МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт права
(наименование института полностью)

Кафедра «Уголовное право и процесс»
(наименование кафедры полностью)
40.03.01 Юриспруденция
(код и наименование направления подготовки, специальности)
Уголовно-правовой
(направленность (профиль)/специализация)

БАКАЛАВРСКАЯ РАБОТА

на тему «Уголовная ответственность за преступления в сфере компьютерной информации»

Студент Р.А. Алашев _____
(И.О. Фамилия) (личная подпись)

Руководитель П.А. Кабанов _____
(И.О. Фамилия) (личная подпись)

Допустить к защите

Заведующий кафедрой канд. юрид. наук, доцент, С.В. Юношев _____
(ученая степень, звание, И.О. Фамилия) (личная подпись)

«_____»_____20_____г.

Тольятти 2019

АННОТАЦИЯ

Цель исследования – углубленный анализ и дальнейшее развитие существующих теоретических и практических наработок отечественных и зарубежных специалистов в сфере Уголовной ответственности за преступления в сфере компьютерной информации. На основе изучения и исследование различных точек зрения специалистов этого направления, – раскрыть и проанализировать различные подходы ученых к формированию дискуссионных вопросов, касающихся актуальных проблем указанной преступности, предложить собственное видение отдельных аспектов исследования этого новоявленного разновидности «беловоротничковой» преступности.

Реализация цели обусловила необходимость решить следующие основные задачи:

- определить сущность, криминалистическую классификацию преступлений в сфере компьютерной информации;

- исследовать нормативно-правовую основу регулирования отношений в сфере компьютерной информации;

- рассмотреть развитие правоотношений в сфере компьютерной информации и криминализация компьютерных правонарушений;

- исследовать объективные признаки компьютерных преступлений;

- рассмотреть субъективные признаки преступлений в сфере компьютерной информации;

- выявить некоторые проблемы, связанные с квалификацией компьютерных преступлений;

Объект исследования – преступления в сфере компьютерной информации, а также общественные отношения, связанные с их совершением.

Предмет исследования – механизм совершения регулирования преступлений в сфере компьютерной информации.

Структура работы. Работа состоит из введения, трёх глав, объединяющих в себе шесть параграфов, заключения и списка использованных источников.

Оглавление

Введение

Дальнейшее развитие современных информационных технологий, совершенствование производства и расширение сферы применения новейшей кибернетической техники дали возможность зарождения специфического, сложного вида преступных деяний, где компьютерное оснащение и электронная информация является объектом противоправного посягательства. Наряду с положительными достижениями информатизация сопровождается побочным, негативным явлением криминогенного характера, к которому относят преступления в сфере компьютерной информации, или же «компьютерную преступность» (сокращенное название этого вида преступлений). На современном этапе технологизации общества: обработки и обмена информацией с помощью международной глобальной сети INTERNET, происходят негативные процессы – переход от простой одиночной компьютерной преступности с организованной сложной. Наблюдается динамика слияния новоявленной преступности с международным криминалитетом, что несет в себе соответствующую угрозу обществу в целом. Следует отметить, что такая распространенность усложняет возможности раскрытия и расследования этой категории преступлений работниками правоохранительных органов различных государств. В большинстве документов, принятых на международном уровне, отмечается, что для эффективной борьбы против киберпреступности необходимо более широкое, оперативное и налажено международное сотрудничество. В июне 2001 г. Европейским комитетом совместно с комитетом экспертов в исследовании проблем преступности был разработан проект Конвенции о киберпреступности. В ноябре того же года Конвенция была утверждена комитетом министров Совета Европы и подписана 35 странами, которые взяли на себя обязательства осуществлять согласованную политику борьбы с преступностью в этой сфере. Статистические данные свидетельствуют о достаточно высокий процент таких правонарушений в общем спектре преступности, а их количество, как и

сложность, целенаправленно продвигаются вперед. Наработанные материалы показали, что «хакерское» движение в РФ стремительно развивается и в определенной степени обгоняет в своем развитии другие страны бывшего СССР. К перечню негативных факторов распространения этой категории преступлений можно отнести:

1. Низкий уровень контроля за тиражированием и распространением программной компьютерной продукции.

2. Высокую латентность преступлений. Лишь 10 – 15 % компьютерных преступлений становятся известными. По мнению большинства пострадавших субъектов, разглашения о таком преступлении может повредить их дальнейшей репутации, поэтому довольно часто компьютерные жертвы страдают весомыми убытками ради сохранения собственного престижа.

3. Недостаточность теоретических знаний и практических навыков расследования преступлений в сфере информационных технологий практическими работниками правоохранительных органов, невозможность доведения до суда возбужденных уголовных дел этой категории.

По официальным данным в России за последние пять лет (2013 – 2018) зарегистрирован: 2432 преступления, связанные с неправомерным доступом к компьютерной информации (ст. 272 УК РФ), 579 – с созданием, использованием и распространением вредоносных носителей для ЭВМ (ст. 273 УК РФ) и 175 – с нарушением правил эксплуатации ЭВМ, систем ЭВМ или их сетей (ст. 274 УК РФ). Сотрудниками подразделений по борьбе с преступлениями в сфере высоких технологий выявлено лиц, совершивших данные преступления: 1111 – по ст. 272 УК РФ, 316 – по ст. 273 УК РФ и 92 – по ст. 274 УК РФ.

Исходя из изложенных выше данных, можно прийти к выводу об актуальности затронутой проблематики вопроса, в частности ее криминалистического аспекта. Бесспорно, этот феномен преступности не остается без внимания ученых и других отраслей права, и каждый из них стремится внести свои наработки в общую, заглубленную в глобализационные

процессы дело. Так, например, диссертационные исследования, посвященные уголовно-правовому аспекту преступлений в сфере информационных компьютерных технологий научно обоснован отечественными исследователями: Д.С. Азаровым, Н.В. Карчевским, Н.А. Розенфельд и др. По нашему мнению, несмотря на теоретическую и практическую значимость проведенных и опубликованных исследований, недостаточно уделено внимания именно вопросу организации и расследования компьютерных преступлений.

Цель и задачи исследования – углубленный анализ и дальнейшее развитие существующих теоретических и практических наработок отечественных и зарубежных специалистов в сфере Уголовной ответственности за преступления в сфере компьютернои информации. На основе изучения и исследование различных точек зрения специалистов этого направления, – раскрыть и проанализировать различные подходы ученых к формированию дискуссионных вопросов, касающихся актуальных проблем указанной преступности, предложить собственное видение отдельных аспектов исследования этого новоявленного разновидности «беловоротничковой» преступности.

Реализация цели обусловила необходимость решить следующие **основные задачи**:

- определить сущность, криминалистическую классификация преступлений в сфере компьютерной информации;

- исследовать нормативно-правовую основу регулирования отношений в сфере компьютерной информации;

- рассмотреть развитие правоотношений в сфере компьютерной информации и криминализация компьютерных правонарушений;

- исследовать объективные признаки компьютерных преступлений;

- рассмотреть субъективные признаки преступлений в сфере компьютерной информации;

- выявить некоторые проблемы, связанные с квалификацией компьютерных преступлений;

Объект исследования – преступления в сфере компьютерной информации, а также общественные отношения, связанные с их совершением.

Предмет исследования – механизм совершения регулирования преступлений в сфере компьютерной информации.

Методы исследования. Согласно цели и задач исследования в диссертации использованы следующие методы познания:

• диалектический метод, который дал возможность проанализировать тенденции и закономерности развития научно-технического прогресса, а вместе с ним негативных явлений, которые появились в обществе и пути противодействия этим явлениям обусловленного потребностями практики борьбы с преступностью;

• системно-структурный метод позволил исследовать взаимосвязи между элементами криминалистической характеристики преступлений в сфере компьютерной информации как систему источников доказательственной информации о преступлении;

• формально-логический метод, который дал возможность определить понятие и характеристику отдельных данных предмета исследования и дать им криминалистическую оценку;

• статистический метод, который позволил исследовать и оценить масштабы развития преступности в сфере компьютерной информации и тенденции негативного влияния этой категории преступлений на общество;

• конкретно-социологические методы: анализ, сравнение, анкетирование, обобщение, которые дали возможность выявить осведомленность лиц, которые обеспечивают расследование этих преступлений и общественности, что определило эмпирическую базу исследования;

• сравнительный метод, который определил место методики расследования преступлений в сфере компьютерной информации в общей методике расследования отдельных видов преступлений.

Эмпирическая база исследования. Для достижения цели в работе использованы результаты эмпирических исследований, в частности: ознакомление с материалами пяти уголовных дел, связанных с расследованием преступлений в сфере компьютерной информации; статистические данные этой категории преступлений на примере деятельности правоохранительных органов России за период с 2013 до 2018 года.

Научная новизна полученных результатов заключается в том, что в исследовании, среди других научных работ такого плана, впервые в правовой литературе рассмотрены теоретические и практические вопросы уголовной ответственность за преступления в сфере компьютернои информации. На основе проработанных научных данных, различных точек зрения ученых, их подходов и трактовок, расширено, дополнено, регулирование уголовной ответственности за преступления в сфере компьютернои информации, в частности:

• исследовано теоретическое обоснование криминалистической характеристики преступлений в сфере компьютерной информации, определено ее структуру и содержание;

• определены и исследованы элементы криминалистической характеристики указанной категории преступлений и установлены взаимосвязи между ними;

• установлено специфику организации и планирования начального и дальнейшего этапов расследования преступлений этой категории;

• рассмотрено уголовная ответственность за преступления в сфере компьютернои информации

• рассмотрено правовая регламентацию преступлений в сфере компьютерной информации;

• исследовано уголовно-правовую характеристику компьютерных преступлений;

• выявлено некоторые проблемы, связанные с квалификацией компьютерных преступлений.

Теоретическое и практическое значение результатов исследования заключается в том, что в ней изложены основные положения уголовной ответственности за преступления в сфере компьютернои информации. Ориентированное исследование на практическое применение соответствующими специалистами правоохранительных органов, а также на углубленное изучение студентами высших учебных заведений этой категории преступлений.

Разработки, подготовленные по материалам исследования, могут использоваться в учебном процессе кафедрой уголовного права, процесса и криминалистики высших учебных заведений РФ.

Положения, выносимые на защиту.

1. Обоснование необходимости комплексной разработки правовых (уголовно-правовых, уголовно-процессуальных и иных), криминалистических, информационных и технических проблем, возникающих при формировании и совершенствовании уголовную ответственности за преступления в сфере компьютернои информации».

2. Предложения по уточнению отдельных категорий используемых при формировании уголовной ответственности за преступления в сфере компьютернои информации («кибернетическое пространство», как среда совершения преступления, ((компьютерная информация», ((электронно-вычислительная машина», ((модификация информации», «блокирование информации» и т.п.), обеспечивающие возможность совершенствования механизмов уголовно-правового и уголовно-процессуального регулирования правоотношений в сфере компьютерной информации.

3. Теоретические положения, раскрывающие сущность и принципы построения криминалистической характеристики преступлений в сфере

компьютерной информации, как «системы знаний» (научной абстракции), предназначенной для

4. Предложения и рекомендации по совершенствованию регулирования уголовной ответственности за преступления в сфере компьютернои информации.

Личный вклад соискателя. Теоретические выводы и результаты работы получены на основании личных исследований автора.

Структура работы. Работа состоит из введения, трёх глав, объединяющих в себе шесть параграфов, заключения и списка использованных источников.

Глава 1. Правовая регламентация преступлений в сфере компьютерной информации

1.1 Сущность, криминалистическая классификация преступлений в сфере компьютерной информации

Обеспечение информационной безопасности относит к важнейшим функциям государства[1].

Переход индустриального общества к информационному сопровождался стремительным развитием компьютерных технологий, непосредственно внедрением средств компьютерной техники до производства, торговли, а также к жизни и быта людей. Компьютерные технологии стали основным средством обмена информации, которые значительно облегчили как жизни, так и работу людей. Но вместе со значительными преимуществами данные технологии создают реальные угрозы как для правопорядка в определенной страны, так и мирового правопорядка, поскольку появились новые возможности для совершения ранее неизвестных правонарушений, которые имеют свои особенности.

По экспертным оценкам, сегодня в мире доходы в сфере компьютерной преступности занимают третье место после доходов наркобизнеса и торговли оружием[2]. И на сегодня преступления в сфере использования компьютеров это одна из групп общественно опасных деяний, динамично развивается и набирает обороты.

---

[1] Телийчук В.Г. Способы совершения компьютерных преступлений в сфере высоких технологий и меры противодействия / В.Г. Телийчук //Актуальные вопросы юридической науки: теория и практика : материалы междунар. наук.- практ. конф, 11 декабря 2013 г. / КИДМУ КПУ, 2013. – С. 281-284.

[2] Гавловский В.Д., М.В. Гуцалюк, В.С. Цимбалюк Совершенствование информационного законодательства как средство оптимизации противодействия компьютерной преступности // – 2001. – № 3. – С. 20-24

Как указывает А. В. Войциховский[3], широкое использование современных информационных технологий в государственных и негосударственных структурах, а также в обществе в целом, выдвигает решения проблем информационной безопасности в число основных. Кроме прямого вреда от возможных случаев несанкционированного доступа к информации, ее модификации или уничтожения, информатизация может превратиться в источник серьезной угрозы государственной безопасности и правам человека.

Привлечение компьютерных технологий в все большего количества сфер деятельности государства, приближает нашу страну не только до мировых стандартов и тенденций, но и к их негативным последствиям. Экономика, логистика и безопасность страны все больше зависят от технической инфраструктуры и ее защищенности. Для повышения эффективности борьбы с киберпреступностью, РФ довольно давно начала соответствующие работы, необходимые для создания собственной стратегии кибербезопасности. Мировой опыт в этой области призывает к созданию системы глобального обмена информацией. Как свидетельствуют результаты исследований и многочисленных общественных опросов, вопросы киберпреступности беспокоит не только государство в целом, но и каждого отдельно взятого ее жителя. В этом смысле изучение опыта зарубежных стран, имеющих достаточный опыт борьбы с киберпреступлениями, было бы достаточно актуальным.

Особое внимание проблеме уделяется в западных странах. Изучение отечественными учеными и исследователями состояния научной разработанности проблем сотрудничества и взаимодействия правоохранительных органов различных государств в борьбе с киберпреступностью, также не стоит на месте. Впрочем, их исследование

[3] Войциховский, А. В. Международное сотрудничество в борьбе с киберпреступностью [Электронный ресурс] // Портал : Национальная библиотека имени В. И. Вернадского. – Режим доступа \www/ URL : http ://www.archive.nbuv.gov.ua/portal/.../PB-4_26.pdf . – (Дата обращения 17.04.2019)

свидетельствует, что на современном этапе специальные исследования по проблемам киберпреступности является недостаточно активными. Однако необходимо отметить, что отдельные аспекты такого сотрудничества рассматривались в научных работах Ю. М. Батурина, П. Д. Биленчука, В. Б. Вехова, В. А. Голубева, Н. Д. Дегтяренко, Б. Х. Толеубекова и некоторых других ученых[4].

В 2012 году американская компания, разработчик антивирусного программного обеспечения McAfee, которая принадлежит Intel Corporation, выступила спонсором в создании глобального отчета о состоянии мировой кибербезопасности[5]. Отчет, который был подготовлен брюссельской компанией Security & Defence Agenda, впервые сообщил в открытых источниках о текущей готовности к кибератакам информационных систем различных стран. Отчет был составленный специально для того, чтобы помочь правительствам и организациям понять, насколько они кибернетически защищены в сравнении с другими странами. Базой для составления отчета были исследования группы экспертов в составе 80 специалистов из двадцати семи стран. Они предоставили компании Security & Defence Agenda официальные выводы о текущей готовности к кибератакам информационных систем различных стран.

Кроме группы экспертов к исследованию были привлечены представители 250 мировых лидеров в области ИТ-технологий, информационной безопасности, защиты информации, борьбы с киберпреступностью и из 21 страны. Технологии исследования предполагалось и было выполнено их анонимный опрос. По результатам работы группы экспертов и после обработки результатов опрос, Security & Defence Agenda

[4] Войциховский, А. В. Международное сотрудничество в борьбе с киберпреступностью [Электронный ресурс] // Портал : Национальная библиотека имени В. И. Вернадского. – Режим доступа \www/ URL : http ://www.archive.nbuv.gov.ua/portal/.../PB-4_26.pdf . (Дата обращения 17.04.2019)

[5] McAfee and Security & Defence Agenda (SDA) Unveil Global Cyber Defense Report [Електронний ресурс] // Портал : An Intel Company. – Режим доступу \www/ URL : http://www.mcafee.com/us/about/news/2012/q1/20120120-01.aspx . – (Дата обращения 17.04.2019)

провела ранжирование и установила рейтинг по 5-балльной системе. При этом была исследована текущая готовность к кибератакам информационных систем 23 стран. Состояние готовности для отдельных стран был продемонстрирован на примере рейтинга McAfee, который там используется в качестве основного средства борьбы с киберпреступлениями

Высокий результат, то есть 4,5 балла, было поставлено всего 3 странам, которые имеют довольно небольшую площадь: Швеции, Израиля и Финляндии. Еще 8 стран, включая США, Великобританию, Францию и Германию, получили второе место с 4 баллами. Россия и Польша заняли 4 место с 3-бальным результатом. Из тех данных отчета Security & Defence Agenda.

Из отчета Security & Defence Agenda можно выделить результаты опроса экспертов.

Статистика свидетельствует о следующем:

– 57% мировых экспертов считают, что в киберпространстве происходит «гонка вооружений»;

– 36% считают, что кибербезопасность является более важной проблемой, чем противоракетная оборона;

– 43% определили кибернетическое создание препятствий или нанесения ущерба жизненно важным инфраструктурам, как наибольшую угрозу с катастрофическими экономическими последствиями;

– 45% респондентов считают, что кибербезопасность столь же важна, как безопасность границ государства;

– 56% отмечают, что существует необходимость решения проблемы подготовки квалифицированных кадров по вопросам борьбы с киберпреступностью.

Отчета Security & Defence Agenda содержит большое количество замечаний от группы экспертов. Наиболее существенные из них, это:

– необходимость глобального обмена информацией в режиме реального времени;

– частному и государственному секторам нужны финансовые стимулы для улучшения кибернетической безопасности;

– правоохранительным органам по борьбе с трансграничной киберпреступностью нужно больше полномочий;

– необходима методическая доработка и внедрение в технологии борьбы с киберпреступностью лучших практик институтов международной безопасности;

– существующее дипломатическое упорядочение глобальных кибердоговорённостей должно стать более адресованным;

– для помощи гражданам нужно усовершенствовать и расширить сеть кампаний по информирование населения о методах защиты от кибератак. Практически все специалисты каждой из 27 стран, которые были опрошены в ходе составления отчета, единодушно сошлись в том, что для повышения эффективности борьбы с киберпреступностью необходим глобальный обмен информацией. Кроме того, все они отметили необходимость не просто обеспечение обмена информацией, а именно его оперативность и скорость в принятии управляющих решений.

Европейское агентство по сетевой и информационной безопасности (англ.: European Network and Information Security Agency – ENISA) в своей «Программе надежности и защиты ключевой информационной инфраструктуры» (англ.: Cisco International Internship Program – CIIP), как и эксперты, которые были привлечены Security & Defence Agenda, также настаивает на необходимости начала сотрудничества с целью гарантий согласованности характерных методик киберборьбы[6].

Для РФ такая тенденция является в целом положительной: пока собственная стратегия по защите киберпространства только разрабатывается, чрезвычайно ценной является возможность ознакомления с опытом стран,

[6] Государственные стратегии кибербезопасности [Электронный ресурс] // Портал : Security Lab. – Режим доступа \www/ URL : http://www.securitylab.ru/analytics/429498.php . (Дата обращения 17.04.2019)

которые работают в данном направлении не первый год. И хотя общий вид такой стратегии может сильно варьироваться в зависимости от политики и технических субъективных факторов, многое остается вполне пригодным.

Вообще, компьютерная преступность – это особый вид преступлений, связанных с незаконным использованием современных информационных технологий и средств компьютерной техники.

Данный вид преступлений появился относительно недавно и имеет ряд особенностей, которые присущи и характеризуют только их. Так, необходимо обратить внимание на предмет преступления. Ими будут: электронно-вычислительные машины (ЭВМ), автоматизированные компьютерные системы (АКС), компьютерные сети, носители компьютерной информации. ЭВМ – комплекс электронных технических средств, построенных на основе микропроцессоров и предназначенных для автоматической обработки информации при решении вычислительных и информационных задач. АС – это организационно-технические системы, в которых реализуется технология обработки информации с использованием технических и программных средств.

Социально-экономическое и научно-техническое развитие на современном этапе связанные с решением проблем информатизации государства, общества, правопорядка.

Информационное обеспечение оперативно-розыскной деятельности являются составной информатизации правоохранительных органов, что является неотъемлемой частью информационной системы.

Понятие «компьютерная преступность» и его трансформации в понятие преступлений в сфере информационных технологий мы исследовали ранее, поэтому нет смысла останавливаться на этих вопросах. Только следует напомнить, что выявление и раскрытие компьютерных преступлений, особенно таких, которые совершаются организованными преступными группировками, требует специального профессионального образования и высокого интеллектуального уровня работников правоохранительных органов, им нужно иметь хорошие знания не только в области права, но и в области информатики.

В последнее время наблюдается тенденция к сращивание компьютерной преступности с традиционной организованной преступностью, интернационализации этого вида преступлений. Это проявляется в несанкционированном проникновении в банковские кредитные компьютерные системы, электронную торговлю, в том числе через Интернет, в том числе мошенничестве с магнитными карточками и тому подобное.

Термин «компьютерные преступления» был разработан для определения как абсолютно нового вида преступности, что ориентируются на компьютеры, телекоммуникационные сети и их пользователей, так и для более традиционных преступлений, для совершения которых сегодня используют компьютерное оборудование. Среди компьютерных преступлений, совершенных в мире, все больше становится «международным», таких, как средства или жертвы используют информационные системы различных государств мира, с возможностью доступа к национальным, в том числе и специально защищенных информационных ресурсов, что создает новые условия для организованной преступности – использование Интернет не только для совершения правонарушений, но и для организации виртуальных банд.

Распространенное в зарубежной литературе определение «киберпреступность» охватывает любое преступление, которое совершается с помощью компьютера, компьютерной системы с использованием глобальной сети Интернет, или против компьютерной системы или сети. Этот срок охватывает такие виды деяний, которые обычно определяются как противоправные или ближайшее время могут быть отнесены к уголовным деяниям.

Специфическая особенность глобальной сети – отсутствие границ. Обмен предложениями между членами преступных группировок возможен через анонимные почтовые адреса, которые закрываются после успешного завершения операции. Распространенным видом незаконного использование глобальной компьютерной сети является несанкционированное вмешательство в работу автоматизированных систем телефонной связи, что дает возможность

бесплатно пользоваться услугами международных телефонных переговоров. Но самыми опасными преступниками в киберпространстве есть профессионалы, которые используют свои знания для промышленного шпионажа, политических целей, терроризма.

В свою очередь Сьюзан В. Бренер выделяет следующие особенности, отличающие данные преступления от других.

Во-первых, данный вид преступления не требует физического сближения между жертвой и субъектом преступления в момент совершения преступления. Во-вторых, они часто являются «автоматизированными». В-третьих, субъект данного преступления не подвластен ограничениям, которые существуют в реальном физическом мире. В-четвертых, наука не способна еще устанавливать модели распространение различных видов данных преступлений географически и демографически. И последней особенностью является сложность установления места преступления[7].

Если говорить про первую особенность, то внимание обращается на то, что субъект и потерпевшее лицо непосредственно могут находиться вообще на разных континентах и это не будет обстоятельством, которое будет мешать субъекту совершить данное преступление.

Относительно того, что данный вид преступлений – «автоматизированные», то это означает, что субъект преступления с помощью компьютерных технологий и за относительно короткий промежуток времени может повысить количество преступлений, которые совершаются.

Одной из особенностей преступлений и самых главных проблем для правоохранительных органов является установление места совершения преступления, а также – право какого государства должно применяться, если объект и субъект находятся в разных странах. Вопрос определения места совершения преступления решается по-разному на усмотрение национальных судов.

[7] Brenner S. W. Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement? 30 Rutgers Computer & Tech. L.J. 1 (2004). C. 33

Необходимо обратить внимание также и на то, суды разных стран мира устанавливают свою территориальную юрисдикцию в отношении преступлений с использованием компьютерных технологий в зависимости от следующих оснований:

1) место совершения преступного деяния;

2) место нахождения компьютера;

3) место нахождения (субъект преступления или лицо, которое является потерпевшим от преступления, находится на территории страны) – принцип субъективной территориальности;

4) место наступления общественно опасного последствия (существенное вредное следствие деяния наступает на территории страны) – принцип объективной территориальности;

5) место нахождения любой из перечисленных оснований, в том числе и транзит через территорию страны.

Еще одной особенностью данной группы преступлений является разграничение их в зависимости от объекта.

То есть, в зависимости от того, на что посягает субъект преступления. Так, выделяют преступления, которые нацелены и наносят ущерб конкретным объектам (например, хищение конфиденциальной информации с компьютера) и преступления, которые нацелены и посягают на неопределенный круг объектов (например, создание и распространение вирусных программ).

Таким образом, преступления с использованием компьютерных технологий становятся все распространёнными, но они до сих пор остаются феноменами, так как наука еще не способна четко установить правовое регулирование ответственности за данные преступления, поскольку они имеют ряд своих особенностей и технологии достаточно стремительно развиваются, что и предопределяет появление новых видов преступлений с использованием компьютерных технологий.

Важнейшим элементом криминалистической характеристики преступления является способ его совершения, который состоит из комплекса

специфических действий правонарушителя по подготовке, совершению преступления и его маскировки. Эти действия представляют собой определенную систему, они во внешней обстановке образуют соответствующие отображения, которые в информационном плане является своеобразной моделью преступления.

Отношении киберпреступлений наибольший интерес представляют следы, указывающие на то, как преступник попал и скрылся с места происшествия, преодолел преграды, использовал свое служебное положение, выполнил намеченную преступную цель, какие знания и навыки использовал, попытался скрыть следы своих действий. Важны также следы, свидетельствующие о характере связи преступника с предметом преступного посягательства и тому подобное.

Способ совершения преступления в ряде составов является необходимым элементом объективной стороны преступления и входит в его уголовно-правовые характеристики, а иногда служит даже квалифицирующим обстоятельством. Однако в уголовно - правовой характеристике способ совершения преступления представлен в общем виде, для нее безразличны конкретные способы проникновения, средства, которые используют при этом, источники их получения и т. д. Если же эти обстоятельства существенны, применяют криминалистическую характеристику способа совершения преступления.

Элементы криминалистической характеристики преступлений достаточно изучены и описаны, в частности Есть. И. Зуевым[8]. Однако киберпреступления отличаются от известных криминалистической науке преступных посягательств определенной спецификой.

[8] Криминалистика : актуальные проблемы / под ред. Е. И. Зуева. - М., 1988. С. 120

Так, Н. Г. Шурухнов разделяет способы неправомерного доступа к компьютерной информации на такие три группы: способы непосредственного доступа; способы удаленного доступа; комплексные способы[9].

К первой группе относятся способы, которые в литературе иногда называют «за дураком» (когда для проникновения в запретную зону правонарушитель, держа в руках предметы - элементы маскировки, вместе с какой-то особой проникает в помещение) и «уборка мусора» (использование отходов информационного процесса - физических или электронных, оставленных пользователем после работы с компьютером)[10].

Ко второй группе способов относятся: подключение телекоммуникационного оборудования, компьютерной системы или сети; проникновение в компьютерные сети, путем автоматической переборки абонентских номеров с последующим соединением с тем или другим компьютером; проникновение в компьютерную систему с использованием чужих паролей («неспешный выбор»); непосредственное и электромагнитного перехвата информации. Последний способ основывается на том, что работа электронных устройств (дисплеи, принтеры) сопровождается побочными электромагнитными излучениями (так, сигналы с электронно-лучевой трубки дисплея можно принимать, записывать и анализировать на расстоянии свыше 1000 м).

Третью группу образуют такие способы: ввод в компьютерную программу команд, позволяющих осуществлять незапланированные функции («троянский конь»); модификация компьютерной программы («мистификация»); доступ к базам данных и файлам путем нахождения слабых

[9] Расследование неправомерного доступа к компьютерной информации / под ред. Н. Г Шурухнова. - М. : Щит-М, 1999. С. 254

[10] Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. - М. : Юрид. лит., 1991. С. 160

мест в системах защиты («маскарад»); использование ошибок и недостатков в компьютерной программе[11].

Лиц, совершающих компьютерные преступления (киберпреступления), в криминалистической литературе разделяют на несколько категорий. Так, М. С. Полевой и. В. Крылов выделяют следующие типы:

- нарушители правил пользования ЭВМ (несанкционированное использование компьютеров, распространения вирусов и т. п.);

- «бело воротниковые» преступники;

- «компьютерные шпионы» - подготовленные профессионалы, целью которых является получение важных стратегических данных о противнике в экономической, политической, технической и других сферах;

- «хакеры» («одержимые программисты») - технически подготовленные лица, которые, совершая преступления, часто не преследуют при этом прямых материальных выгод (для них имеет значение самоутверждение, месть за обиду, желание подшутить и тому подобное)[12].

В целом соглашаясь с такой классификацией, считаем, что указанные авторы не в полной мере характеризуют «хакеров». Ведь это не просто «одержимые программисты», а еще и «компьютерные хулиганы».

Кроме того, подавляющее большинство опрошенных (слушателей-офицеров, курсантов и студентов) в начале разговора о компьютерных преступлениях вспоминают, прежде всего, именно хакеров, на самом деле не вполне соответствует действительности. Так, в результате изучения уголовных дел ученые обнаружили, что лишь в 10 % уголовных дел, классифицированных как киберпреступления, личность преступника можно назвать специалистом высокого уровня - хакером. А в 90 % дел - это обычный компьютерный пользователь, который владеет специфической информацией в связи с занятием определенной должности. Одновременно в США в 80-х годах прошлого века из

[11] Полевой Н. С. Компьютерные технологии в юридической деятельности / Н. С. Полевой, В. В. Крылов. - М. : БЕК, 1994.с.239. С. 30-32

[12] Полевой Н. С. Компьютерные технологии в юридической деятельности / Н. С. Полевой, В. В. Крылов. - М. : БЕК, 1994. С. 234-239

каждой тысячи компьютерных преступлений только семь совершали хакеры, однако сейчас, по данным Национального центра криминальной информации США, хакеры совершают уже около 20 % таких правонарушений. То есть вскоре можно ожидать повышения уровня киберпреступлений, совершенных подготовленными специалистами – хакерами[13].

Мы полностью поддерживаем позицию Е. Козлова, который в этой классификации уточняет название второй группы правонарушителей, предлагая именовать их лицами, которые страдают на новый разновидность психической неполноценности - информационные болезни или компьютерные фобии[14].

При наличии подобных фактов в процессе расследования назначают судебно-психиатрическую экспертизу на предмет установления вменяемости преступника во время совершения им преступных действий.

Потерпевшими от преступлений чаще всего являются юридические лица. Это обусловлено тем, что процесс компьютеризации широко охватывает, прежде всего, юридических лиц (организации, учреждения), а в значительно меньшей степени - физических лиц.

Выделяют три главные группы потерпевших от таких преступлений: собственники компьютерной системы, клиенты, пользующиеся их услугами, иные лица. Следует отметить, что потерпевшая сторона первой группы, как правило, неохотно обращается (если делает это вообще) в правоохранительные органы по факту совершения преступления, что, в частности, является одним из главных факторов, который влечет за собой высокий уровень латентности такого вида преступлений.

При расследовании компьютерных преступлений следователь сталкивается с виртуальными следами преступления. Они недоступны непосредственному восприятию. Поэтому получение и анализ доказательств по

[13] Бутузов В. М. Документирование преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи при проведении доследственной проверки : наук. практ. пособ. / [В. М. Бутузов, В. Д. Гавловский, Л. П. Скалозуб и др.]. - К. : Вид. дом «Аванпост-Прим», 2010. С. 54-55

[14] Козлов В. Е. Теория и практика борьбы с компьютерной преступностью / Козлов В. Е. - М. : Горячая линия-Телеком, 2002. С. 162

делам о преступлениях в сфере компьютерной информации представляет собой большую практическую сложность. Объектами поиска могут быть даже записи в виде электронных импульсов в запоминающих устройствах работающего компьютера или телекоммуникационной сети[15].

А.И. Усов отмечает, что «при расследовании преступлений вышеуказанной категории участие специалиста обязательна, поскольку даже малейшие неквалифицированные действия с компьютерной системой зачастую заканчиваются необратимой утратой ценной розыскной и доказательственной информации»[16]. Поэтому, если рассматривать следователя как носителя специальных знаний, то при расследовании компьютерных преступлений их не хватит для полноценного анализа доказательств, поэтому в этом случае не обойтись без привлечения специалиста или эксперта как процессуальной фигуры.

Таким образом, криминалистическая характеристика преступлений в сфере компьютерных технологий является обобщенной информационной моделью, что представляет собой систематизированное описание типичных криминалистических значимых признаков, которые имеют существенное значение для выявления и расследования компьютерных преступлений. С учетом недостаточности знаний практических работников правоохранительных органов, на которых возлагается задача расследовать нетрадиционные преступления, считаем целесообразным детализированный подход к формированию элементов ее криминалистической характеристики. В частности, она должна состоять из таких структурных элементов:

• способы совершения преступлений данной категории;

---

[15] Згадзай О.Э., Казанцев С.Я. Доказательства по делам о преступлениях в сфере компютерной информации: проблемы получения и использования [Электронный ресурс]. – Режим доступа: URL: http://www.crime-research.ru/library/Zgaday.htm. – Название с экрана.(дата обращения 17.04.2019)

[16] Усов А.И. Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств [Электронный ресурс]. – Режим доступа: URL: http://jurfak.spb.ru/conference/1810200/usov.htm. – Название с экрана. (дата обращения 17.04.2019)

• следовая картина этих преступлений;

• личность преступника, мотивы и цель совершения преступления;

• некоторые обстоятельства совершения преступления (место, время, обстановка).

Вопросы борьбы с киберпреступностью в нашей стране является очень актуальным. При этом, в течение последних лет количество раскрытых преступлений в сфере ИТ-технологий в РФ почти не изменилось, хотя в сфере компьютерных и Интернет-технологий, количество раскрытых преступлений увеличилось в несколько раз. Такая ситуация коррелируется с перечисленными выше проблемами и свидетельствует о том, что увеличение уровня защищенности информации в нашей стране требует поддержки и развития.

Таким образом, в среде, где постоянно появляются и эволюционируют киберугрозы, не можно оставаться незащищенным: сложившаяся в мире ситуация обязывает к постоянному совершенствованию методов борьбы с киберпреступлениями и стимулирует построение государственной модели, направленной на обеспечение кибербезопасности страны.

1.2 Нормативно-правовая основа регулирования отношений в сфере компьютерной информации

В цивилизованном обществе любая отрасль деятельности нуждается в правовом регулировании. В России для информационной сферы в настоящее время базовым выступает Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[17]. Статьей 2 данного закона информация определяется как сведения (сообщения, данные) независимо от формы их представления.

Под компьютерной информацией закон понимает не сами сведения, а форма их представления в машиночитаемом виде, т. е. совокупность

[17] Федеральный закон Российской Федерации информационных технологиях и о защите информации»//// Российская газета. 2006. 29 июля.

специфических символов, зафиксированная в памяти компьютера либо на машинном носителе (оптическом, магнитооптическом диске либо ином материальном носителе). При раскрытии и расследовании преступлений в сфере компьютерной информации необходимо учитывать, что в определенных условиях и физические поля могут являться носителями криминалистически значимой компьютерной информации.

Вместе с тем, существует понятие «электронный документ», которое во многих случаях используется как синоним «компьютерной информации». Пункт 11.1 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» определяет электронный документ как документированную информацию, представленную в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах. Анализ данного определения позволяет выделить важный признак компьютерной информации – она всегда представлена в форме, пригодной для обработки с помощью компьютерных устройств.

Логическим развитием правовой системы, создающей условия безопасности компьютерной информации, стало включение в Уголовный кодекс РФ еще в 1996 г. группы статей, предусматривающих основания уголовной ответственности за компьютерные преступления[18].

Вступивший в действие с 1 января 1997 г. Уголовный кодекс Российской Федерации устанавливал ответственность за преступления в сфере компьютерной информации. Имевшееся в то время в статье 272 УК РФ разъяснение «то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети» тоже не являлось строгим в юридическом смысле. Федеральным законом от 7 декабря 2011 г. №

[18] Уголовный кодекс Российской Федерации« от 13.06.1996 N 63-ФЗ (ред. от 01.04.2019)//Собрание законодательства Российской Федерации от 17 июня 1996 г. N 25 ст. 2954

420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»[19] к ст. 272 УК РФ было добавлено Примечание 1, в котором разъясняется, что «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

Электронные вычислительные системы стали общедоступным источником информации, которая с успехом используется сотрудниками правоохранительных органов для раскрытия и расследования преступлений. Учитывая, что, как правило, информация в сети сохраняется длительное время, а затем помещается в резервные хранилища, она является ценным источником доказательств по уголовному делу, а также все более частным предметом совершения преступлений.

1.3 Развитие правоотношений в сфере компьютерной информации и криминализация компьютерных правонарушений

Проблематика юридической ответственности всегда занимала одно из центральных мест в юридической науке. В современной юридической доктрине наиболее распространенным является деление юридической ответственности на четыре вида: уголовную, гражданскую, административную и дисциплинарную. Однако сейчас все больше ученых склоняются к мысли, что такая дифференциация не является исчерпывающей и не соответствует современным правовым реалиям.

В частности, становление и развитие нового вида юридической ответственности – информационно-правовой – вызывает широкую дискуссию среди исследователей, что обуславливает актуальность выбранной темы

[19] Федеральный закон »О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации« от 07.12.2011 N 420-ФЗ (последняя редакция)//Собрание законодательства Российской Федерации от 12 декабря 2011 г. N 50 ст. 7362

публикации. Сегодня в информационной сфере происходят качественные изменения, связанные с массовым использованием компьютерных и информационных технологий. Эта обстоятельство непосредственно связывается с научно-технической революцией и переходом общества к качественно новому состоянию – информационному. Концепция информационного общества приобрела значительное распространение.

Несогласованность и противоречия концепции информационного общества не остались вне поля зрения специалистов, которые призывают к более взвешенному подходу к оценкам и перспективам развития информационных технологий и их влияния на общество.

С развитием информационного общества происходит увеличение количества нарушений правовых норм, регулирующих информационные отношения. Ежегодно в государстве регистрируется несколько миллионов случаев нарушения информационного законодательства, однако, к сожалению, при отсутствии разработанности информационно-правовой ответственности как правовой категории правонарушители не испытывают привлечения к ответственности. Стоит также подчеркнуть, что нарушение норм информационного права предопределяет не только собственно информационно-правовую ответственность, но и ответственность, предусмотренную другими отраслями права.

Информационная ответственность может реализовываться параллельно с административной, уголовной, гражданской и дисциплинарной. При этом в разных случаях информация может играть как главную, так и второстепенную роль.

В информационных правонарушениях информационная составляющая является неотъемлемой от предмета правонарушения. Предметом необходимо понимать информацию как документированные или публично объявленные сведения события и явления, происходящие в обществе, государству и окружающей среде. То есть предметом информационного правонарушения являются конкретные объекты материального мира, в отношении которых

совершено правонарушение. Объектами информационных отношений является документированная или публично оглашаемая информация о событиях и явлениях в области политики, экономики, культуры, здравоохранения, а также в социальной, экологической, международной и других сферах. При определении правонарушения как информационного стоит принимать во внимание принципы, предложенные Ю.Е. Максименко. По мнению исследователя, информационным правонарушением является то правонарушение, которое наносит вреда (опасности) информационным правам или свободам человека и гражданина, информационной инфраструктуре государства или совершается с помощью информационно-телекоммуникационных технологий или средств связи[20].

Ю.Е. Максименко и В.А. Липкан предлагают под информационным правонарушением понимать общественно опасное, противоправное, виновное деяние (действие или бездействие), за совершение которого деликтным законодательством в сфере информации предусмотрено юридическую ответственность и которое фактически является общественно опасным посягательством на информационные правоотношения, охраняемые нормами информационного законодательства, которым оно может причинить или причиняет вред. [21]

По содержанию информационное правонарушения является виновным деянием субъекта информационно-правовой ответственности, а по форме – противоправным действием или бездействием, за совершение которого предусматривается юридическая ответственность в сфере информации[22].

---

[20] Максименко Ю.Е. Информационные правонарушения: понятие и признаки / Ю.Е. Максименко // Глобальной организации союзнического лидерства [Электронный ресурс]. – Режим доступа : http://www.goal-int.org/informacijni-pravoporushennyaponyattya-ta-oznaki.(дата обращения 17.04.2019)

[21] Липкан В.А. Правовой режим налоговой информации: [монография] / [В.А. Липкан, А.В. Шепета, А.А. Мандзюк] ; за заг. ред. В.А. Липкана. – К. : ФОТ О.С. Липкан, 2015. С. 305

[22] Липкан В.А. Основы развития информационной деликтологии / У.А. Липкан, Ю.Е. Максименко // Право. – 2013. – № 10. – С. 249-256

Схожую позицию имеет О.В. Полушкин, который заметил: »Информационные правонарушения происходят преимущественно в особой сфере человеческой деятельности – в информационной сфере, то есть в области поиска, создания, обработки, передачи, получения, хранения, защиты и использования любых сведений об окружающем мире (информации). Нередко они происходят с использованием информационных средств и технологий работы с информацией независимо от ее формы. Информационное правонарушение может происходить также в других сферах человеческой деятельности. Важными обстоятельствами совершения таких деяний есть условия информационной среды их реализации, связанные с использованием информации, информационных средств и технологий работы с информацией независимо от ее формы»[23].

Следовательно, информационное правонарушение – это противоправное, виновное (умышленное или неосторожное) действие или бездеятельность, которая посягает на урегулированные законом общественные отношения, возникающие при осуществлении информационной деятельности (получения, использования, распространения и хранения участниками информационных правоотношений информации), и за которую законом предусмотрено информационную ответственность. Руководствуясь необходимостью определения четких различий между информационными, административными, уголовными, гражданскими и дисциплинарными правонарушениями и преступлениями, приведем основные признаки, характеризующие такие различия.

Во-первых, информационные правонарушения посягают на урегулированные законом общественные отношения, возникающие во время осуществления информационной деятельности, а именно во время создания, сбора, получения, хранения, использования, распространения, охраны и защиты информации, тогда как административные правонарушения посягающие на

[23] Полушкин О.В. О понятии информационного правонарушения / О.В. Полушкин // Российский юридический журнал. – 2009. – № 3. – С. 207–210.

общественный порядок, дисциплинарные – на правила трудовой дисциплины, гражданско-правовые – на имущественные и личные неимущественные отношения, а преступления – общественную безопасность.

Во-вторых, объектами информационных правонарушений является документированная или публично оглашаемая информация о событиях и явлениях в области политики, экономики, культуры, здравоохранения, а также в социальной, экологической, международной и других сферах, тогда как объект преступления – это общественные отношения, охраняемых законом об уголовной ответственности.

Технический прогресс в информационной сфере происходит стремительно. Указанные процессы поставили законодателя перед необходимость эффективного юридического упорядочения общественных отношений в информационной сфере. В русле данной тенденции за последнее десятилетия в сфере информации было принято ряд новых нормативно-правовых актов.[24]

Однако существуют пробелы в законодательстве, которые касаются важных вопросов сохранения и защиты информации, пользования сетью Интернет и тому подобное.

Нерешенность таких правовых вопросов способствует злоупотреблению информационной свободой и неподконтрольной вредной деятельности в информационной сфере, в том числе применении информационных технологий. Применение информационных технологий значительно ускоряет информационные процессы, однако усложняет правовое регулирование этого вопроса и приводит к росту социальной напряженности.

Эти и другие факторы предопределяют повышение научного интереса к проблемам правового регулирования отношений, возникающих по поводу информации. Комплексное исследование информационных правоотношений сегодня приобретает особую актуальность, однако имеющиеся научные

[24] Коваленко Л.П. Некоторые вопросы относительно правонарушений в информационной сфере / Л.П. Коваленко // Форум права. – 2013. – № 4. – С. 158-167

разработки по указанным проблемам, по нашему мнению, не раскрывают их специфику.

В теории права существует мнение, что сейчас приступить к изучению юридической ответственности с позиции информационных отношений трудно, поскольку определение информационной ответственности не существует на законодательном уровне, а также отсутствует единый кодифицированный нормативно-правовой акт, в котором содержался б перечень информационных правонарушений и определялась бы специфичность санкций информационного права.

Проблема отсутствия такого определения проявляется в неправильном применении норм на практике.

Нередко в правоприменительной практике встречаются случаи, когда уполномоченные органы ошибочно рассматривают некоторые правомерны действия владельца информации как информационное правонарушения.

Для того чтобы законодатель мог быстро и правильно реагировать на названные негативные тенденции в отрасли технического прогресса, правовой науке следует тщательно анализировать, искать новые правовые средства, а также разрабатывать научно-практические нормативные рекомендации по устранению таких пробелов в законодательстве.

Одним из таких средств могло бы стать формулирование единого комплексного правового института информационных правонарушений, который включал бы в себя основные понятия, принципы и правовые конструкции, направленные на единое понимание, толкование и правоприменения в этой сфере.

Следовательно, установленный разделение юридической ответственности на уголовную, гражданскую, административную и дисциплинарную не отвечает современным реалиям развития правовой мысли. Несмотря на отсутствие определения понятия «информационная ответственность» в отечественном законодательстве, такая ответственность существует объективно и требует дальнейшего углубленного научного разработку.

Глава 2. Уголовно-правовая характеристика компьютерных преступлений

2.1 Объективные признаки компьютерных преступлений

Чрезвычайно важное место для определения общественной опасности занимает объективная сторона совершения преступления. Объективная сторона в определенной мере определяет мотивы и цели поступка, поскольку субъективные факторы влияют на общественную опасность через внешние формы поведения. Объективная сторона преступления вообще делится на деяния, последствий, причинной связи между деянием и последствиями. Академик В.М.Кудрявцев указывает на то, что объективная сторона преступления является процессом общественно опасного и противоправного посягательства на интересы, охраняемые, с точки зрения последовательного развития тех событий и явлений, которые начинаются с преступного действия или бездействия субъекта и заканчиваются преступным результатом[25].

Уголовное право выделяет два подхода к пониманию объективной стороны:

1) элемент преступления, объективная сторона – это реальное явление, объективная сторона;

2) элемент состава преступления – это элемент научной абстракции, которая необходима для более глубокого познания преступления.

Однако необходимо отметить, что только активное действие или пассивное бездействие, как проявление поведения человека может быть преступлением. А следовательно, основанием уголовной ответственности может быть только преступное поведение людей, что оказалась в конкретном деянии лица.

[25] Кудрявцев В.Н. Объективная сторона преступления. – М.: Госюриздат, 1960. – С. 9.

Действовать – значит не просто вносить изменения в существующий объективный ход событий, но вносить эти изменения целенаправленно[26]. Наука уголовного права исходит из понятия преступного действия как волевого поступка. Это значит, что преступным и уголовно наказуемым может быть только такое деяние, носящее волевой характер[27]. Волевой акт – это акт, свободно и сознательно выбранный человеком с учетом условий, времени, места, обстоятельств[28]. Лицо не может привлекаться к уголовной ответственности, если оно действует против своей воли, под влиянием физического принуждения или непреодолимой силы. Не могут быть признаны действиями человека и рефлекторные реакции, которые не подлежат контролю со стороны сознания.

Любой поступок, выбираемый человеком по собственной воле, имеет иной социальный смысл, чем когда такая воля отсутствует. Свобода воли выражает сознательную активность личности. Человек строит свое поведение в соответствии с собственным желанием, стремлением и целями[29].

В уголовном праве различают две формы преступного поведения: действие и бездействие. Эти формы противоправного поведения положены в основу конструкции конкретных видов преступлений, предусмотренных особой частью уголовного законодательства[30]. Нормы уголовного законодательства или запрещают под страхом наказания совершение конкретных действий, или, наоборот, требуют активно действовать определенным образом. Таким образом, запрет, содержащийся в норме закона может быть возбуждено лицом путем как активного, так и пассивного поведения. Уголовно-правовое действие

---

[26] Волков Б.С. Детерминистическая природа преступного поведения. – Казань: Издат-во Казанского унив-та, 1975. – С. 39-40.
[27] Тимеи□ко Г.В. Общее учение об объективнои□ стороне преступления. – Ростов-на-Дону: Издат-во унив-та, 1977. – С. 29.
[28] Кузнецова Н.Ф. Цель и механизм реформы УК // Государство и право. – 1992. – No 6. – С. 14-31.
[29] Волков Б.С. Детерминистическая природа преступного поведения. – Казань: Издат-во Казанского унив-та, 1975. – С. 39–40.
[30] Никулин С.И., Чугаев А.П. О проекте УК РФ // Государство и право. – 1992. – No 7. – С. 94.

– это активный, осознанный, волевой акт внешнего проявления поведения, который выражается в совершении общественно опасного посягательства, предусмотренного уголовным законом. Уголовно-правовое бездействие – это общественно опасное, волевое поведение, которое по сути является невыполнением лицом своих юридических обязанностей.

Важной характерной чертой каждого преступления является его общественная опасность. Действие, которое не имеет общественной опасности, не может быть объективной стороной состава преступления. По своим объективным признакам любое преступление является общественно-опасным деянием, поскольку в нем находит свое выражение посягательство на определенные общественные отношения. То есть, общественная опасность – это свойство уголовно-правового деяния в целом, это его объективное свойство[31].

Действительно большой вред причиняется общественным отношениям преступлениями в сфере использования электронно - вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи, в частности, данный вред может быть причинен действиями, характер которых определяется свойствами самого объекта, например, незаконное вмешательство в работу ЭВМ, компьютеров и компьютерных сетей и сетей электросвязи возможно только с использованием ЭВМ.

Говоря о противоправности действия в уголовно-правовом смысле слова, мы, с одной стороны, имеем в виду действие, содержащее в себе совокупность всех признаков, указанные в законодательном определении преступления, а с другой, исходим из того, что противоправность действия в уголовном праве является только юридическим выражением его общественной опасности.

Указывая на сложный характер действия, закон определяет, какое именно действие является общественно опасным, то есть, определяет конкретность

[31] Гришаев П.И. Советское уголовное право. Объективная сторона. Часть Общая. Выпуск 7. – М.: Мин-во высшего и среднего образования РСФСР. Всесоюзныи□ юридическии□ заочныи□ институт, 1961. – С. 12.

содержания действия. Иногда в законе не определяется форма действия, то есть любое действие может быть признано признаком состава преступления. Решающее значение в этом случае имеет степень тяжести совершенного преступления, то есть, размер ущерба, причиненного объекту. Признаками общественной опасности и противоправности характеризуются как действие, так и бездействие лица.

При определенных обстоятельствах, бездействие лица не является «ничем», а является определенным поведением. Общественная опасность – это материальная характеристика действия, противоправность – правовая характеристика, которую часто называют формальной в том смысле, что она является юридической формой своего материального содержания – общественной опасности. В.М. Кудрявцев определяет преступное действие как общественно опасный в данных условиях места, времени и обстоятельств противоправный акт внешнего поведения лица. При этом под внешней понимается поведение под контролем сознания и то, что осуществляется собственным движением тела данного лица[32]. Вообще, категория «общественно опасное поведение» может рассматриваться в двух аспектах: содержательном (с точки зрения отражения ею общественно опасного поведения, как социального явления в целом) и прикладном (в плане использование в научном, законотворческом процессе представления, отображения и оценки реалий антисоциального поведения).

В.В. Мальцев выделяет три формы отражения и оценки общественно опасного поведения в уголовном праве: конкретно-юридический, абстрактно-юридическую и абстрактно-социолого-правовую[33].

Первая форма – общественно-опасное поведение – отражается в уголовном праве через все множество установленных законодателем разновидностей конкретных преступлений. Вторая форма – такое поведение

[32] Кудрявцев В.Н. Объективная сторона преступления. – М.: Гос.издат. юрид. лит., 1960. – С. 71.
[33] Мальцев В.В. Категория «общественно опасное поведение» и ее уголовно-правовое значение // Государство и право. – 1995. – 9. – С. 59.

отражается через формулирование общей законодательной концепции преступления, и такое, что вбирает в себя понятие преступления, определяя его более важные признаки, стадии совершения, характер участия его субъектов и обстоятельства, исключающие общественную опасность деяния. Третья форма изучает соотношение общественно опасного поведения с признаками уголовного закона. Когда идет речь об общественной опасности «компьютерных преступлений», то имеют в виду тот вред, который причиняется интересам общества, которые охраняются. Если ущерб уже имеет место, то вернее было бы говорить не об опасности деяния, а его тяжести.

Способ действия – определенный порядок, метод, последовательность движений и приемов, применяемых лицом. Способ – объективная характеристика действия, не зависящая от того, с какой формой вины оно совершено. Средства совершения преступления и орудие совершения деяния – это материальные предметы, которые использует преступник для воплощения своей цели. При характеристике объективной стороны уголовный закон в некоторых случаях дает специальное указание о времени и месте совершения преступления, поэтому, что способ, место, время, средства, обстановка существенно влияют на степень общественной опасности деяния. В таких случаях они указываются в диспозиции уголовного закона и приобретают значение обязательных признаков состава преступления. Способ, как признак объективной стороны преступления, принадлежит непосредственно действию или бездействию, и придает им качественную определенность, уточняет, конкретизирует их, вследствие чего преступное действие или бездействие наделяется устойчивыми индивидуальными признаками, которые отличают ее от других деяний. В данном случае, установление способа в каждом конкретном преступлении имеет важное значение как тогда, когда он указан в законе и является непосредственным признаком состава преступления, так и тогда, когда в законе способ не указан.

Способ совершения преступления имеет влияние на субъективная сторона преступления по типу обратной связи: субъективная сторона в

некоторой степени определяется способом совершения преступления. Формирование мотивов, целей совершения преступления осуществляется на базе и с учетом внешних объективных условий, в которых действует лицо и позволяющие осуществить действие (бездействие) определенным способом.

Таким образом, принимая решение о совершении преступления лицо избирает и возможный способ его осуществления. Способ и объект «компьютерных преступлений» находятся между собой в тесной связи, поскольку способ определяется объектом преступления. Образ всегда выступает как средство совершения преступного посягательства на объект, он обеспечивает выполнение действий, которые составляют объективную сторону преступления.

При рассмотрении вопроса о последствиях конкретного общественно опасного действия или бездействия лица следует установить, причинило ли данное общественно опасное последствие именно этим действием или бездействием лица. Если причинная связь между действиями (бездействием) и преступными последствиями отсутствует, лицо несет ответственность только за фактически совершенное деяние (бездействие).

Каждое преступление всегда причиняет вред общественным отношениям, охраняемым законом. Способность деяния причинять вред объекту посягательства или создавать реальную возможность причинения такого вреда является основанием отнесения определенных действий к преступным. Объективным следствием любого преступления всегда является причинение или возможность причинения вреда интересам, охраняемым законом. Если проанализировать систему преступлений по уголовному законодательству, можно сделать вывод, что большинство преступлений имеют несколько последствий, причиняют вред не одной группе общественных отношений.

Второй элемент всегда имеет место, потому что именно из-за правовой формы осуществляется нарушение охраняемого блага. Кроме этих двух элементов, может существовать и третий, а именно: материальный элемент, который не является определяющим, так как причинение вреда предмету

преступления еще не дает полной информации о решении вопроса относительно объекта преступного посягательства. Преступным результатом (последствиями) являются такие предусмотренные уголовным законом изменения, причиняемых действием или бездействием. Такие последствия могут иметь материальный или нематериальный характер.

Материальными последствиями он называет причинения потерпевшему материального ущерба, физическими – причинение вреда здоровью и жизни человека, моральные касаются преступлений, которые посягают на честь и достоинство, а политические имеют место при нарушении субъективных прав граждан. А.Н.Игнатов и Ю.А.Красиков среди последствий выделяют еще престиж власти и государственного аппарата: взяточничество, превышение власти или служебных полномочий[34].

Реальная возможность наступления вредных последствий является результатом каждого преступного деяния. В одних случаях эта возможность заключается исключительно в самом преступном деянии, в других – в дальнейших изменениях в состоянии объективной действительности, вызванные деянием. Поэтому реальная возможность наступления вредных последствий зависит от конкретных особенностей преступления. Для установления «значимости» последствий следует отталкиваться от признаков, определяющих характер общественной опасности причиненного вреда.

Вообще, стоит заметить, что материальные и физические последствия доминируют над другими. Такой вывод дает система Уголовного РФ. Материальные последствия по содержанию являются наиболее распространенными.

Что касается «компьютерных преступлений», то в данном случае определение материальных последствий имеет свою специфику. Определение существенности причиненного вреда, как квалифицирующего признака зависит от многих обстоятельств и определения денежного предела не имеет. Следует

[34] Уголовное право России. Учебник для ВУЗов. В 2-х т. / Ответств. Редакторы Игнатов А.Н., Красиков Ю.А. – М.: Издат. Группа НОРМА–ИНФРА М, 1999. – Т. 1. – С. 130.

учитывать, что именно произошло в результате совершения «компьютерного преступления», какие убытки понесли владельцы, пользователи, распорядители АС и их деловые партнеры, сколько было потрачено средств на ремонт машин, ликвидацию вируса, восстановление программ, как определяются размеры упущенной выгоды. Считается, что при расчетах не должны учитываться затраты на установление технической защиты от несанкционированного доступа к информации и ее сокрытие. Ценность объекта должна учитываться при определении опасности преступных последствий.

Отсутствие вредных последствий означает, что деяние не имеет признаков преступного и приобретает содержания административного, дисциплинарного или просто аморального проступка. Полное отсутствие вредных последствий порой имеет место и при приготовлении к преступлению, когда преступные последствия отсутствуют при условии, что не зависят от субъекта, а потому лицо будет нести уголовную ответственность на общих основаниях.

Вообще, наступление указанных в законе последствий в отношении «компьютерных преступлений» является свидетельством законченного материального состава преступления и обстоятельства, придает преступлению квалифицированного вида. Моральные последствия имеют место при посягательстве на честь и достоинство лица, а также при любом нарушении прав человека, где виновный всегда своими действиями выражает неуважение к законных интересов лица, чьи права он нарушает. Поэтому, при совершении компьютерного преступления субъект, кроме материального вреда, причиняет и моральный вред. Именно пренебрежение права другого лица на сохранение информации и является содержанием морального вреда преступления. Отличием морального вреда от любой другой является возможность его возмещения в порядке гражданского производства, то есть, по гражданскому иску. Размер морального вреда законодательно не ограничен, так как права человека-явления нематериальные, их нельзя измерить, посчитать, невозможно определить объем нарушения чести или достоинства. Политические

последствия имеют место в том случае, когда виновное лицо посягает или на установленный в государстве строй, или на права граждан, что может привести к политическим последствиям глобального характера.

Соответственно объективная сторона совершения преступления в значительной мере отражает общественную опасность преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи и является важным фактором при квалификации данного вида преступлений.

«Статья 272 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации, если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы вычислительных систем»[35].

В статья 272 УК РФ довольно четко описывает объект, объективную сторону, субъект данного преступления. Опираясь на диспозицию данной статьи можно выделить следующие обязательные признаки объективной стороны преступления: копирование информации, приведшее к ее блокированию, модификации или уничтожению. Обязательно наличие причинно-следственной связи между неправомерными действиями в отношении защищаемой информации и наступившими последствиями.

«Преступление, предусмотренное ст.272 считается оконченным с момента наступления общественно опасных последствий. Причины совершения данного преступления могут быть любыми: корыстные мотивы, проверка собственного профессионализма, месть и др. Объектом преступного посягательства являются общественные отношения, связанные с безопасностью использования компьютерной информации»[36].

Объективная сторона преступления может быть осуществлена с использование специальных технических или программных средств, действующих учетных данных пользователей, хищения цифровых носителей

[35] Козлов В.Е.Теория и практика борьбы с компьютерной преступностью – М., Горячая линия, Телеком, 2012. – С. 13.
[36] Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность, 1997. – № 1. – С. 8

информации (при условии организации охраны этих носителей). В качестве предмета преступного посягательства выступает компьютерная информация.

Ответственность за создание различного вредоносного программного обеспечения предусмотрена статьей 273 УК РФ.

Состав данного преступления (по части 1) является усеченным по признаку «создания программ для ЭВМ или внесения изменений в существующие программы» Безопасные общественные отношения, связанные с использованием ЭВМ, программного обеспечения являются непосредственным объектом данного преступления. Часть 1 ст.273 представляет собой формальный состав, характеризующийся закрытым перечнем совершаемых действий. К этим действиям законодатель относит создание программ, внесение изменений обладающих схожими функциями в готовые программные продукты, распространением вредоносных программ, использование носителей, содержащих такие программы, распространение этих носителей.

Объективную сторону преступления, предусмотренного ст.273 УК РФ, составляют следующие неправомерные действия.

1) Создание программ для ЭВМ, заведомо приводящих к общественно опасным последствиям.

2) Внесение изменений в существующие программ для ЭВМ, заведомо приводящих к общественно опасным последствиям.

3) Использование таких программ или машинных носителей с такими программами.

4) Распространение таких программ или машинных носителей с такими программами.

«При этом следует обратить внимание на то, что, согласно буквы и смысла закона, состав преступления, предусмотренный ч.1. ст.273 УК, сконструирован как формальный. Следовательно, для признания преступления оконченным не требуется реального наступления вредных последствий в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Достаточно установить сам факт совершения общественно опасного деяния, если оно создавало реальную угрозу наступления альтернативно перечисленных выше вредных

последствий. В том случае, когда виновный умышленно создает вредоносную программу для ЭВМ или вносит изменения в существующую программу, доводя ее до качества вредоносной, а равно использует либо распространяет такие программы или машинные носители с такими программами и при этом не совершает неправомерного доступа к охраняемой законом компьютерной информации, то его действия подлежат квалификации по ст.273 УК»[37].

Выход из строя одной из компьютерных систем может, в конечном счете, привести к трагедии в связи с этим законодатель уделил особое внимание безопасности ЭВМ, систем ЭВМ или их сетей, установив уголовную ответственность за нарушение правил их эксплуатации. Данный состав преступления размещен в ст. 274 УК РФ.

Состав части 1 статьи сформулирован как материальный.

При этом общественно опасные последствия заключаются в одновременном наличии двух факторов:

- уничтожения, блокирования или модификации охраняемой законом информации ЭВМ;

- вызванного этим существенного вреда. Необходимо учитывать, что поскольку речь идет о правилах эксплуатации именно ЭВМ, т.е. программно-аппаратной структуры, то и нарушение их должно затрагивать только техническую сторону несоблюдения требований безопасности компьютерной информации, а не организационную или правовую.

Объективная сторона данного преступления состоит в нарушении правил эксплуатации ЭВМ и характеризуется:

1) Общественно опасным деянием (действием или бездействием), которое заключается в нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети.

2) Наступлением общественно опасных последствий в виде уничтожения блокирования или модификации компьютерной информации, причинивших существенный вред или повлекших по неосторожности тяжкие последствия.

---

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

3) Наличием причинной связи между действием и наступившими последствиями.

При описании объективной стороны данного вида общественно опасных посягательств законодатель использует бланкетный способ: указание в диспозиции статьи на действие (бездействие) носит общий характер – «нарушение правил». Конкретное содержание этих правил раскрывается в нормативных актах других отраслей права. Правила эксплуатации ЭВМ могут быть предусмотрены как в общих требованиях по технике безопасности и эксплуатации ЭВМ и периферийных устройств, так и в специальных правилах и инструкциях, регламентирующих особые условия эксплуатации ЭВМ (например, продолжительность работы и последовательность операций).

2.2 Субъективные признаки преступлений в сфере компьютерной информации

Диспозиция ст.272 УК РФ не содержит в себе указания на форму вины, однако в данном случае с уверенностью можно говорить об умысле (прямом или косвенном). В случае совершения данного состава преступления лицо осознает, что его действия носят неправомерный характер, предвидит или может предвидеть наступления общественно опасных последствий, но при этом допускает их наступление.

«Неправомерный доступ к компьютерной информации - умышленное деяние, поскольку в диспозиции ст.272 УК не указано обратное»[38].

«По общему правилу, ответственность за совершение преступлений, предусмотренных статьей 272 УК РФ наступает с 16 лет, однако часть вторая ст.272 предусматривает наличие специального субъекта, совершившего данное преступление»[39].

[38] Постатейный Комментарий к Уголовному кодексу РФ / под ред. Наумова А.В. – М., 2015 – С. 330.
[39] Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция, 1997. – №10.

В преступлении, предусмотренном ст.272 УК, неправомерный доступ к компьютерной информации осуществляется следующими лицами:

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

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

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

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

При анализе данного состава преступления необходимо обратиться к ч.2 ст.72 УК РФ, говорящей о том, что деяние признается совершенным по неосторожности, лишь в том случае, когда это оговорено соответствующей нормой УК РФ. Это подтверждает нашу точку зрения касательно того, что преступления предусмотренные ст.273 УК РФ совершаются исключительно с формой вины в виде прямого умысла.

Для объективной стороны ч.1 ст.273 необходимо наличие двух признаков: наличие вредоносной программы или изменений в программе, несанкционированность последствий.

Субъект преступления - общий, т.е. субъектом данного преступления может быть любой гражданин, достигший шестнадцати лет.

Субъективную сторону части 1 ст.274 данной статьи характеризует наличие умысла направленного на нарушение правил эксплуатации ЭВМ. В случае наступления тяжких последствий ответственность по части 2 ст.274 наступает только в случае неосторожных действий. Умышленное нарушение правил эксплуатации ЭВМ, систем ЭВМ и их сети влечет уголовную ответственность в соответствии с наступившими последствиями и нарушение правил эксплуатации в данном случае становится способом совершения преступления. Субъект данного преступления - специальный, это лицо в силу

должностных обязанностей имеющее доступ к ЭВМ, системе ЭВМ и их сети и обязанное соблюдать установленные для них правила эксплуатации. Часть 2 - состав с двумя формами вины, предусматривающий в качестве квалифицирующего признака наступление по неосторожности тяжких последствий. Содержание последних, очевидно, аналогично таковому для ч.2 ст.273.

Современный уровень технологий способствует тому, что хакеры специализировались в отдельных направлениях. Такая специализация дает возможность выделить в общей массе хакеров «группы по интересам», например «крекеров» (cracker) - специалистов по обхождению механизмов безопасности; «кранчеров» (cruncher) - специалистов по знатью с программного обеспечения защиты от копирования; «крешеров» (cruncher) - любители активно экспериментировать с компьютерной системой с целью исследования возможностей управления ею. В зависимости от предмета деятельности, хакеров можно разделить на три группы: Software hackers, софтверные хакеры, занимаются тем, что «взламывают» программное обеспечение. Это даже сам много многочисленная группа хакеров, и ущерб от деятельности этих людей измеряется миллионами долларов.

Phreks, по определению фрикер - это лицо, что предпочитает «альтернативным» способам оплаты теле - и прочих коммуникационных услуг (например, заставит заплати за телефон соседа вместо себя, если на телефоне стоит блокиратор). В последнее время среди фрикеров появился новый слой - carders. Кардеры - это лица, которые перепрограммировать телефонные карты таким образом, что на карте открывается практически безграничный кредит на телефонные разговоры. Это, пожалуй, самые более опасная часть фрикеров. Они имеют глубокие знания в области радиоэлектроники и программирования микросхем.

Поскольку они потенциально могут принести большой вред, за их действиями внимательно следят специальные службы. Net hacers - эта группа людей отделилась от фрикеров, когда начали активно развиваться технологии в

сетях. Сетевой хакер должен очень хорошо разбираться в сетях связи и способах их защиты. Сетевые хакеры взламывают защиту серверов Интернет, атакуют государственные и корпоративные информационные системы. Цель атак может быть разной, вплоть до промышленного шпионажа по заказу конкурирующих кампаний.

Важными современными задачами правовой науки, нормотворчества и правоохранительной деятельности является создание гарантий сбалансированного соотношения интересов личности и государства в борьбе с преступностью.

Глава 3. Некоторые проблемы, связанные с квалификацией компьютерных преступлений

Одним из проблемных вопросов квалификации преступлений со сложными составами является, в частности, вопрос о том, охватываются ли ими перечисленные простые составы либо требуется квалификация по совокупности. В юридической литературе отмечается, что «составляющие сложные составные деяния не могут выходить за пределы родового объекта посягательства и быть по категории и связанной с ней наказуемостью опаснее, нежели единое сложное преступление»[40].

Поэтому будет ли правомерным пиратское тиражирование компьютерных программ квалифицировать только по ст. 146 УК РФ либо хищение денежных средств с использованием компьютерных сетей - только по ст. 159 или 158 УК РФ даже при наличии в этих статьях такого квалифицирующего признака, как использование компьютерных средств.

При незаконном проникновении в компьютерную сеть и модификации или копировании охраняемой информации преступник не только посягает на отношения собственности или личности, но и нарушает информационную безопасность, которая является видовым объектом по отношению к родовому - общественной безопасности. Этот объект не охватывается составами преступлений против собственности, государства или личности. Ведь если лицо совершает какое-то деяние с использованием оружия, то в большинстве случаев речь пойдет о квалификации по совокупности этого преступления и незаконного ношения (хранения и т.п.) оружия, так как в данном случае страдает еще один объект - отношения общественной безопасности.

Таким образом, представляется, что при посягательстве на различные объекты (собственность, права граждан, государственная безопасность и т.п.), совершенном посредством компьютера или компьютерных сетей, при реальном

[40] Кузнецова Н.Ф. Квалификация сложных составов преступлений // Уголовное право. – 2000. – № 1. – С. 26.

выполнении виновным нескольких составов квалификация должна осуществляться по совокупности соответствующих статей, предусматривающих ответственность за преступления против собственности, прав граждан и т.п., и статей, предусмотренных гл. 28 УК РФ.

Точно так же необходимо поступать и в случаях с компьютерным пиратством.

Анализ корыстных преступлений, совершаемых с использованием компьютеров, и конструкций статей УК РФ, содержащихся в гл. 21, 28 и в отдельных статьях некоторых других глав (например, ст.201), позволяет сделать вывод о многообъектности указанных преступных посягательств и, следовательно, о сложности их квалификации В ряде случаев проникновение в компьютерные сети и доступ к нужной информации осуществляется с помощью различных технических средств. В результате преступники получают возможность снимать с компьютерных счетов клиентов наличные деньги любой валюте. Совершению этих преступлений также предшествует определенная подготовка, характер которой зависит от степени связей правонарушителей с деятельностью вычислительного центра банка. Посторонние лица продумывают пути доступа к компьютерной системе, пытаются выяснить пароли и ключи программ. Программисты, операторы и другие работники компьютерного центра либо других подразделений банка, замышляющие подобную аферу, выбирают наиболее благоприятную для ее совершения обстановку, могут создать подставную фирму с расчетным счетом для «перекачивания» похищенных денег и т.д.

В этих условиях возникает проблема отграничения хищений от преступлений, предусмотренных в гл. 28 УК РФ.

«Представляется, что злоумышленники, совершающие действия, предусмотренные диспозициями ст. 272-274 УК РФ, и не имеющие корыстной цели, а преследующие, допустим, исследовательский интерес, должны наказываться именно по этим статьям при условии наступления указанных в них последствий. Если же лицо, преодолев системы защиты компьютерной

информации, подобрав пароли и ключи, проникло в компьютерную сеть банка и внесло в нее определенные изменения, а затем внесение таких изменений позволило ему перевести на свои счета денежные средства, то в этом случае по ныне действующему законодательству его действия необходимо будет квалифицировать по совокупности ст. 272 УК РФ и статьи, предусматривающей ответственность за хищение. Некоторые авторы безапелляционно утверждают, что хищение в данном случае происходит в форме мошенничества»[41].

Этот вопрос можно считать дискуссионным. В строгом значении этого слова злоумышленник обманывает не потерпевшего, а компьютер, компьютерную систему.

Мировые экономические процессы на современном этапе все больше смещаются в сторону киберпространства. Ведь его применение как инструмента ведение бизнеса дает возможность значительно повысить прибыли. Вместе с тем можно наблюдать и сдвиги криминального элемента в сторону этого виртуального среды, значительную часть которого составляет всемирная сеть. Такому продвижению нередко способствует определенная анонимность, которой можно добиться в сети. Поэтому сегодня в Интернете появляется большое количество данных, содержащих признаки правонарушений.

Нередки случаи продажи наркотических средств, огнестрельного и холодного оружия, распространение порнографических предметов через Интернет. Кроме перечисленных общеуголовных преступлений особого вреда наносят высокотехнологичные правонарушениях, среди которых взлома систем дистанционного банковского обслуживания, заказные DDOS-атаки на электронные ресурсы, взлом и мошенничество с телекоммуникационными системами операторов связи.

[41] Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция. – 1999. – № 1. – С. 44-45.

Оценка криминогенной обстановки в киберсфере дает основания к принятию решительных мер по стороны правоохранителей всего мира с целью ее улучшение, уменьшение риска для рядовых граждан попасть в ловушку киберпреступников.

Вопросы противодействия киберпреступности на мировом уровне является объектом внимания значительной части ученых и практиков, среди которых можно выделить отечественных специалистов. М. Бутузова, И. А. Воронова, В. А. Голубева, Н. В. Гуцалюка, В. П. Захарова, А. В. Манжая, Ю. Ю. Орлова, Е. В. Рыжкова, Ю. В. Степанова, В. П. Шеломенцева и др.

Следует констатировать, что наиболее значимые достижения в сфере борьбы с киберпреступностью на сегодня имеют Великобритания (Serious and Organised Crime Agency), Китай (People's Police), Германия (Bundeskriminalamt), Российская Федерация (Управление К), США (Federal Bureau of Investigation), Франция (Office central de lutte contre la criminalite liee aux technologies de l'information et de la communication), Япония (National Police Agency).

В последнее время в УБК было накоплено много информации о контингенте лиц, причастных к организации и совершению киберпреступлений. В соответствующем банке данных есть не только граждане РФ, в последние годы количество иностранных граждан также существенно возросла. Это подчеркивает необходимость широкого международного сотрудничества[42].

Во многих странах разработана и активно применяется нормативно-правовая база, посвященная вопросам борьбы с киберпреступностью. Как правило, соответствующие нормы изложены в нескольких законодательных, а также подзаконных актах, имеющих ведомственный или межведомственный характер. Примером последних является Online Investigative Principles for Federal Law Enforcement Agents 1999 г., FBI Domestic Investigations and

[42] Литвинов М. Деятельность управления по борьбе с киберпреступностью на современном этапе [Електронний ресурс] / Максим Литвинов. – Режим доступу: http://cybersafetyunit.com/deyatelnost-upravleniya-po-borbe-s-kiberprestupnostyu-mvd-ukrainyi-na-sovremennom-etape/. – (дата обращения 17.04.2019)

Operations Guide от 15.10.2011 (США), Постановление Государственного Совета КНР от 20.09.2000 № 292 «Мероприятия по управление сферой Интернет-услуг» и тому подобное.

В Германии вопросам борьбы с киберпреступностью посвящен § 20k Закона «О федеральное управление уголовной полиции и сотрудничество федерации и земель по уголовным делам» от 07.07.1997, согласно которому в отдельных случаях разрешается проводить санкционированный негласный онлайн-обыск.

В Китае в. 11 Закона КНР «Об органах государственной безопасности» от 22.02.1993[43] и ст. 6 Закона КНР «О народной полиции» от 28.02.1995[44] также косвенно затрагивают проблемы кибербезопасности. Тоже самое касается Regulation of Investigatory Powers Act (Великобритания), Copyright Act, Act on Punishment of Activities Relating to Child Prostitution and Child Pornography (Япония).

Подразделения борьбы с киберпреступностью участвуют в формировании и обеспечении реализации государственной политики по предупреждению и противодействию криминальным правонарушением, механизм подготовки, совершения или сокрытия которых предполагает использование электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи, а также другим уголовным правонарушением, содеянным с их использованием (сфера борьбы с киберпреступностью).

Проблема качественной подготовки кадров для подразделений борьбы с киберпреступностью является характерной не только для РФ. Например, в Германии соответствующих специалистов подбирают с числа выпускников

[43] State Security Law of the People's Republic of China : of 22.02.1993 No. 6 [Електронний ресурс]. – Режим доступу: http://en.pkulaw.cn/display.aspx?id=530&lib=law&SearchKeyword=state%20security&SearchCKeyword=(дата обращения 17.04.2019)

[44] People's Police Law of the People's Republic of China : of 28.02.1995 No. 40 [Електронний ресурс]. – Режим доступу: http://en.pkulaw.cn/display.aspx?id=123&lib=law&SearchKeyword=&SearchCKeyword=.(дата обращения 17.04.2019)

технических вузов, в Российской Федерации их готовит Московский университет МВД России по специальности «Информационная безопасность», в США для подготовки таких специалистов существуют специализированные курсы в Академии ФБР.

Проанализировав деятельность государственных органов различных стран в сфере борьбы с киберпреступностью, хотелось бы обозначить ряд наиболее актуальных вопросов в этой сфере, которые требуют решения. Во-первых, это международное нормирование отношений в киберпространстве и особого порядка взаимодействия правоохранительных органов различных стран в сфере кибербезопасности между собой и с представителями частных структур, деятельность которых связана с предоставлением услуг через сеть Интернет или в сфере коммуникаций. Во-вторых, формирование подразделениями борьбы с киберпреступностью качественного личного состава высокой квалификации, способного эффективно противодействовать киберпреступности. И, во-третьих, это разработка специализированного программного обеспечения.

Проблема неправомерного доступа к компьютерной информации становится все актуальнее в наши дни в связи с ростом информационных технологий и роботизацией нашей повседневной жизни. Многие люди ведут деловую переписку, хранят персональные данные и сведения, представляющие коммерческую тайну в электронном виде на своих компьютерах или на просторах интернета. Это существенно упрощает возможность заинтересованных лиц незаконно ознакомиться с интересующей их информацией.

Заключение

Результаты проведенного нами исследования позволяют сформулировать следующие основные выводы, рекомендации и предложения, что, сделают, по мнению диссертанта, определенный вклад в общую теорию науки криминалистики, а также в практическую деятельность по выявлению, расследованию преступлений, связанных с использованием информационных компьютерных технологий:

Преступления в сфере компьютерных технологий представляют собой одно из сложных антисоциальных явлений в обществе. Грамотное расследование преступлений, в частности противоправных действий, связанных с использованием высоких компьютерных технологий – один из ключевых вопросов для любого государства, в том числе и для РФ. Международный характер противодействия этому феномену современности – залог дальнейшей стабильности и развития всех сфер человеческого бытия.

Основанием для возбуждения уголовного дела о совершенном преступлении, в том числе и компьютерный, есть достаточные данные, указывающие на наличие признаков состава преступления. Исходя из содержания уголовно-правовой характеристики, компьютер и его программное обеспечение может быть, как предметом преступления, так и средством, с помощью которого реализуется замысел преступника.

Криминалистическая характеристика преступлений в сфере компьютерных технологий является обобщенной информационной моделью, что представляет собой систематизированное описание типичных криминалистических значимых признаков, которые имеют существенное значение для выявления и расследования компьютерных преступлений. С учетом недостаточности знаний практических работников правоохранительных органов, на которых возлагается задача расследовать нетрадиционные

преступления, считаем целесообразным детализированный подход к формированию элементов ее криминалистической характеристики. В частности, она должна состоять из таких структурных элементов:

• способы совершения преступлений данной категории;

• следовая картина этих преступлений;

• личность преступника, мотивы и цель совершения преступления;

• некоторые обстоятельства совершения преступления (место, время, обстановка).

а) Способы совершения преступлений данной категории предложены Ю.М. Батуриным и изложены в пяти группах, больше отражают способы противоправных действий, чем способы совершения компьютерных преступлений. По мнению диссертанта, их содержание должно быть изложено таким образом:

• способы непосредственного доступа к компьютерной информации или операционной системы;

• способы удаленного (опосредованного) доступа;

• способы изготовление, распространение на технических носителях вредоносных программ для ЭВМ.

б) Следовая картина этих преступлений. Ее можно рассматривать как совокупность абстрагированной информации о типичные материальные и идеальные следы-признаки и условия совершения субъектом противоправных действий с использованием компьютерных технологий:

• Следовая картина незаконного вмешательства в работу электронно-вычислительных машин (компьютеров), систем и компьютерных сетей.

• Следовая картина похищение, присвоение, вымогательство компьютерной информации или завладение ею путем мошенничества или злоупотребления служебным положением.

• Следовая картина нарушение правил эксплуатации автоматизированных электронно-вычислительных систем.

в) Личность преступника, мотивы и цель совершения преступления. По статистическим данным отечественной и зарубежной практик, возраст лиц, совершающих компьютерные преступления, достигает от 15 до 45 лет. Материалы экспертных исследований определяют, что на момент совершения противоправных действий возраст 33 % преступников не превышал 20 лет; 13 % – были старше 40 лет; 54 % имели возраст от 20 до 40 лет.

Мотивы и цель совершенного преступления. Они зависят от многих факторов, в частности, на что именно была направлена противоправное действие. Исходя из анализа мировой и отечественной практик, их можно построить в такой последовательности:

• корыстные – на долю которых приходится 66 % компьютерных преступлений;

• политические – 17 % (шпионажа, подрыв финансово-экономической деятельности и кредитной политики);

• любопытство, любознательность – 7 %;

• хулиганские намерения – 5 %;

• месть – 5 %.

г) Некоторые обстоятельства совершения преступления (место, время, обстановка). Особенностью компьютерных преступлений является то, что место, откуда было совершено противоправное действие (место, где выполнялись действия объективной стороны состава преступления) и место наступления вредных последствий (место, где наступил результат преступления) могут не совпадать. Таким местом может быть любое помещение различной формы собственности, в котором находится компьютерно-техническое оснащение, обеспеченное выходом к глобальной сети типа Интернет. Время совершения противоправных действий с компьютерными технологиями всегда конкретно определен.

С целью оказания практической помощи следователю в решении организационных вопросов обеспечения первоначального этапа расследования преступлений в сфере информационных компьютерных технологий, автор

предлагает некоторые рекомендации, касающиеся подготовки и проведения процессуальных мероприятий. В тактике следственных действий расследование компьютерных преступлений есть свои особенности в отличие от традиционных видов преступлений, в частности:

а) подготовительный этап должен состоять из двух этапов: до выезда на следственный осмотр и действия на месте происшествия до начала рабочего этапа. Особая роль на этом этапе должна отводиться оперативно-розыскной деятельности правоохранительных органов и формированию состава рабочей группы, которая будет выезжать на следственное действие;

б) рабочий (исследовательский) этап должен включать общий обзор (статическую) и подробную (динамическое) действия. Видное место на этом этапе отводится работе специалистов с электронными документами, которые могут нести доказательственную информацию о совершенном преступлении;

в) на заключительном этапе проведения следственного действия должно происходить не только грамотное оформление надлежащих процессуальных документов, но и правильность изъятия обнаруженных вещей и предметов доказательного значения, а также обращения с электронными носителями информации.

Принимая во внимание тот факт, что преступления в сфере высоких компьютерных технологий являются нетрадиционными и мало расследованным, диссертант предлагает, как практическую помощь рассмотреть такие типичные следственные ситуации, которые могут сложиться на первоначальном этапе следствия:

• выявлен факт несанкционированного вмешательства в информацию, которая циркулирует в банковской или кредитно-финансовой сфере, но отсутствуют данные о способе совершения преступления и причастных к нему лиц;

• выявлен факт внесения любого плана изменений в компьютерную информацию, при этом способ доступа к базам данных отсутствует или же имеет опосредованный характер, субъект преступления неизвестен;

• выявлен факт внесения изменений в компьютерную информацию, зафиксировано способ доступа к базам данных, отдельных программ, известна вероятная личность преступника;

• выявлен факт внесения в программное обеспечение или отдельные файлы вредных, опасных вирусных программ, способ заражения и личность преступника неизвестны;

• выявлен факт уничтожения информации в компьютерной системе, данные о способе совершения и причастных к преступлению лиц неизвестны;

• выявлен факт похищения (завладения) компьютерной информации, при этом сведения о способе доступа к информации и о субъекте преступления неизвестны;

• выявлен факт модификации баз данных или манипуляции информацией в отдельных программных файлах, данные о способе и о вероятном субъекте известные.

Для эффективного проведения процессуальных следственных мероприятий следственно-оперативная группа должна иметь необходимое техническое оснащение. По нашему мнению, целесообразно, наряду с традиционными криминалистическими чемоданами, ввести специализированное научно-техническое снаряжение для выявления, фиксации и отбора информационных следов на месте совершения преступления. Анализ практики свидетельствует, что среди технических средств, используемого при проведении отдельных следственных действий в преступлениях с компьютерных технологий, наиболее используемыми являются: фотографирование, около – 40 % и видеозапись – 28 %. Специализированное под компьютерную технику и программное обеспечение оснащение используется в 9% случаев, а поисковое оборудование для обнаружения информации и воздействие на нее, в 2 % случаев.

Учитывая, что основу организации расследования преступлений, в том числе и указанной категории, составляет планирование, а оно осуществляется, исходя из криминалистических версий, автор предлагает несколько типовых

версий, которые могут применяться работниками правоохранительных органов при расследовании уголовных дел в сфере информационных компьютерных технологий, в частности:

• компьютерный преступление совершено с целью получения материального вознаграждения ради наживы;

• нарушение работы автоматизированных систем путем уничтожения информации, модификации компьютерных программ, блокировка работы технического оснащения операционных систем;

• распространение конфиденциальной информации и нарушении авторских прав.

В рамках соблюдения процессуальных норм, кроме традиционного ведения протокола допроса, целесообразно использовать другие технические средства фиксации информации (аудио-, видеозаписывающие устройства). Вместе с тем на стадии свободного рассказа допустим следственном приостанавливать допрашиваемого субъекта при условии использования им компьютерно-технической терминологии, с целью избежания недоразумений и неточностей при оформлении процессуального документа, а также неправильного восприятия следователем отдельного факта события, расследуется. Особенно это может касаться допроса операторов, программистов-компьютерщиков, системников, персонала который обслуживает компьютерное обеспечение и др.

10. Тактика проведения обыска и выемки объектов доказательного значения на последующем этапе расследования указанной категории преступлений должна соответствовать следующим критериям:

• психологической настроенности следователя на проведение процессуального действия;

• умению не реагировать на признаки некоторой неопределенности, недостаточной уверенности, предчувствие отсутствия результативности проведения следственного мероприятия;

• определению оптимальных условий (места, времени, обстановки, обстоятельств) успешной реализации следственных действий;

• выбору и применению предупредительной формы или фактора внезапности во время обыска, выемки на месте совершения преступления;

• особенностям использования традиционных технических средств (магнитных искателей и тому подобное) при выявлении соответствующих тайников во время проведения отдельных следственных действий.

Проблема неправомерного доступа к компьютерной информации становится все актуальнее в наши дни в связи с ростом информационных технологий и роботизацией нашей повседневной жизни. Многие люди ведут деловую переписку, хранят персональные данные и сведения, представляющие коммерческую тайну в электронном виде на своих компьютерах или на просторах интернета. Это упрощает возможность заинтересованных лиц незаконно ознакомиться с интересующей их информацией.

Для того чтобы законодатель мог быстро и правильно реагировать на названные негативные тенденции в отрасли технического прогресса, правовой науке следует тщательно анализировать, искать новые правовые средства, а также разрабатывать научно-практические нормативные рекомендации по устранению таких пробелов в законодательстве.

Одним из таких средств могло бы стать формулирование единого комплексного правового института информационных правонарушений, который включал бы в себя основные понятия, принципы и правовые конструкции, направленные на единое понимание, толкование и правоприменения в этой сфере.

Следовательно, установленный разделение юридической ответственности на уголовную, гражданскую, административную и дисциплинарную не отвечает современным реалиям развития правовой мысли. Несмотря на отсутствие определения понятия «информационная ответственность» в отечественном законодательстве, такая ответственность существует объективно и требует дальнейшего углубленного научного разработку.

Список используемых источников

1.Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 01.04.2019)//Собрание законодательства Российской Федерации от 17 июня 1996 г. N 25 ст. 2954

2.Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 07.12.2011 N 420-ФЗ (последняя редакция)//Собрание законодательства Российской Федерации от 12 декабря 2011 г. N 50 ст. 7362

3.Федеральный закон Российской Федерации информационных технологиях и о защите информации»//// Российская газета. 2006. 29 июля.

4.State Security Law of the People's Republic of China : of 22.02.1993 No. 6 [Электронный ресурс]. – Режим доступу: http://en.pkulaw.cn/display.aspx?id=530&lib=law&SearchKeyword=state%20security&SearchCKeyword=(дата обращения 17.04.2019)

5.People's Police Law of the People's Republic of China : of 28.02.1995 No. 40 [Электронный ресурс]. – Режим доступу: http://en.pkulaw.cn/display.aspx?id=123&lib=law&SearchKeyword=&SearchCKeyword=. (дата обращения 17.04.2019)

6.Бутузов В. М. Документирование преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи при проведении доследственной проверки : наук. практ. пособ. / [В. М. Бутузов, В. Д. Гавловский, Л. П. Скалозуб и др.]. - К. : Вид. дом «Аванпост-Прим», 2010. - 245 с.

7.Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. - М. : Юрид. лит., 1991. - 160 с.

8.Войциховский, А. В. Международное сотрудничество в борьбе с киберпреступностью [Электронный ресурс] // Портал : Национальная библиотека имени В. И. Вернадского. – Режим доступа \www/ URL : http

://www.archive.nbuv.gov.ua/portal/.../PB-4_26.pdf . – (Дата обращения 17.04.2019)

9.Волков Б.С. Детерминистическая природа преступного поведения. – Казань: Издат-во Казанского унив-та, 1975. – С.39–40.

10.Гришаев П.И. Советское уголовное право. Объективная сторона. Часть Общая. Выпуск 7. – М.: Мин-во высшего и среднего образования РСФСР. Всесоюзныи□ юридическии□ заочныи□ институт, 1961.

11.Государственные стратегии кибербезопасности [Электронный ресурс] // Портал : Security Lab. – Режим доступа \www/ URL : http://www.securitylab.ru/analytics/429498.php . (Дата обращения 17.04.2019)

12.Гавловский В.Д., М.В. Гуцалюк, В.С. Цимбалюк Совершенствование информационного законодательства как средство оптимизации противодействия компьютерной преступности // – 2001. – № 3. – С. 20-24.

13.Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция, 1997. – №10.

14.Згадзай О.Э., Казанцев С.Я. Доказательства по делам о преступлениях в сфере компютерной информации: проблемы получения и использования [Электронный ресурс]. – Режим доступа: URL: http://www.crime-research.ru/library/Zgaday.htm. – Название с экрана.(дата обращения 17.04.2019)

15.Коваленко Л.П. Некоторые вопросы относительно правонарушений в информационной сфере / Л.П. Коваленко // Форум права. – 2013. – № 4. – С. 158-167.

16.Кузнецова Н.Ф. Цель и механизм реформы УК // Государство и право. – 1992. – No 6. – С. 14-31.

17.Кудрявцев В.Н. Объективная сторона преступления. – М.: Гос.издат. юрид. лит., 1960. – С.71.

18.Козлов В.Е.Теория и практика борьбы с компьютерной преступностью – М., Горячая линия, Телеком, 2012. – С.13.

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

20.Козлов В. Е. Теория и практика борьбы с компьютерной преступностью / Козлов В. Е. - М. : Горячая линия-Телеком, 2002. - 336 с.

21.Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция. – 1999. – № 1. – С. 44-45.

22.Криминалистика : актуальные проблемы / под ред. Е. И. Зуева. - М., 1988. с.120

23.Липкан В.А. Правовой режим налоговой информации: [монография] / [В.А. Липкан, А.В. Шепета, А.А. Мандзюк] ; за заг. ред. В.А. Липкана. – К. : ФОТ О.С. Липкан, 2015. – 404 с.

24.Липкан В.А. Основы развития информационной деликтологии / У.А. Липкан, Ю.Е. Максименко // Право. – 2013. – № 10. – С. 249-256.

25.Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. – 1997. – № 1. – С.19.

26.Литвинов М. Деятельность управления по борьбе с киберпреступностью на современном этапе [Електронний ресурс] / Максим Литвинов. – Режим доступу: http://cybersafetyunit.com/deyatelnost-upravleniya-po-borbe-s-kiberprestupnostyu-mvd-ukrainyi-na-sovremennom-etape/. – (дата обращения 17.04.2019)

27.Максименко Ю.Е. Информационные правонарушения: понятие и признаки / Ю.Е. Максименко // Глобальной организации союзнического лидерства [Электронный ресурс]. – Режим доступа : http://www.goal-int.org/informacijni-pravoporushennyaponyattya-ta-oznaki.(дата обращения 17.04.2019)

28.Мальцев В.В. Категория «общественно опасное поведение» и ее уголовно-правовое значение // Государство и право. – 1995. – 9. – С.59.

29.Никулин С.И., Чугаев А.П. О проекте УК РФ // Государство и право. – 1992. – No 7. – С. 94.

30.Постатейный Комментарий к Уголовному кодексу РФ / под ред. Наумова А.В. – М., 2015 – С.330.

31.Полевой Н. С. Компьютерные технологии в юридической деятельности / Н. С. Полевой, В. В. Крылов. - М. : БЕК, 1994.с.239.

32.Полушкин О.В. О понятии информационного правонарушения / О.В. Полушкин // Российский юридический журнал. – 2009. – № 3. – С. 207–210.

33.Расследование неправомерного доступа к компьютерной информации / под ред. Н. Г Шурухнова. - М. : Щит-М, 1999. -254 с.

34.Тимеи□ко Г.В. Общее учение об объективнои□ стороне преступления. – Ростов-на-Дону: Издат-во унив-та, 1977. – С. 29.

35.Телийчук В.Г. Способы совершения компьютерных преступлений в сфере высоких технологий и меры противодействия / В. Г. Телийчук //Актуальные вопросы юридической науки: теория и практика : материалы междунар. наук.- практ. конф, 11 декабря 2013 г. / КИДМУ КПУ, 2013. – С. 281-284.

36.Уголовное право России. Учебник для ВУЗов. В 2-х т. / Ответств. Редакторы Игнатов А.Н., Красиков Ю.А. – М.: Издат. Группа НОРМА–ИНФРА М, 1999. – Т. 1. – С.130.

37.Усов А.И. Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств [Электронный ресурс]. – Режим доступа: URL: http://jurfak.spb.ru/conference/1810200/usov.htm. – Название с экрана. (дата обращения 17.04.2019)

38.McAfee and Security & Defence Agenda (SDA) Unveil Global Cyber Defense Report [Електронний ресурс] // Портал : An Intel Company. – Режим доступу \www/ URL : http://www.mcafee.com/us/about/news/2012/q1/20120120-01.aspx . – (Дата обращения 17.04.2019)

39.Brenner S. W. Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement? 30 Rutgers Computer & Tech. L.J. 1 (2004).