взлом инфраструктуры общественного значения.

Существовавшее на момент 1990 года законодательство Соединенного королевства не позволяло эффективно реагировать и противодействовать на преступления в сфере компьютерной информации, что послужило принятию Парламентом таких законов как «О неправомерном использовании компьютеров» (Computer Misuse Act) и «О злоупотреблении компьютером». Последний, выделял и конкретизировал виды преступлений связанных с

¹ Жиделев В.Г. Эволюция законодательства об уголовной ответственности за совершение преступлений в сфере высоких технологий // Вестник Удмуртского университета. Серия «Экономика и право». - 2011. - №4. - С. 115.

² 9-48.000 - Computer fraud and abuse act // The U.S Department of justice. - URL: <https://www.justice.gov/jm/jm-9-48000-computer-fraud> (дата обращения: 30.04.2023).

неправомерным использованием компьютерных технологий, с которыми необходимо было бороться.¹

Если говорить о странах СНГ, то многие из них имеют уголовное законодательство схожее с российским, обладая почти идентичным перечнем деяний, которые признаются компьютерными преступлениями, хотя и имеются некоторые отличия.

Например, в уголовном кодексе Казахстана, в главе 7 «Уголовные правонарушения в сфере информатизации и связи», содержатся дополнительные статьи, которые устанавливают наказания за более широкий спектр компьютерных преступлений. Там указаны такие преступления как неправомерное распространение компьютерной информации, компьютерный саботаж, принуждение к передаче информации и другие, которые не предусмотрены в Уголовном кодексе Российской Федерации.²

В разных странах компьютерные преступления, как правило, рассматриваются в уголовном законодательстве как отдельная категория преступлений или в качестве квалифицирующих признаков, которые дополняют составы уже существующих преступлений. В Италии используется последний подход.³ Этот подход, который будет обсуждаться в третьей главе, мог бы стать хорошим дополнением и к уголовному кодексу России.

Из вышеизложенного можно сделать вывод, что преступность в сфере компьютерной информации является одним из самых специфических, сложных и динамичных видов преступлений. Сегодня она представляет собой серьезную угрозу как для отдельных государств, так и для международного сообщества в целом. Ущерб от компьютерной преступности огромен и

¹ Карамнов А.Ю., Дворецкий М. Ю. Законодательство Великобритании о преступлениях в сфере компьютерной информации // Социально-экономические явления и процессы. - 2013. - №8. - С. 164.

² Уголовный кодекс Республики Казахстан от 16.07.1997 (ред. от 20.05.2023) // Ведомости Парламента Республики Казахстан. - 1997. - № 15-16. - Ст. 211.

³ Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. - М.: Юрлитинформ, 2002. - С. 269.

исчисляется миллиардами долларов. Для эффективной борьбы с с ней необходимо совершенствовать законодательство, регулирующее уголовную ответственность за за подобного рода преступления. Крайне важно использовать положительный опыт многих зарубежных стран и обновить действующее российское законодательство в этой области, в том числе Уголовный кодекс.

1.2 Понятие и виды преступлений в сфере компьютерной информации

В современном информационном обществе одной из наиболее актуальных проблем является компьютерная преступность. Появление компьютеров и развитие информационных технологий привели к тому, что информация стала ценным ресурсом, который может быть использован не только в легальных целях, но и для совершения преступлений. Поэтому понимание того, что из себя представляет преступность в сфере компьютерной информации и определение ее видов является крайне важным для правоохранительных органов, а что самое главное - для законодателя.

Вопрос определения преступности в сфере компьютерной информации является дискуссионным в среде исследователей уголовно-правовых норм. Каждый из авторов дает свое определение преступлений в сфере компьютерной информации и на данный день нет единой трактовки и когда кто-то из ученых выдвигает свою, то в основном он ориентируется на главу 28 УК РФ «Преступления в сфере компьютерной информации».

Что же все таки принято понимать под преступностью в сфере компьютерной информации и какие ее виды выделяет Российский законодатель? В этом параграфе мы постараемся ответить на данный вопрос. Также, в контексте данного вопроса мы немного затронем такие термины как

«Компьютерные преступления» и «Киберпреступность», чтобы убрать всю путаницу в дальнейшем повествовании, и отграничить их от понятия преступности в сфере компьютерной информации.

Что такое преступность в сфере компьютерной информации? Приведем в качестве примера мнения некоторых исследователей по данному вопросу.

Так, согласно М. А. Зубовой, преступность в сфере компьютерной информации может быть определена как виновно совершенные общественно опасные действия, нарушающие нормальный порядок обращения компьютерной информации, что запрещено Уголовным кодексом РФ и подлежит уголовному наказанию.¹

В. Л. Кудрявцев подчеркивает, что преступления в сфере компьютерной информации, предусмотренные главой 28 раздела IX Уголовного кодекса РФ, направлены на нарушение информационной безопасности и они затрагивают компьютерную информацию в форме электрических сигналов, независимо от способа ее хранения, обработки и передачи. Он рассматривает эти преступления как общественно опасные деяния, которые посягают на сведения (сообщения, данные), представленные в форме электрических сигналов.²

В соответствии с взглядами В. И. Алескерова, преступления в сфере компьютерной информации являются посягательствами на безопасность компьютерной информации, которые вызывают или создают угрозу значительного вреда личности, обществу и государству в связи с использованием соответствующей информации. Он отмечает, что эти

¹ Зубова М.А. Компьютерная информация как объект уголовно-правовой охраны: специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: автореф. дис. на к.ю.н. - Казань, 2008. – С. 119.

² Кудрявцев В. Л. Преступления в сфере компьютерной информации: общая характеристика // «Уголовное законодательство в XXI веке: современное состояние, проблемы трактовки и применения его положений с учетом задач дальнейшего укрепления экономического правопорядка»: материалы международной научно-практической конференции, Нижний Новгород, 1 марта 2012 г. - Нижний Новгород: НИУ ВШЭ. - 2012. - С. 72.

действия охватываются нормами статей 272-274 главы 28 раздела 9 Уголовного кодекса Российской Федерации.¹

В «Соглашении о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации», которое Российская Федерация ратифицировала на своей территории, преступление в сфере компьютерной информации определяется как уголовно наказуемое деяние, посягающее на компьютерную информацию.²

Основные же виды преступности в сфере компьютерной информации названы и закреплены главе 28 УК РФ.

- Неправомерный доступ к компьютерной информации – статья 272 УК РФ. Включает незаконный доступ к охраняемой законом компьютерной информации, хранящейся в компьютерных системах и сетях. Нарушения могут включать уничтожение, блокирование, модификацию или копирование информации, а также нарушение работы компьютерных систем.

- Создание, использование и распространение вредоносных программ для ЭВМ – статья 273 УК РФ. Охватывает действия, которые включают создание программ, преднамеренно приводящих к несанкционированному уничтожению, блокированию, модификации или копированию информации, а также нарушению работы компьютерных систем. Это также может включать внесение изменений в существующие программы и использование или распространение вредоносных программ или машинных носителей.

- Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети – статья 274 УК РФ. Включает нарушения правил эксплуатации компьютерных

¹ Алескеров В. И. О преступлениях, совершаемых в сфере телекоммуникаций и компьютерной информации / В. И. Алескеров // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений: сборник научных трудов. - Воронеж: Воронежский институт МВД России, 2018. – № 1. – С. 5.

² Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Собрание законодательства Российской Федерации. - 2001. - № 26. - Ст. 2674.

систем и сетей, приводящие к уничтожению, блокированию или модификации охраняемой законом информации. Это преступление требует причинения или создания угрозы причинения существенного вреда.

Эти группа преступлений относятся к институту Особенной части уголовного законодательства. Объектом данных преступлений являются общественные отношения, связанные с обеспечением безопасности информации и систем обработки информации с помощью ЭВМ.

В указанных выше видах преступлений ясно определяется их общий предмет - компьютерная информация. Компьютерная информация определяется в комментариях к статье 272 УК РФ как сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от способов их хранения, обработки и передачи.

Таким образом, преступность в сфере компьютерной информации охватывает уголовно наказуемые действия, которые нарушают нормальный порядок обращения компьютерной информации, причиняют ущерб информационной безопасности и создают угрозу существенного вреда личности, обществу и государству. Эти действия регулируются соответствующими статьями 28 главы Уголовного кодекса РФ и являются объектом уголовного преследования.¹

Следует отметить, что в 2012 году в Уголовный кодекс РФ были введены новые статьи, касающиеся уголовной ответственности за различные формы кибермошенничества (статьи 159.3 и 159.6 УК РФ), которые формально не входят в главу 28 Уголовного кодекса, хотя тесно с ней соприкасаются.

В области уголовно-правовой науки существует смежное понятие информационного преступления, которое относится к нарушениям информационной безопасности. В этом контексте следует обратить внимание на классификацию преступлений против информационной безопасности,

¹ Полежаев А.П. Компьютерные технологии в правоохранительной сфере: сборник научных трудов. - М.: Академия МВД РФ, 1993. - С. 81.

представленную в главе 30 Модельного Уголовного кодекса стран Содружества Независимых Государств (СНГ).

Эта классификация включает шесть составов преступлений, из которых три состава совпадают с преступлениями, предусмотренными главой 28 Уголовного кодекса Российской Федерации: незаконный доступ к компьютерной информации (аналог статьи 272 УК РФ), разработка, использование и распространение вредоносных программ (аналог статьи 273 УК РФ) и нарушение правил эксплуатации компьютерной системы или сети (аналог статьи 274 УК РФ).

Однако, Модельный Уголовный кодекс стран СНГ также содержит три состава преступлений, которые не присутствуют в действующем Уголовном кодексе Российской Федерации: компьютерный саботаж (статья 288), незаконное завладение компьютерной информацией (статья 289) и производство и сбыт специальных средств для получения незаконного доступа к компьютерной системе или сети (статья 290).¹

Конструкции «преступления в сфере компьютерной информации» и «компьютерные преступления» имеют различные подходы и соотносятся между собой в разных правовых системах. В уголовно-правовой практике некоторых зарубежных государств, таких как Франция, США и Великобритания, понятие «компьютерные преступления» охватывает широкий спектр правонарушений, где компьютер может выступать как объектом, так и средством совершения преступлений. Например, кража компьютера или распространение незаконных материалов через компьютерные сети могут быть квалифицированы как компьютерные преступления.

¹ Модельный уголовный кодекс - участников Содружества Независимых Государств: Принят Постановлением Межпарламентской Ассамблеи государств - участников Содружества Независимых Государств 17.02.1996 (ред. от 16.11.2006) // Информационный бюллетень Межпарламентской ассамблеи государств. - 1997. - № 10.

В отличие от этого, в странах постсоветского пространства, включая Россию, Польшу, Болгарию и другие, уголовное законодательство склонно признавать компьютерную информацию объектом или орудием преступления, а не сам компьютер как материальный объект. Таким образом, в указанных случаях квалификация преступлений будет зависеть от сферы правонарушения: кража компьютера будет рассматриваться как преступление против собственности, а распространение незаконной порнографии с использованием компьютерных сетей будет рассматриваться как преступление против общественной нравственности.¹

В уголовно-правовой науке России отсутствует четкое определение понятия «компьютерные преступления».

Выделяют различные подходы к определению этого понятия.

Один из подходов связывает компьютерные преступления с преступлениями в сфере компьютерной информации, считая их одним и тем же. Другая группа ученых шире определяет компьютерные преступления, включая в них не только действия, направленные на компьютерную информацию, но и использование компьютерной информации в качестве инструмента для совершения преступлений.

При использовании компьютерной информации в качестве инструмента для совершения преступлений, сама информация становится объектом общественно опасного деяния. Однако, в Российском Уголовном кодексе отсутствует отдельный квалифицирующий признак, указывающий на совершение преступления с использованием компьютерной информации. Вместо этого, компьютерная информация может рассматриваться в контексте совокупности преступлений, которые совершаются при ее использовании.

Важно отметить, что для противоправного использования компьютерной информации необходимо нарушение ее правовой защиты, что

¹ Китайкина О.О. О соотношении понятий «компьютерные преступления» и «преступления в сфере компьютерной информации» // Научный формат. - 2020. - №6. - С. 229.

может включать такие действия, как уничтожение, модификация, копирование, блокирование, предоставление и распространение информации, как указано в Федеральном законе «Об информации, информационных технологиях и о защите информации».¹

Третий же подход утверждает, что компьютерные преступления имеют условный характер. Некоторые авторы, например, Ю. М. Батурин, считают, что в юридическом смысле компьютерные преступления не являются отдельной группой преступлений, и можно говорить только о компьютерных аспектах преступлений, не выделяя их в отдельную категорию.

По мнению Н. А. Селиванова, в России термин «компьютерные преступления» должен использоваться как условное наименование для преступлений, перечисленных в главе 28 Уголовного кодекса РФ, а также для тех, которые являются логическим продолжением других преступлений и совершаются с использованием компьютерной техники. На сегодняшний день эта позиция считается наиболее правильной.

Что касается понятия «киберпреступления», в современной юридической литературе под ним понимаются различные виды преступлений, связанных с компьютерной информацией, информационными технологиями, высокими компьютерными технологиями и информационным пространством. Многие ученые и исследователи предпринимают попытки определить это понятие.

Согласно В. А. Номоконову и Т. Л. Тропиной, киберпреступление является более широким понятием, чем компьютерная преступность, и точно отражает преступность в информационном пространстве. В Конвенции о киберпреступности под киберпреступлениями понимаются действия, направленные против конфиденциальности, целостности и доступности

¹ Семкин, С.Н. Основы правового обеспечения защиты информации: учебное пособие для студентов высших учебных заведений. - М.: Горячая линия - Телеком, 2007. - С. 192.

компьютерных систем, сетей и данных, а также злоупотребления такими системами, сетями и данными.

Подводя итог, можно сказать, что термин «преступления в сфере компьютерной информации» имеет законодательное закрепление и корректно использовать его, имея в виду главу 28 Уголовного кодекса Российской Федерации. Термин «компьютерные преступления» имеет доктринальный характер, поскольку Уголовный кодекс РФ не содержит специфического квалифицирующего признака для преступлений, совершенных с использованием компьютерной информации, техники, информационно-вычислительных систем и средств телекоммуникаций. Поэтому условно мы можем относить к «компьютерным преступлениям» любое преступление, совершенное при помощи компьютера. Термин «киберпреступления» имеет международный характер и фактически объединяет все преступления, которые осуществляются в виртуальном пространстве с использованием компьютерных систем или сетей.

2 Уголовно-правовой анализ преступлений, совершаемых в сфере компьютерной информации

2.1 Неправомерный доступ к компьютерной информации (ст. 272 УК РФ)

Положение настоящей статьи 272 УК РФ, которая называется «Неправомерный доступ к компьютерной информации» говорит о том, что получение несанкционированного доступа к компьютерной информации является незаконным и влечет за собой уголовно-правовую ответственность если оно повлекло за собой уничтожение, блокирование, модифицирование или копирование компьютерной информации.

Федеральным законом «Об информации, информационных технологиях и о защите информации» определено, что информация представляет собой сведения независимо от их формы.¹

Согласно определению термина «Компьютерная информация», сформулированному в приложении 1 статьи 272 УК РФ, компьютерная информация означает данные, сообщения или сведения, которые представлены в виде электрических сигналов, независимо от того, как они хранятся, обрабатываются и передаются. Оно было введено Федеральным законом № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 7 декабря 2011 года, который в целом внес множество изменений в данную статью, действующих и в наше время. Они будут затронуты ниже.

Под «неправомерным» понимается получение доступа к компьютерным данным или информации, хранящимся в электронном виде, без согласия собственника или иного законного владельца такой информации. Также к

¹ Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 3524-1 (ред. от 29.12.2022) // Собрание законодательства Российской Федерации. - 2006. - № 31. - Ст. 3448.

незаконному доступу относится получение доступа с использованием специальных программ или устройств, созданных для этой цели.

Сама статья 272 является одной из 5 основных статей 28 главы уголовного кодекса, регулирующих сферу компьютерной информации в Российской Федерации. Она направлена на предотвращение незаконного доступа к компьютерной информации и защиту прав ее владельцев, что имеет важное значение для обеспечения не только информационной безопасности, но и защиты основополагающих конституционных прав граждан.

Так статья 23 конституции Российской Федерации, гарантирует неприкосновенность частной жизни и сохранение тайны переписок, которая может быть нарушена получением неправомерного доступа к личным данным граждан.¹

Стоит заметить, что статья 272 УК РФ также плотно пересекается со сферой авторского права, а в частности с главой 70 части 4 ГК РФ. Например, статья 1225 «Охраняемые результаты интеллектуальной деятельности и средства индивидуализации» устанавливает, что результатом интеллектуальной деятельности может являться и компьютерная информация, такая как программы ЭВМ, базы данных и др. А согласно статье 1261 ГК - программы ЭВМ во всех формах защищаются как и произведения литературы, являясь такими же объектами защиты авторского права.²

Предметом преступного посягательства выступает компьютерная информация, которая защищена законом, включая личные и служебные данные, хранящиеся на компьютерах или их сетях.

Объектом является нарушение общественных отношений в области сохранения и конфиденциальности компьютерной информации.

¹ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Собрание законодательства РФ. - 2009. - № 4. - Ст. 445.

² Гражданский кодекс Российской Федерации от 13.11.1994 (ред. от 14.04.2023) // Собрание законодательства Российской Федерации. - 1994. - № 32. - Ст. 3301.

Объективная сторона преступления заключается в получении неправомерного доступа к защищенной законом компьютерной информации. Хотя законодатель не определяет явно, что считать «охраняемой законом информацией», любая информация, которая имеет специальный статус, например, персональные данные граждан или государственная или коммерческая тайна, могут рассматриваться как таковые.

Обязательными признаками объективной стороны являются совершение общественно опасного действия и возможные последствия, которые могут произойти в результате этого действия.

Субъектом преступления может стать любое дееспособное физическое лицо, достигшее 16-летнего возраста. 3 часть статьи выделяет еще и специальный субъект - должностное лицо, пользующееся своим служебным положением.

Субъективная сторона преступления заключается в умысле (прямом или косвенном) совершения действия. Это означает, что лицо, совершающее преступление, знает, что его действия запрещены и нацелены на получение неправомерного доступа к компьютерной информации.

Состав этого преступления является материальным, так как первая часть статьи предусматривает ответственность за возможные негативные последствия, такие как уничтожение, модификация, блокирование или копирование информации.

В уголовном праве уничтожение информации означает потерю информации, которую невозможно восстановить. Блокирование информации означает, что информацию нельзя использовать, но при этом она сохраняется. Модификация информации означает изменение ее содержания по сравнению с оригинальной информацией, находившейся в распоряжении законного пользователя или собственника. Копирование информации - это процесс переписывания или создания дополнительных копий с сохранением оригинала.

Что касается истории появления. Статья 272 УК РФ «Неправомерный доступ к компьютерной информации» впервые появилась в новом уголовном кодексе, вступившем в силу 1 января 1997 года и действует до сих пор, на момент 2023 года.

Первоначально статья включала в себя только первые две части, которые сильно отличались от нынешних, указывая в качестве компьютерной информации только ту, которая находилась на машинном носителе ЭВМ.

В первой части запрещался незаконный доступ к компьютерной информации с использованием технических средств, который повлек за собой какое-либо изменение данных, приведшее к негативным последствиям. Санкция данной части за годы претерпела малое количество изменений, оставшись почти в подлинном виде и в наше время. В дальнейших редакциях были только добавлены ограничение свободы до двух лет и принудительные работы на такой же срок, а также изменены размеры и сроки выплат штрафов.

Вторая часть же устанавливала наказание за то же деяние, но совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения. Данная часть претерпела за годы наибольшее количество правок и редактирований, полностью изменившись к нынешнему времени.

Самые кардинальные изменения в статью 272 УК были внесены Федеральным законом от 7 декабря 2011 г. N 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», упомянутым выше.

Начнем с того, что до внесения изменений в статью 272 УК РФ, которые были приняты 7 декабря 2011 года, первая часть этой статьи была сформулирована следующим образом: «Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию

либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети». Сейчас же эта часть статьи звучит так: «Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации».

Первоначально, может показаться, что изменения не существенны, так как больше нет указания ЭВМ в качестве основного места хранения компьютерной информации, но новая формулировка решила ряд проблем, которые возникали при применении данной статьи на практике. Из-за предыдущей диспозиции правоприменителю было затруднительно определять перечень устройств, которые подпадали под определение ЭВМ. Например, к таким не относились мобильные телефоны, смартфоны и карманные персональные компьютеры, хотя они также могли обрабатывать и хранить компьютерную информацию, охраняемую законодательством. Нынешняя же диспозиция первой части убрала конкретизацию перечня устройств, установив в качестве основного объекта правовой охраны саму компьютерную информацию как таковую, что позволило эффективнее ее защищать, независимо от места хранения.

Посягательства, совершаемые группой лиц по предварительному сговору или организованной группой, а также лицом, использующим свое служебное положение, были перенесены из части 2 в часть 3 статьи 272 Уголовного кодекса Российской Федерации и получили статус особо отягчающего обстоятельства в рамках уголовно-правовой ответственности.

На место 2 части были внесены новые квалифицирующие признаки, такие как: причинение крупного ущерба или совершенное из корыстной заинтересованности.

Данная статья претерпела изменения, касающиеся примечаний.

Из части первой было убрано определение «компьютерной информации» и введено в примечание 1 к статье, где оно было

переформулировано следующим образом: «Сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

Добавлялось примечание 2 которое уточнило то, что понималось под крупным ущербом из части 2, определяя его как ущерб, нанесенный на сумму более 1 миллиона рублей.¹

Заметно как статья 272 менялась, чтобы вовремя реагировать на стремительно меняющиеся виды и условия совершения компьютерных преступлений и эффективно им противостоять. Особенно это заметно на примере новой 2 части, которая включает корыстный умысел как один из квалифицирующих признаков, так как с каждым днем растет количество людей, осваивающих владение компьютерными технологиями на высоком уровне, а вместе с ними и тех, кто готов использовать свои навыки в корыстных и преступных целях.

Согласно предоставленной статистике от сайта Агентства правовой информации, в период с 2018 по 2022 годы наибольшее количество раскрытых преступлений по статье 272 было совершено по третьей части, когда деяния, предусмотренные первой или второй частью статьи, были совершены группой лиц по предварительному сговору, организованной группой или лицом, использующим свое служебное положение.

Из 531 осужденных по данной статье за пять лет, 408 приходится только на третью часть, что составляет 76% от общего числа.²

Существует несколько возможных причин, почему третья часть статьи 272 УК РФ, связанная с преступлениями, совершаемыми группой лиц по предварительному сговору или организованной группой, а также лицами,

¹ Дворецкий М. Ю. Корреляции главы 28 УК РФ в контексте оптимизации уголовной ответственности и повышения эффективности правоприменительной практики // Вестник ТГУ. - 2012. - №6. - С. 267.

² Сайт Агентства правовой информации. - URL: <https://stat.xn----7sbqk8achja.xn--p1ai/> (дата обращения: 03.05.2023).

использующими свое служебное положение, может иметь наибольшее количество раскрытых дел:

- Уровень организованной преступности: Дела, связанные с организованной преступностью, обычно требуют серьезных расследований и силовых операций со стороны правоохранительных органов. Организованные преступные группировки могут специализироваться в области компьютерных преступлений и иметь развитую структуру, что делает их деятельность более заметной и вызывающей пристальное внимание правоохранительных органов.

- Технические возможности: Современные технологии и распространение компьютеров и интернета предоставляют все больше возможностей для совершения преступлений в сфере компьютерной информации. Группы преступников могут использовать сложные технические методы, чтобы получить неправомерный доступ к компьютерной информации и использовать ее в своих интересах.

- Мотивация и выгода: Возможность получить доступ к чужой компьютерной информации или использовать свое служебное положение для совершения преступления может представлять значительную мотивацию для преступников. Это может быть связано с финансовой выгодой, конкурентными преимуществами или осуществлением незаконных действий в интересах определенных групп или организаций.

- Улучшение правоохранительной работы: Раскрытие большего количества дел по третьей части статьи 272 может также указывать на улучшение работы правоохранительных органов в области выявления и пресечения компьютерных преступлений. Усиление сотрудничества с различными специалистами, внедрение новых методов расследования и повышение осведомленности о компьютерных преступлениях могут способствовать увеличению числа раскрытых дел.

В целом, сочетание этих факторов может быть причиной большого количества раскрытых дел по третьей части статьи 272 УК РФ, чем по другим частям этой статьи.

В качестве примера можно рассмотреть приговор, вынесенный Железнодорожным районным судом г. Хабаровска по части 3 статьи 272 УК РФ (Неправомерный доступ к компьютерной информации) под номером 1-127/2017. Суд установил, что Чуйков Сергей Владимирович, занимая должность оператора колл-центра в филиале № ПАО ВТБ 24, сознательно и с корыстными побуждениями планировал воспользоваться автоматизированной банковской системой «ИРБИС» для изменения данных клиента ФИО1 с целью хищения с его счета денежной суммы в размере 9 миллионов рублей.

Чуйков С.В., в качестве главного специалиста-кассира согласно должностной инструкции, осознавая общественную опасность и незаконный характер своих действий, предвидел неизбежность возникновения общественно опасных последствий, таких как причинение имущественного ущерба, и желал их наступления. Без ведома и присутствия владельца вклада (ФИО1) и с использованием логина и пароля сотрудника (ФИО10), Чуйков С.В. незаконно получил доступ к системе и произвел неправомерные изменения данных клиента ФИО1. В результате этих действий данные клиента были изменены на фиктивные данные клиента ФИО2 и связаны с банковской картой, открытой на имя несуществующего клиента ФИО2. Затем с именного счета клиента ФИО1 были сняты денежные средства в размере 9 миллионов рублей. Чуйков С.В., с целью замаскировать преступление, восстановил прежние данные клиента ФИО1 и отвязал их от счета, открытого на имя ФИО2.

Чуйков Сергей Владимирович был признан виновным в совершении преступления, предусмотренного частью 3 статьи 272 Уголовного кодекса

Российской Федерации. Судом ему было назначено наказание в виде 10 месяцев лишения свободы.

Исходя из статьи 69 часть 5 Уголовного кодекса РФ, учитывая совокупность преступлений путем частичного сложения с наказанием, уже назначенным приговором Железнодорожного районного суда г. Хабаровска, окончательно было принято решение о назначении Чуйкову Сергею Владимировичу 4 лет и 4 месяца лишения свободы с отбыванием наказания в исправительной колонии общего режима.¹

Этот пример наглядно подчеркивает значимость служебного положения в совершении преступления и обращает внимание на проблему внутренней угрозы безопасности данных, когда сотрудники злоупотребляют своими привилегиями и доступом. Также он позволяет проанализировать мотивацию преступника (корыстная заинтересованность) и последствия его действий (хищение денежных средств).

Изучение этого примера может помочь в разработке и внедрении мер безопасности, которые могут предотвратить подобные преступления в будущем. Анализ случаев реальных преступлений позволяет выявить уязвимые места и разработать меры предосторожности для защиты компьютерной информации.

К таким мерам может относиться:

- Обновление политики безопасности: Организации должны пересмотреть и усовершенствовать свою политику безопасности информации, включая правила доступа, аутентификации, защиты паролей и контроля доступа к конфиденциальным данным. Регулярное обновление политики и ее актуализация с учетом изменений в угрозах и технологиях является критическим шагом.

¹ Приговор Железнодорожного районного суда г. Хабаровска от 21.02.2017 по делу № 1-127/2017. - URL: <https://advocate-service.ru/sud-praktika/ugolovnyye-dela/prigovory-sudov-po-st.-272-uk-rf-nepravomernyj-dostup-k-kompjuternoj-informatsii/prigovor-suda-po-ch.-3-st.-272-uk-rf--1-1272017--nepravomernyj-dostup-k-kompjuternoj-informatsii.html> (дата обращения: 03.05.2023).

- Многоуровневая аутентификация: Реализация многофакторной аутентификации (МФА) для доступа к компьютерным системам может значительно повысить безопасность. Это может включать комбинацию пароля, физического устройства (например, токена доступа или смарт-карты) или биометрических данных.

- Системы мониторинга и обнаружения инцидентов: Внедрение систем мониторинга и обнаружения инцидентов позволяет раннее обнаружение подозрительной активности и несанкционированного доступа к компьютерной информации. Это может включать мониторинг журналов событий, сетевой трафик и поведение пользователей.

- Ограничение привилегий доступа: Ограничение привилегий доступа сотрудников на основе их роли и необходимости помогает уменьшить риск злоупотребления и несанкционированного доступа. Принцип наименьших привилегий следует применять при назначении прав доступа.

- Регулярные аудиты безопасности: Проведение регулярных аудитов безопасности поможет выявить уязвимости в информационных системах и принять соответствующие меры по их исправлению. Это включает проверку наличия обновлений программного обеспечения, устранение уязвимостей и оценку соответствия политикам безопасности.

- Сотрудничество с правоохранительными органами: Организации могут установить партнерство с правоохранительными органами для обмена информацией о новых угрозах, сотрудничества в расследовании инцидентов и участия в совместных тренировках и учениях.

- Разработка культуры безопасности: Организации должны развивать культуру безопасности среди своих сотрудников, где безопасность информации становится приоритетом для всех. Это может быть достигнуто через обучение, поощрение соответствующего поведения и осведомленность о последствиях нарушений безопасности.

- Внедрение системы отчетности и реагирования на инциденты: Организации должны иметь механизмы для отчетности о подозрительной активности и реагирования на инциденты безопасности. Это включает создание команды по реагированию на инциденты и установление процедур для своевременного обнаружения, анализа и реагирования на нарушения безопасности.

2.2 Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)

Перед тем, как начать разбирать статью 273, стоит определить что такое «вредоносная компьютерная программа» и чем она отличается от иных программ, чтобы правильно оценить опасность данного преступления.

Компьютерная программа - это набор команд, инструкций и правил, написанных на определенном языке программирования, который определяет последовательность выполнения операций, необходимых для решения определенной задачи. Компьютерная программа может быть представлена в виде исходного кода, который после компиляции преобразуется в исполняемый файл, который может быть запущен на компьютере или другом устройстве. Компьютерные программы используются для автоматизации процессов, управления устройствами и системами, анализа данных и многих других задач.

В статье 273 УК РФ термин «компьютерная программа» трактуется как исполняемый код, который позволяет аппаратной части ЭВМ выполнять вычисления или функции управления.

ЭВМ не способна самостоятельно определять какая программа является вредоносной, а какая полезной и поэтому может выполнять заданные ей команды даже во вред собственной системы.

Вредоносность же таких программ определяется только намерениями, которые перед собой ставил ее создатель, когда писал исходный код. За годы борьбы с компьютерной преступностью, было выделено множество целей, с которыми создаются подобные программы, начиная от мелкого вредительства и заканчивая совершением настоящего кибертерроризма.

В научной же литературе в основном определяют вредоносную программу как набор написанных злоумышленником на определенном языке программирования набора машинного кода и инструкций для ЭВМ, выполнение которых приведет несанкционированному уничтожению, блокированию, повреждению, копированию, модификации информации пользователя, нарушению стабильной работы ЭВМ и сетей передачи данных.

Одной из характерных черт многих вредоносных программ выделяют копирование самой себя и распространение через иные ресурсы или носители информации с целью поражения большего количества ЭВМ. Именно такие вредоносные программы получили в народе название «Компьютерных вирусов», распространяясь словно инфекция и заражая огромное количество устройств.

Компьютерные вирусы являются одним из наиболее распространенных способов потери информации.

Вредоносный код может быть скрыт в уже существующем программном обеспечении, не нарушая его нормального функционирования, и проявлять свою активность только при определенных условиях.

Например, логическая бомба может начать работу только при подключении конкретного компьютера к сети, а временная бомба может активироваться только в определенный период времени.

Также есть вредоносные программы, которые вставляют команды в обычную программу, чтобы создавать и уничтожать другие команды, что затрудняет их обнаружение. Эти команды могут создавать другие команды, создавая вредоносную программу в стиле «троянского коня».

Вредоносная программа может быть распространена как активным способом, когда она внедряется в компьютер, систему или сеть с помощью различных методов, позволяющих получить свободный доступ к ней. Также она может быть распространена пассивным способом, когда не вмешиваются в ее самораспространение или когда она передается третьим лицам в любой форме на машинном носителе.

Основная цель таких действий заключается в нарушении неприкосновенности и стабильности компьютерной информации и ее материального носителя - ЭВМ.

Также одной из особенностей вредоносных программ является их несанкционированная деятельность, скрытая от пользователя устройства. До этого, говорилось, что вредоносность программы определяется намерениями ее создателя, но и многие из легальных программ способны совершать действия, что и вредоносные. Главным отличием таких программ является то, что модификацию, уничтожение и прочее изменение информации на устройстве они совершают с уведомления ими позволения. В противном же случае, такие программы также будут считаться вредоносными.¹

Интересной странностью данного преступления является то, что немалое число создателей вредоносных программ пишут их не из корыстных или преступных мотивов, а из личного интереса и желания бросить вызов современным системам компьютерной безопасности, а заодно проверить свои силы. Зачастую, таким промышляют молодые (до 30 лет) специалисты в сфере компьютерной информации, или и вовсе подростки, возрастом до 20 лет, освоившие один из языков программирования и обладающие достаточным уровнем знаний в области компьютерных технологий.²

¹ Энгельгардт А.А. Уголовно-правовая оценка создания, использования и распространения вредоносных компьютерных программ (информации) // Lex Russica. - 2014. - №11. - С. 1324.

² Магомедов М. Д. Криминологические проблемы создания, использования и распространения вредоносных компьютерных программ // Юридический вестник Дагестанского государственного университета. - 2012. - №4. - С. 79.

Из-за этого вытекает еще одна интересная деталь. В предыдущем параграфе, затрагивалась тема того, что программы для ЭВМ также являются объектом авторского права и если следовать этому принципу, то и вредоносные программы должны защищаться авторским правом. Этого не происходит по причине того, что само создание вредоносных программ является уголовно наказуемым деянием, и к тому же статья 10 ГК РФ устанавливает, что гражданские права связанные с причинением вреда другому лицу - не осуществляются. Но не смотря на все это, если вредоносная программа создавалась не в преступных, а, например, исследовательских и научных целях, то они имеют все шансы стать объектом авторского права.¹

Предметом преступного посягательства можно назвать непосредственно сами создаваемые вредоносные программы.

Основным объектом являются общественные отношения, обеспечивающие безопасность в сфере компьютерной информации.

Объективной стороной является создание, использовании или распространении вредоносных компьютерных программ, то есть таких программ, выполнение которых может привести к неправомерному уничтожению, блокированию, изменению или копированию информации, а также нарушению нормального функционирования компьютерных систем.

Субъект данного преступления - общий, представляющий из себя дееспособное физическое лицо, достигшее 16-летнего возраста.

Субъективная сторона преступления выражается в прямом умысле, что означает, что лицо осознает общественную опасность своих действий, предвидит возможность наступления общественно опасных последствий и желает их наступления.

Тяжесть же наступивших последствий не закреплена и является строго оценочной.

¹ Юзефович Ж.Ю., Павлова А.А. Авторско-правовая охрана вредоносного программного обеспечения // Вестник Московского университета МВД России. - 2014. - №12. - С. 106.

Для того чтобы быть признанным виновным в совершении данного преступления, необходимо, чтобы лицо осознавало общественную опасность своих действий и желало наступления указанных законом последствий. Другими словами, виновный должен понимать, что создание или распространение вредоносной программы может нанести вред безопасности компьютерной информации и желать, чтобы эти последствия произошли.

Кроме того, для данного преступления характерен признак заведомости – очевидность для виновного того, что созданная им программа может причинить указанные в законе общественно опасные последствия. То есть, если лицо, создавая вредоносную программу, понимал, что она может нанести вред компьютерной информации, но надеялся на отсутствие негативных последствий, это не исключает его вину.

Если же лицо не знало об опасности распространяемых им программ, то оно не может быть признано виновным в совершении преступления. Таким образом, для привлечения к уголовной ответственности необходимо наличие умысла в совершении преступления.

Состав преступления является формальным. Данное преступление считается совершенным в момент создания, использования или распространения вредоносных программ или информации, которые создают угрозу наступления описанных в законе последствий. Это имеет место независимо от того, наступили ли эти последствия на самом деле или нет.

История данной статьи во многом совпадает с историей статьи 272, которая была рассмотрена ранее. Статья 273 также была введена в уголовный кодекс 1 января 1997 года и за годы своего существования претерпела множество изменений. Одними из наиболее значимых изменений стали те, которые были внесены Федеральным законом № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 7 декабря 2011 года.

Была внесена дополнительная часть, которая криминализует действия, совершенные группой лиц по предварительному сговору или организованной группой, а также действия, совершенные лицом, использующим свое служебное положение, с целью нанесения крупного ущерба или из корыстных побуждений.

Часть вторая переместилась в третью и ввела ответственность не только за сам факт наступления тяжких последствий, но и за создание угрозы их возникновения.

Статья 273 УК РФ относит к тяжким последствиям такие действия как, например, нарушение работы организации на длительный период времени, доступ к охраняемой законом информации, предоставление ее неограниченному кругу лиц, причинение смерти или серьезного вреда здоровью хотя бы одному человеку и т.д.

Это изменение закона расширило возможности правоохранительных органов по предотвращению преступлений до их фактического совершения и предотвращению негативных последствий. Теперь правоохранители имеют право задерживать злоумышленников на этапе создания вредоносных программ или еще до того, как они успели использовать их для достижения своих целей.

Но стоит уточнить, что когда подсудимому предъявляется обвинение в создании угрозы наступления тяжких последствий, то необходимо доказать реальность такой угрозы, в противном случае он не будет нести ответственность по данной части.

В целом, мы видим, что статья 273 УК РФ так же менялась в ответ на растущую угрозу развития компьютерной преступности и методов ее совершения, а в данном случае - вредоносных программ. В нынешнее время, с развитием и общедоступностью компьютерных технологий мы можем заметить как эволюционируют вредоносные программы и способы их применения. Все более изощренно и незаметно они обходят даже самые

продвинутые средства защиты, распространяясь словно инфекция и ставя под угрозу не только личные данные пользователей, но и работоспособность целых отраслей производства и даже человеческой жизни.

Анализируя предоставленную статистику, опубликованную на сайте Агентства правовой информации за период с 2018 по 2022 годы, становится ясно, что, аналогично статье 272, большинство раскрытых преступлений по статье 273 было совершено в случаях, когда деяния осуществлялись группой лиц по предварительному сговору, организованной группой или лицом, использующим свое служебное положение. В отличие от статьи 272, в данной статье такие случаи соответствуют второй части.

Из 323 осужденных по этой статье за пять лет, 220 человек приходится на вторую часть, что составляет 68% от общего числа осужденных.

Кроме того, при изучении данной статистики можно заметить, что полностью отсутствуют раскрытые преступления, совершенные по третьей части статьи 273 в случаях, когда деяния, предусмотренные первой или второй частью этой статьи, повлекли за собой серьезные последствия или создали угрозу их наступления.

Это может быть связано с несколькими возможными причинами:

- Преступления, предусмотренные третьей частью статьи 273, в целом реже совершаются. Это может быть связано с определенными условиями и требованиями для их совершения, отражающими специфику свойственную преступности, связанной с созданием вредоносных программ.

- Преступления, совершенные по третьей части статьи 273, являются сложными в раскрытии и собирании достаточных доказательств. Они требуют специализированных знаний, технических возможностей или длительных расследований, что делает их раскрытие более сложным.

- Недостаток ресурсов, таких как специалисты, техническое оборудование или финансирование, снижает эффективность расследования

преступлений по третьей части статьи 273. Зачастую это может привести к недостаточным усилиям в раскрытии таких преступлений.

- Возможно, применение эффективных мер предупреждения и предотвращения таких преступлений позволяет снизить их количество. Наличие сильной системы безопасности и контроля ограничивает возможности для совершения преступлений по третьей части статьи 273.

Необходимо отметить, что отсутствие раскрытых преступлений по третьей части статьи 273 в данной статистике не означает, что такие преступления не совершаются вообще. Данная статистика только указывает количество осужденных по конкретным статьям за определенный промежуток времени.

Чтобы сформировать полноценную картину такого преступления, стоит рассмотреть одно из них на примере приговора суда по ч. 3 ст. 273 УК РФ № 1-271/2017 | Создание, использование и распространение вредоносных компьютерных программ, вынесенный Коминтерновским районным судом г. Воронежа.

Суд установил, что Рыжов А.Н., подсудимый по этому делу, вступил в преступный сговор с лицом №1, которое в дальнейшем стало объектом отдельного производства.

Целью этого сговора было незаконное обогащение, путем создания вредоносного программного обеспечения, которое использовало уязвимость в программе бензоколонок. Лицо №1, используя свое служебное положение и знание уязвимостей в системе подачи топлива на бензоколонках ОАО «Воронежнефтепродукт», наняло Рыжова А.Н. для создания вредоносной программы в обмен на денежное вознаграждение.

Данная программа изменяла работу бензоколонок, приводя к систематическому недоливу топлива, которое продавалось клиентам. Затем лицо №1, используя отсутствие контрольно-кассового учета над оставшимся топливом, продавало его сторонним лицам.

Оперативно-розыскными мероприятиями сотрудниками УФСБ России было выявлено, что организованные действия Рыжова А.Н. и лица №1, с использованием вредоносных компьютерных программ, привели к снижению прибыли ОАО «Воронежнефтепродукт» на 150 миллионов рублей и серьезному репутационному ущербу.

Это дело было еще более серьезным из-за того, что ОАО «Воронежнефтепродукт» является частью ОАО «НК-Роснефть», которая принадлежит Российской Федерации. Таким образом, ущерб был нанесен не только компании, но и государству.

В итоге, суд признал Рыжова виновным в совершении преступления, предусмотренного статьей 273 части 3 УК РФ и приговорил его к 1 году 6 месяцам лишения свободы.¹

Данный пример дает представление о том, как вредоносные программы могут быть использованы для незаконного обогащения и причинения ущерба организации, а также государству. Из примера видно, что преступление имело серьезные последствия, включая снижение прибыли компании на значительную сумму и репутационный ущерб.

К тому же мы видим что лицо №1 использовало свое служебное положение и знание уязвимостей в системе для достижения своих преступных целей. Это подчеркивает значимость роли, которую может играть должностное лицо при совершении преступления по данной статье.

Рассмотрение данного примера помогает лучше понять специфику и характер таких преступлений, а также их влияние на организации и общество в целом. Это дает основу для дальнейшего исследования и разработки мер для предотвращения и пресечения подобных преступлений.

В качестве таких мер можно предложить следующие решения:

¹ Приговор Коминтерновского районного суда г. Воронежа от 24.04.2017 по делу № 1-271/2017. - URL: <https://advocate-service.ru/sud-praktika/ugolovnye-dela/prigovory-sudov-po-st.-273-uk-rf-sozdanie-ispolzovanie-i-rasprostranenie-vredonosnyh-kompjuternyh-programm/prigovor-suda-po-ch.-3-st.-273-uk-rf--1-2712017--sozdanie-ispolzovanie-i-rasprostranenie-vredonosnyh-kompjuternyh-programm.html> (дата обращения: 03.05.2023).

- Усовершенствование и дополнение законодательства, включая статью 273 УК РФ, для более эффективного наказания виновных лиц и создания более жестких санкций. Это включает привлечение к уголовной ответственности всех участников сговора и организованных групп.

- Разработка и внедрение превентивных мер для защиты компьютерных систем и данных. Это включает использование современных технологий и механизмов защиты, а также регулярное обновление и обслуживание программного обеспечения с целью устранения уязвимостей.

- Разработка и внедрение строгих политик и процедур в организациях для обеспечения безопасности компьютерных систем. Это включает контроль доступа, регулярные проверки безопасности, шифрование данных и резервное копирование, а также мониторинг и обнаружение аномальной активности.

Важно отметить, что эти меры должны рассматриваться в комплексе и применяться с учетом специфики работы каждой организации. Эффективная борьба с преступлениями связанными с вредоносными программами требует совместных усилий со стороны правоохранительных органов, организаций и общества в целом.

2.3 Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ)

Статья 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» устанавливает уголовную ответственность за нарушение правил эксплуатации компьютерной техники и сетей, что может привести к нанесению ущерба имуществу или нарушению прав и законных интересов граждан.

Согласно данной статье, деяния, предусмотренные ею, включают в себя умышленные или неосторожные действия (или бездействия), связанные с эксплуатацией средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, которые приводят к:

- уничтожению, блокированию или модификации компьютерной информации;
- несанкционированному доступу к компьютерной информации;
- нарушению целостности, защиты и безопасности информации;
- нарушению прав и законных интересов граждан и организаций.

Цель статьи 274 УК РФ заключается в защите прав и законных интересов граждан и организаций от преступлений, связанных с эксплуатацией средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, а также в обеспечении безопасности информации.

В уголовно-правовой науке имеются различные взгляды на то, что подразумевается под правилами использования средств хранения, обработки или передачи защищенной компьютерной информации или информационно-телекоммуникационных сетей и соответствующего оборудования, а также правилами доступа к информационно-телекоммуникационным сетям.

Большинство ученых трактуют правила эксплуатации средств хранения, обработки и передачи компьютерной информации как гигиенические требования к видео терминалам, персональным электронно-вычислительным машинам, а также правила, связанные с технической документацией на компьютеры, организацией работы, внутренним распорядком, сертификацией компьютерных сетей и оборудования, должностными инструкциями и правилами использования компьютерных сетей в определенных учреждениях или организациях.

Некоторые исследователи считают, что нарушение правил может проявляться в различных формах, таких как неправильное техническое обслуживание компонентов компьютера, неправильное подключение к источникам питания, отсутствие резервного копирования данных, отказ от использования антивирусных программ и других инструментов защиты, а также обработке конфиденциальной информации на оборудовании, которое не сертифицировано на соответствие требованиям безопасности.¹

К объекту можно отнести отношения, обеспечивающие безопасность эксплуатации средств хранения информации и телекоммуникационных сетей.

Субъект у данного преступления – специальный, так как положение статьи 274 подразумевает, что лицо, совершившее данное правонарушение, имеет доступ к охраняемым источникам информации. Такое лицо обычно занимает должности с определенными служебными обязанностями и несет ответственность за их выполнение. Сюда могут входить программисты, операторы ЭВМ, системные администраторы, техники-наладчики и другие специалисты, которым предоставлен доступ к конфиденциальным базам данных.

По части 2 статьи 274 УК квалифицирующим признаком является наступление тяжких последствий. В статье 274, «тяжкие последствия» понимаются идентично со статьями 272 и 273.

Субъективная сторона может проявляться в виде прямого умысла или неосторожности. Квалифицированные составы могут предполагать наличие двух форм вины.

Состав объективной стороны преступления включает нарушение норм эксплуатации устройств хранения, обработки и передачи компьютерной информации и сетей ИТК, приводящее к уничтожению, блокированию или

¹ Степанов-егиянц В. Г. Новая редакция статьи 274 Уголовного кодекса РФ: проблемы и пути решения // Мониторинг правоприменения. - 2014. - №2. - С. 22.

изменению охраняемой законом информации, если это повлекло значительный ущерб.

Если совершение преступления было сознательным, то нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, как описано в статье 274 УК РФ, может рассматриваться лишь как способ совершения другого преступления.

Для данного преступления характерен материальный состав. Аналогично статье 272, нарушение правил эксплуатации должно привести к уничтожению, блокированию, модификации или копированию компьютерной информации, что является причиной значительного ущерба.

УК РФ Статья 274 (Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей), появилась так же как и статьи 272 и 273 - 1 января 1997 года в новом уголовном кодексе.

Федеральный закон № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 7 декабря 2011 года, как и в статье 272 убрал из диспозиции статьи 274 уточнение, касающееся ЭВМ, как основного места хранения компьютерной информации. Сделано это было по той же причине, связанной с практической проблемой определения перечня устройств, которые можно считать носителями информации.

Правила техники безопасности, рабочий регламент и индивидуальные инструкции, составленные производителем оборудования, также регулируют указанные отношения. В отличие от уголовного кодекса, эти предписания не предусматривают уголовной ответственности за их нарушение и действуют только в пределах организации, однако их несоблюдение может привести к совершению преступления по статье 274 УК РФ.

Нарушение правил, связанных с эксплуатацией средств хранения, обработки или передачи компьютерной информации, информационно-телекоммуникационных сетей, может быть как активным действием, так и бездействием, проявляющимся в форме халатности или легкомыслия. Это важно отличает преступление, предусмотренное статьей 274 УК РФ, от преступлений, описанных в статьях 272 и 273, которые могут быть совершены только путем действий.

В целом, данная статья в большей мере направлена на пресечение халатного и неосторожного обращения с компьютерной информацией, имеющей специальный статус, охраняемый законом, вроде государственной и коммерческой тайны.

Она во многом схожа со статьей 272 УК РФ (Неправомерный доступ к компьютерной информации), с разницей в том, что в статье 274 - уничтожение, изменение, блокирование или модификация компьютерной информации не является самой целью, а результатом недобросовестного отношения специалистов в вопросе выполнения своих прямых обязанностей.

3 Проблемы квалификации преступлений в сфере компьютерной информации и пути их решения

Из всего вышеизложенного следует, что вопрос преступности в сфере компьютерной информации крайне актуален в наше время, особенно учитывая то, что компьютерные технологии все больше проникают в нашу жизнь и могут стать опасным инструментом в руках злоумышленников. Россия, как и многие другие страны, активно внедряет компьютеризацию во все сферы экономики, промышленности, управления, образования и т.д., которые могут также стать объектом преступного посягательства.

Как и криминальные элементы, органы правопорядка также активно совершенствуют свои методы борьбы с преступлениями в сфере компьютерной информации. Однако, как было упомянуто ранее, законодатель сталкивается с определенными проблемами, особенно в формировании четкой квалификации такого рода преступлений.

В уголовном праве, квалификация преступления означает определение точного соответствия между признаками совершенного деяния и составом преступления, указанного в уголовной норме.

На практике возникают сложности при квалификации преступлений в сфере компьютерной информации совместно с другими составами преступлений. Это объясняется неоднородностью объекта компьютерных преступлений, отсутствием соответствующих положений в статьях Особенной части УК РФ, которые рассматривали бы компьютерные технологии как средства совершения других преступлений, а также отсутствием адекватного понятийного аппарата, относящегося к компьютерной информации и современной компьютерной преступности.

В научной литературе, связанной с уголовным правом, существуют два основных подхода к решению проблемы квалификации компьютерных

преступлений. Первая группа авторов предлагает внести изменения в составы ряда преступлений, включая такие способы совершения, как использование компьютерных средств. Например, предлагается расширить диспозиции статей, включив формулировки, которые учитывают применение компьютерной информации, электронно-вычислительных машин, сетей и других высокотехнологичных средств. Однако такой подход может привести к перегруженности статей УК РФ и не учитывать быстрое развитие технологий и появление новых способов совершения преступлений.

Вторая группа ученых считает целесообразным введение отдельной главы или раздела, посвященного компьютерным преступлениям. Предлагается создать самостоятельную главу или раздел, где будут расширены перечень и определения компьютерных преступлений. Однако данный подход также имеет свои ограничения, так как компьютерные преступления могут затрагивать различные объекты и сферы, и введение нового раздела может нарушить принцип системности уголовного законодательства.

Прежде чем говорить о введении нового раздела или внесении изменений, необходимо определить и уточнить виды преступлений, совершаемых с использованием информационных технологий. Возможно, следует рассмотреть включение в УК РФ конкретных преступлений, таких как компьютерный саботаж, компьютерный шпионаж, кибертерроризм, распространение спама и другие, чтобы более точно определить их составы и наказания.

Очевидно, что каждый из упомянутых подходов имеет свои преимущества и недостатки. Для определения наиболее рационального подхода к решению проблемы квалификации компьютерных преступлений, мы можем проанализировать статью 159.6 Уголовного кодекса РФ, которая предусматривает ответственность за мошенничество в сфере компьютерной информации.

Следует отметить, что ранее преступления, такие как кража (статья 158) и мошенничество (статья 159), совершаемые с использованием компьютерных технологий, квалифицировались по совокупности с статьями 272 и/или 273 Уголовного кодекса РФ. Однако внесение поправок Федеральным законом «О внесении изменений в Уголовный кодекс РФ и отдельные законодательные акты РФ» привело к появлению шести квалифицированных составов мошенничества, включая мошенничество в сфере компьютерной информации (статья 159.6). Эти изменения стали ответом законодателя на увеличивающееся число случаев так называемого компьютерного мошенничества.

Статья 159.6 Уголовного кодекса РФ, которая квалифицирует мошенничество в сфере компьютерной информации, отличается от статьи 159, которая регулирует простое мошенничество, по способу совершения преступления, а именно использованием компьютерной информации. В случае мошенничества в сфере компьютерной информации, обман осуществляется путем предоставления недостоверной информации, с целью ввести в заблуждение физическое лицо. Однако при хищении чужого имущества с использованием компьютерной информации, речь не идет о обмане. Хищение представляет собой незаконное завладение вещами, имеющими физическую форму. В то же время, информация не имеет материального проявления.

Вероятно, исходя из этих различий, законодатель ввел статью 159.6 для учета специфики мошенничества с использованием компьютерной информации. Исключение из состава преступления таких «классических» методов, как обман и злоупотребление доверием, позволяет предположить, что статья 159.6 также применяется к краже, совершенной через неправомерный доступ к компьютерной информации. Однако эта статья не охватывает все способы хищения чужого имущества с использованием компьютерной информации. Например, действия лица, которое использует

вредоносную программу, созданную им для обхода средств защиты компьютерной информации и хищения имущества, квалифицируются по совокупности статей 159.6 и 273 Уголовного кодекса РФ.

Необходимо различать случаи, когда ввод, удаление, блокирование, модификация или другое вмешательство в работу устройства являются способами хищения, от случаев, когда компьютер используется как инструмент для совершения мошеннических действий. Например, если человек отправляет пользователю электронное письмо с сообщением о выигрыше большой суммы денег, при условии отправки платного SMS на определенный номер, то такие действия будут рассматриваться в соответствии с частью 1 статьи 159 Уголовного кодекса. Однако, если после прочтения этого электронного письма на компьютер пользователя автоматически устанавливается вредоносная программа, предназначенная для сбора и отправки злоумышленнику информации о его электронных счетах, то такое действие будет квалифицироваться по части 1 статьи 159.6 и части 1 статьи 273 Уголовного кодекса.

Однако название статьи «Сфера компьютерной информации» может быть некорректным. Как указывает М.А. Ефремова, формулировка «сфера компьютерной информации» является довольно абстрактной и не имеет четко определенных границ. В литературе отсутствует единообразный терминологический аппарат для обозначения такого рода преступлений.

Также возникают трудности с определением компьютерной информации, представленной в форме электрических сигналов, как это указано в примечании 1 к статье 272 УК РФ. Это создает проблемы при квалификации мошеннических действий по статье 159.6, совершаемых с использованием других средств передачи, хранения и обработки информации, отличных от компьютера. Существуют устройства, которые хранят информацию без использования электрических сигналов, например, оптоволоконные сети, использующие световые сигналы. В связи с этим

возникают трудности при квалификации «мобильного мошенничества», направленного против мобильных телефонов, планшетных компьютеров, КПК и других устройств. Поэтому предложение М.А. Ефремовой о замене термина «компьютерная информация» на «электронная информация» кажется целесообразным. Такая формулировка способна значительно расширить круг охраняемых уголовным законом отношений и защитить устройства от незаконных посягательств.

Представленный анализ показывает, что законодательство приняло решение о включении специальных составов преступлений, связанных с компьютерными преступлениями, в Уголовный кодекс. Однако низкий уровень юридической точности и отсутствие логики в конструкции состава компьютерного мошенничества, на мой взгляд, маловероятно будут способствовать эффективности уголовного судопроизводства. Избыточное накопление специальных составов компьютерных преступлений нарушает принцип системности уголовного законодательства. Введение отдельного состава мошенничества с использованием компьютерной информации поднимает вопрос о включении аналогичных составов с пометкой 1 к другим статьям Уголовного кодекса. В итоге, применение Уголовного кодекса может стать затруднительным.

Я поддерживаю позицию некоторых авторов, считающих, что наиболее оптимальным решением было бы включение в статью 159 квалифицирующего признака, а именно - использование информационных технологий или электронной информации.¹

Необходимо обратить внимание на проблемы, связанные с определением объекта посягательства при совершении преступлений, направленных против нескольких объектов. В таких случаях на практике возникают ошибки при определении совокупности этих преступлений. Среди

¹ Нагорный А. А. Проблемы квалификации преступлений в сфере компьютерной информации // Наука и мир. - 2013. - №3. - С. 168.

примеров таких проблемных статей можно упомянуть нарушение неприкосновенности частной жизни (статья 137 УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (статья 138 УК РФ), нарушение авторских и смежных прав (статья 146 УК РФ), нарушение изобретательских и патентных прав (статья 147 УК РФ), разглашение тайны усыновления (удочерения) (статья 155 УК РФ), кражу (статья 158 УК РФ), вымогательство (статья 163 УК РФ), незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (статья 183 УК РФ), государственную измену (статья 275 УК РФ), шпионаж (статья 276 УК РФ), публичные призывы к осуществлению экстремистской деятельности (статья 280 УК РФ), разглашение государственной тайны (статья 283 УК РФ) и другие аналогичные статьи.

На примере некоторых из статей, рассмотрим какие изменения можно внести.

Так, статья 138 УК РФ определяет нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, в том числе гражданских. Если информация, к которой был получен несанкционированный доступ, была заблокирована, изменена или скопирована, то такое деяние должно рассматриваться как совокупность преступлений согласно статье 272 части 1 УК РФ и статье 138 части 1 УК РФ. Если же преступление было совершено с использованием служебного положения, то оно должно быть квалифицировано по статье 272 части 2 УК РФ и статье 138 части 2 УК РФ.

Статья 146 УК РФ затрагивает вопросы нарушения авторских и смежных прав, что означает возможность автора контролировать использование и распространение его произведения или программы. Статья 272 УК РФ, в свою очередь, направлена на обеспечение информационной безопасности, а статья 146 УК РФ - на защиту конфиденциальности

информации, связанной с правом владельца ограничивать доступ к ней. Для нарушения авторских прав необходимо преодолеть средства защиты информации, используемые владельцем. Если копирование и модификация информации возможны без обхода защиты, то это не является неправомерным доступом. Поэтому, даже законный владелец лицензионной версии программы может нарушать авторские права, если взламывает ее и вносит изменения, позволяющие незаконно копировать программу для продажи и использования другими лицами. Если такое действие причиняет крупный ущерб правообладателю, то его можно рассматривать как совокупность преступлений по статьям 272 и 146 УК РФ. Если же лицо устанавливает на свой компьютер нелегальное программное обеспечение или копирует нелегальную информацию, но не преодолевает защиту, то это деяние нельзя квалифицировать по статьям 272 и 146 УК РФ в совокупности. Лицо, которое использует уже взломанное программное обеспечение или носители с нелегальным аудио-видео материалом, даже если знает, что продукт является пиратским, не совершает неправомерный доступ к законно охраняемой компьютерной информации, а лишь нарушает имущественные права авторов или правообладателей продукта. В этом случае производитель защищает свой продукт от несанкционированного копирования с целью получения прибыли от его продажи.

Статья 183 УК РФ устанавливает уголовную ответственность за незаконное получение и разглашение сведений, которые законом признаны коммерческой, налоговой или банковской тайной. Квалификация этого деяния достаточно сложна, поскольку такие сведения защищены законодательством. Если данная информация находится в электронном виде, то нарушение прав доступа к этой информации и ее незаконное использование считаются совершением сразу двух преступлений. Это позволяет квалифицировать такие

действия как совокупность преступлений, предусмотренных статьями 183 и 272 УК РФ.¹

Также, самые спорные нормы в системе уголовных преступлений связаны со статьей 274 УК РФ. Эта статья устанавливает ответственность за нарушение правил эксплуатации компьютерной информации и информационно-телекоммуникационных сетей.

Для определения объективной стороны преступления используется прием бланкетности, в соответствии с которым указание на деяние имеет обобщенный характер - «нарушение правил». Для определения этих правил статья отсылает к инструкциям и положениям, устанавливающим правила эксплуатации в организации или учреждении. Однако отсутствует единая правовая основа для определения порядка защиты информации, которая приводит к спорам о правильной квалификации преступлений.

Одним из решений такой проблемы могло бы стать создание единого подзаконного нормативно-правового акта, содержащего правила защиты эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Также одной из проблем квалификации преступлений в сфере компьютерной информации является недостаток знаний и навыков в расследовании таких преступлений, из-за высокой латентности, что затрудняет формирование опыта борьбы с ними. Это приводит к неоднозначной практике и отсутствию стандартов реагирования на инциденты, что усложняет борьбу с компьютерной преступностью. Часто преступников не удается поймать, и правоохранительным органам приходится

¹ Расова Е.В. Некоторые проблемы квалификации преступлений в сфере компьютерной информации // Научно-практический электронный журнал Аллея Науки. Сер. Право. - 2019. - №1. - С. 743.

работать только с последствиями их преступлений, что приводит к своеобразному правовому нигилизму.¹

Кроме того, недостаток специалистов в области IT-технологий в системе следствия и на досудебном этапе производства снижает качество рассмотрения дел по данной категории. Для решения этой проблемы необходимо повышать мониторинг данной категории преступлений, разрабатывать программы повышения квалификации следователей и улучшать технические возможности криминалистических лабораторий, специализирующихся в данной области.

Кроме того, можно взять пример из других стран, например, США, и ужесточить меры наказания за компьютерные преступления, чтобы использовать их в качестве превентивных мер в борьбе с ними.

¹ Лысак Е.А. Проблемы квалификации преступлений в сфере компьютерной информации // Научный журнал КубГАУ. - 2013. - №90. - С. 4.

ЗАКЛЮЧЕНИЕ

В ходе исследования уголовно-правовой характеристики преступлений в сфере компьютерной информации были проведены анализ отечественного и зарубежного опыта, изучены история возникновения и развития компьютерных преступлений, судебная практика, научная литература, а также понятия и виды преступлений в данной сфере. Было осуществлено детальное рассмотрение статей 272, 273 и 274 Уголовного кодекса Российской Федерации, а также выявлены проблемы квалификации таких преступлений и предложены пути их решения.

Одним из основных выводов работы является то, что компьютерные преступления представляют собой серьезную угрозу информационной безопасности общества и экономическим интересам государства и частных лиц. Было показано, что такие преступления являются относительно новым явлением, которое несет в себе сложности в определении и квалификации.

Анализ статей 272, 273 и 274 УК РФ позволил выявить пробелы и противоречия в законодательстве, которые затрудняют эффективное преследование и наказание лиц, совершающих преступления в сфере компьютерной информации. Были выявлены проблемы в доказывании виновности, определении объема причиненного ущерба и установлении ответственности за совершение данных преступлений.

В рамках исследования были предложены следующие пути решения проблемы преступности в сфере компьютерной информации:

Совершенствование законодательства: необходимо провести адаптацию уголовного законодательства к быстро меняющейся информационной среде, включая уточнение понятий и расширение квалифицирующих признаков компьютерных преступлений.

Необходимо ввести новый квалифицирующий признак «Преступление, совершенное с использованием информационных технологий». Стоит

добавить, что вместо термина «Компьютерные технологии» лучше будет использовать более широкий термин «Информационные технологии», как охватывающий больший спектр способов передачи информации различными электронными устройствами.

Введение нового квалифицирующего признака заметно облегчит работу правоприменителей, так как на данный момент при рассмотрении дел с использованием компьютерных технологий, зачастую используется совокупность из двух или более статей, что может ввести некоторую путаницу в определении точного состава преступлений.

Также, можно дополнить главу 28 некоторыми статьями, которые присутствуют в уголовных кодексах других стран.

Например, одним из таких нововведений может быть введение статьи «Компьютерный саботаж», которая, учитывая нынешнюю обостренную политическую обстановку в мире, будет особенно актуальна.

Также, если говорить о заграничном опыте борьбы с компьютерной преступностью, то одним из возможных решений было бы усиление санкций в отношении правонарушителей. Например увеличение размера выплачиваемых штрафов и срока лишения свободы, особенно за такие статьи как 274.1 и 274.2.

В заключение можно отметить, что компьютерные преступления являются актуальной и сложной проблемой, требующей комплексного подхода и совместных усилий со стороны законодателей, правоохранительных органов, специалистов в области информационной безопасности и общественности. Реализация предложенных в работе путей решения проблем квалификации преступлений в сфере компьютерной информации позволит эффективнее бороться с данной формой преступности и обеспечить безопасность в информационной среде.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно-правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Собрание законодательства РФ. - 2009. - № 4. - Ст. 445.

2. Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Собрание законодательства Российской Федерации. - 2001. - № 26. - Ст. 2674.

3. Модельный уголовный кодекс - участников Содружества Независимых Государств: Принят Постановлением Межпарламентской Ассамблеи государств - участников Содружества Независимых Государств 17.02.1996 (ред. от 16.11.2006) // Информационный бюллетень Межпарламентской ассамблеи государств. - 1997. - № 10.

4. Уголовный кодекс Российской Федерации от 13.06.1996 (ред. от 28.04.2023) // Собрание законодательства Российской Федерации. - 1996. - № 25. - Ст. 2954.

5. Уголовный кодекс Республики Казахстан от 16.07.1997 (ред. от 20.05.2023) // Ведомости Парламента Республики Казахстан. - 1997. - № 15-16. - Ст. 211.

6. Гражданский кодекс Российской Федерации от 13.11.1994 (ред. от 14.04.2023) // Собрание законодательства Российской Федерации. - 1994. - № 32. - Ст. 3301.

7. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 3524-1 (ред. от 29.12.2022) // Собрание законодательства Российской Федерации. - 2006. - № 31. - Ст. 3448.

8. О связи: Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 18.00.2023) // Собрание законодательства Российской Федерации. - 2003. - № 28. - Ст. 2895.

9. О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации: Указ президента от 03.04.1995 № 334 (ред. от 25.07.2000) // Собрание законодательства Российской Федерации. - 1995. - № 15. - Ст. 1285.

10. Об участии в международном информационном обмене: Федеральный закон от 04.07.1996 № 85-ФЗ (ред. от 27.07.2006) // Собрание законодательства Российской Федерации. - 1996. - № 28. - Ст. 3347. (утратил силу).

11. О правовой охране топологий интегральных микросхем: Федеральный закон от 23.09.1992 № 3526-1 (ред. от 02.02.2006) // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. - 1992. - № 42. - Ст. 2328. (утратил силу).

12. О правовой охране программ для ЭВМ и баз данных: Федеральный закон от 23.09.1992 № 3524-1 (ред. от 18.12.2006) // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. - 1992. - № 42. - Ст. 2326. (утратил силу).

13. О правовой охране программ для электронных вычислительных машин и баз данных: Федеральный закон от 23.09.1992 № 3523-1 (ред. от 18.12.2006) // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. - 1992. - № 42. - Ст. 2325. (утратил силу).

Учебная и научная литература

14. Алескеров В.И. О преступлениях, совершаемых в сфере телекоммуникаций и компьютерной информации / В. И. Алескеров // Преступность в сфере информационных и телекоммуникационных

технологий: проблемы предупреждения, раскрытия и расследования преступлений: сборник научных трудов. - Воронеж: Воронежский институт МВД России, 2018. - 140 с.

15. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. - М.: Юрлитинформ, 2002. - 496 с.

16. Зубова М.А. Компьютерная информация как объект уголовно-правовой охраны: специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: автореф. дис. на к.ю.н. - Казань, 2008. - 215 с.

17. Кудрявцев В.Л. Преступления в сфере компьютерной информации: общая характеристика // Уголовное законодательство в XXI веке: современное состояние, проблемы трактовки и применения его положений с учетом задач дальнейшего укрепления экономического правопорядка: материалы международной научно-практической конференции, Нижний Новгород, 1 марта 2012 г. / Под ред.: Козлова А.В., Панченко П.Н. - Нижний Новгород: НИУ ВШЭ. - 2012. - 525 с.

18. Полежаев А.П. Компьютерные технологии в правоохранительной сфере: сборник научных трудов. - М.: Академия МВД РФ, 1993. - 192 с.

19. Попов А.Н. Преступления в сфере компьютерной информации: учебное пособие. - СПб.: Санкт-Петербургский юридический институт Академии Генеральной прокуратуры РФ, 2018. - 69 с.

20. Семкин С.Н. Основы правового обеспечения защиты информации: учебное пособие для студентов высших учебных заведений. - М.: Горячая линия - Телеком, 2007. - 238 с.

Публикации в научных журналах, сборниках и СМИ

21. Бессонов С.А. История и зарубежный опыт правовой регламентации компьютерной преступности // Теория науки. - 2013. - № 2. - С. 231-237.

22. Дворецкий М. Ю. Корреляции главы 28 УК РФ в контексте оптимизации уголовной ответственности и повышения эффективности правоприменительной практики // Вестник ТГУ. - 2012. - №6. - С. 266-271.
23. Жиделев В.Г. Эволюция законодательства об уголовной ответственности за совершение преступлений в сфере высоких технологий // Вестник Удмуртского университета. Серия «Экономика и право». - 2011. - №4. - С. 114-118.
24. Карамнов А.Ю., Дворецкий М. Ю. Законодательство Великобритании о преступлениях в сфере компьютерной информации // Социально-экономические явления и процессы. - 2013. - №8. - С. 164-167.
25. Китайкина О.О. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации: история и современность // Научный формат. - 2020. - №7. - С. 118-126.
26. Китайкина О.О. О соотношении понятий «компьютерные преступления» и «преступления в сфере компьютерной информации» // Научный формат. - 2020. - №6. - С. 227-235.
27. Лысак Е.А. Проблемы квалификации преступлений в сфере компьютерной информации // Научный журнал КубГАУ. - 2013. - №90. - С. 1-10.
28. Магомедов М. Д. Криминологические проблемы создания, использования и распространения вредоносных компьютерных программ // Юридический вестник Дагестанского государственного университета. - 2012. - №4. - С. 78-80.
29. Нагорный А. А. Проблемы квалификации преступлений в сфере компьютерной информации // Наука и мир. - 2013. - №3. - С. 168-171.
30. Никеров Д.М. Хохлова О.М. Преступления в сфере высоких технологий в современной России // Вестник Восточно-Сибирского института МВД России. - 2019. - №2. - С. 204-215.

31. Расова Е.В. Некоторые проблемы квалификации преступлений в сфере компьютерной информации // Научно-практический электронный журнал Аллея Науки. Сер. Право. - 2019. - №1. - С. 741-746.

32. Степанов-егиянц В. Г. Новая редакция статьи 274 Уголовного кодекса РФ: проблемы и пути решения // Мониторинг правоприменения. - 2014. - №2. - С. 18-23.

33. Энгельгардт А.А. Уголовно-правовая оценка создания, использования и распространения вредоносных компьютерных программ (информации) // Lex Russica. - 2014. - №11. - С. 1316-1325.

34. Юзефович Ж.Ю., Павлова А.А. Авторско-правовая охрана вредоносного программного обеспечения // Вестник Московского университета МВД России. - 2014. - №12. - С. 106-108.

Источники на электронных носителях

35. 9-48.000 - Computer fraud and abuse act // The U.S Department of justice. - URL: <https://www.justice.gov/jm/jm-9-48000-computer-fraud> (дата обращения: 30.04.2023).

36. Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff Brief History of the Internet // Internet Society. - 1997. - URL: <https://www.internetsociety.org/internet/history-internet/brief-history-internet/> (дата обращения: 30.04.2023).

37. Morris Worm // FBI. - 2019. - URL: <https://www.fbi.gov/history/famous-cases/morris-worm> (дата обращения: 30.04.2023).

38. Генеральная прокуратура Российской Федерации [официальный сайт]. - URL: <https://epp.genproc.gov.ru/web/gprf> (дата обращения: 30.04.2023).

39. МВД Российской Федерации [официальный сайт]. - URL: <http://www.mvd.ru> (дата обращения: 30.04.2023).

40. Приговор Железнодорожного районного суда г. Хабаровска от 21.02.2017 по делу № 1-127/2017. - URL: <https://advocate-service.ru/sud-praktika/ugolovnye-dela/prigovory-sudov-po-st.-272-uk-rf-nepravomernyj-dostup-k-kompjuternoj-informatsii/prigovor-suda-po-ch.-3-st.-272-uk-rf--1-1272017--nepravomernyj-dostup-k-kompjuternoj-informatsii.htm> (дата обращения: 03.05.2023).

41. Приговор Коминтерновского районного суда г. Воронежа от 24.04.2017 по делу № 1-271/2017. - URL: <https://advocate-service.ru/sud-praktika/ugolovnye-dela/prigovory-sudov-po-st.-273-uk-rf-sozдание-ispolzovanie-i-rasprostranenie-vredonosnyh-kompjuternyh-programm/prigovor-suda-po-ch.-3-st.-273-uk-rf--1-2712017--sozдание-ispolzovanie-i-rasprostranenie-vredonosnyh-kompjuternyh-programm.html> (дата обращения: 03.05.2023).

42. Сайт Агентства правовой информации. - URL: <https://stat.xn----7sbqk8achja.xn--p1ai/> (дата обращения: 03.05.2023).