МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
Кафедра уголовно-правовых дисциплин

Заведующий кафедрой
канд. юрид. наук, доцент,
заслуженный юрист РФ
В.И. Морозов

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
магистерская диссертация

Уголовно-правовая характеристика преступлений в сфере компьютерной информации

40.04.01 Юриспруденция
Магистерская программа «Уголовное право, уголовный процесс»

Выполнил работу
студент 3 курса
заочной формы обучения — Головатюк Владимир Игоревич

Научный руководитель
докт. юрид. наук,
профессор — Шарапов Роман Дмитриевич

Рецензент
начальник кафедры
организации деятельности
охранно-конвойных подразделений
ОВД ТИПК МВД России,
канд. юрид. наук, доцент — Гарманов Виктор Михайлович

Тюмень
2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Фундаментальные принципы коммуникации между группой компьютеров были заложены Агентством Министерства обороны США по перспективным исследованиям в 1969 г. В настоящее время приемник данных принципов - информационно-телекоммуникационная сеть «Интернет», насчитывает количество пользователей свыше 4,5 млрд человек, что составляет более 50 % от всех жителей планеты Земля. Повсеместная популярность цифровой инфраструктуры порождает, новые механизмы коммуникации, в том числе вызывающий преступный умысел у злоумышленников. Таким образом, бурное развитие цифровых технологий должно сопровождаться своевременным реагированием уголовно-процессуальных норм.

По данным ГИАЦ МВД России количество зарегистрированных преступлений в сфере компьютерной информации за последние 5 лет, систематически увеличивается (2016 г. – 1748, 2017 г. – 1883, 2018 г. – 2500, 2019 г. – 2883, 2020 г. – 4498).

Процессы по совершенствованию уголовно-правовых механизмов не прекращаются и по сей день, однако отличительной особенностью рассматриваемых видов преступлений, является трансграничность. В целях решения которой необходимо выработать единый подход к киберпреступлениям в различных правовых система, что на фоне многогранности правовых систем является сложно достижимым.

Объектом исследования, являются общественные отношения в сфере борьбы с преступлениями против компьютерной информации, закрепленные в главе 28 УК РФ.

Предметом исследования вступают нормы уголовного законодательства, регулирующие отношения в сфере использования компьютерной информации, а также судебная практика по уголовным делам о преступлениях, предусмотренных главой 28 УК РФ. Теоретические положения, тенденции

развития и совершенствования методов уголовно-правовой защиты информации, прав и законных интересов её обладателей.

Цели и задачи исследования. Целью настоящего исследования является исследование теоретических вопросов механизма уголовно-правовой защиты информации, прав и законных интересов её обладателей.

Для реализации указанной цели поставлены следующие задачи:

-°Изучить научные подходы к понятию составов преступлений, предусмотренных гл. 28 УК РФ и их соотношение с действующим законодательством РФ;

-°Исследовать правоприменительную практику при рассмотрении судами уголовных дел о преступлениях против компьютерной информации;

-°Обосновать значение понятийного аппарата в области законодательства и доктрины для правоприменительной практики;

-°Выявить недостатки правового регулирования рассматриваемых отношений;

-°Разработать рекомендации, направленные на повышение эффективности механизма уголовно-правовой зашиты информации, прав и законных интересов её обладателей.

Методология исследования. В работе использованы сравнительно-правовой, системно-структурный и формально-логический методы исследования.

Теоретическая база исследования. Конституция РФ и действующее законодательство Российской Фармации, а также иные международно-правовые акты. В работе использованы основные концепции, рассмотренные в монографиях «Уголовно-юрисдикционная деятельность в условиях цифровизации» и «Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования». Также в работе использованы труды таких ученых, как Абов А.И. Алескеров В.И., Айсанов Р.М., Батурин Ю.М., Бачило И.Л., Бойцов А.И., Бородин А.В., Бражник С.Д., Васильев Н.В. и другие ученые.

Эмпирическую базу исследования представляют результаты анализа судебной практики уголовных дел рассматриваемых в рамках главы 28 УК РФ.

Основные положения, выносимые на защиту:

1.°В рамках рассматриваемой уголовно - правовая характеристики преступлений, совершаемых с использованием информационных технологий отличительной особенностью является трансграничность, в связи с чем рассмотрено место совершение преступления в «цифровом пространстве».

2.°На фоне рассмотренных международно-правовых норм и законодательств зарубежных стран сделан вывод об отсутствии единого теоретического подхода к преступлениям в сфере компьютерной информации, в силу различных научных подходов.

3.°Рассмотрены наиболее часто встречающиеся проблемы квалификации преступлений в сфере неправомерного доступа к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; неправомерное воздействие на критическую информационную инфраструктуру российской федерации.

Научно-практическая значимость исследования. В работе развиваются представления о понятии и предмете преступлений, направленных против компьютерной информации, содержащихся в гл. 28 УК РФ. Анализ сложившейся ситуации в соотношении доктрины и закона позволяет сформулировать ряд конкретных практических рекомендаций и предложений, направленных на повышение эффективности борьбы с преступностью в данном направлении.

Апробация результатов исследования. Основные положения магистерской диссертации были изложены в научной статье:

«Развитие отечественных уголовно-правовых мер по противодействию преступлениям в сфере компьютерной информации» // Международный научный журнал «Молодой ученый» №°43°(385), октябрь 2021°г. (стр. 97-98). URL: https://moluch.ru/archive/385/84797/

Структура работы: работа состоит из введения, двух глав, заключения и библиографического списка.

ГЛАВА 1. УГОЛОВНО - ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.

1.1.°Цифровое пространство как место совершения преступлений.

Отличительной особенностью преступлений, предусмотренных главой 28 Уголовного Кодекса Российской Федерации, является место совершения преступления. Злоумышленник может осуществлять противоправные действия из любой точки мира, в том числе с использованием серверов находящихся в-третьих странах. Таким образом любой персональный компьютер и гаджет подключенный к информационно-телекоммуникационной сети «Интернет» может стать жертвой преступления.

Механизм совершения преступления порождает необходимость совершенствования понятийного аппарата. Введение понятия «цифровое пространство» на законодательном уровне, способствовало бы наиболее полной детализации уголовно-правовых механизмов.

Рассмотрим возможность применения имеющихся в уголовном праве принципов действия уголовного закона в пространстве относительно информационно-телекоммуникационной сети «Интернет», для которой характерна децентрализованная система государственного регулирования и трансграничность.

В отечественном праве закреплено понятие «информационное пространство» [Указ Президента Российской Федерации № 203, 2017 г., стр. 7] - совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры. На наш взгляд оно наиболее полно отражает понятие «цифровое пространство», но необходима его детализация, как отдельного цифрового сегмента информации.

В конце 2011 г. в Уголовный кодекс РФ вводится понятие «компьютерная информация» [Уголовный кодекс Российской Федерации № 63-ФЗ,

с. 247] к которому относятся сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В целях наиболее полной формулировки рассмотрим понятие «информационная инфраструктура» [Указ Президента Российской Федерации № 646, с. 6] отраженного в Указе Президента РФ, к которому относится совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории РФ, а также на территориях, находящихся под юрисдикцией РФ или используемых на основании международных договоров РФ.

Таким образом рассмотренные понятия определяют совокупность явлений, выражающихся в действиях объекта уголовного права в цифровом пространстве в совокупности с территориальной привязкой.

Рассмотрим понятие «Интернет», в нормативно правовой литературе не нашло своего отражения, но нормы уголовного законодательства относят его к информационно-телекоммуникационной сети, которой принято считать технологическую систему, предназначенную для передачи по линиям связи информацию, доступ к которой осуществляется с использованием средств вычислительной техники [Федеральный закон № 149-ФЗ, с. 11].

По нашему мнению к «цифровое пространство» следует понимать как совокупность информационных ресурсов, созданных субъектами информационной среды, средств взаимодействия таких субъектов, их информационных систем и сайтов в сети «Интернет» и сетей связи.

Таким образом, детализация понятийного аппарата, путем введения понятия «цифровое пространство» способствовала совершенствованию уголовно-правовых механизмов, в которой затрагиваются интересы нескольких государств осуществляющих коммуникацию между различными субъектами правоотношений в цифровом пространстве.

Стоит также отметить, что в рамках приятого решения Высшего Евразийского экономического совета от 11.12.2020 № 12 «О Стратегических

направлениях развития евразийской экономической интеграции до 2025 года» формированию цифрового пространства отдается наиболее приоритетное направление [Решение Высшего Евразийского экономического совета № 12, с.17].

В обществе юристов не прекращаются дискуссии о понятии «место совершения преступления» [Тимошенко, 2015 г., стр. 37-39], т.к. до настоящего времени оно не нашло отражение в законодательстве. Рассматривая место совершения преступления, через призму цифрового пространства, целесообразно сконцентрировать внимание на пространственных пределах, в совокупности с определением факультативного признака одного из составов преступления. В результате можно выделить следующие подходы:

1)°это место нахождения лица, совершившего преступление;

2)°это место наступления общественно опасных последствий;

3)°это место совершения действия (бездействия), содержащего все признаки состава преступления.

По общим уголовно-правовым принципам, местом совершения преступления признано считать территорию, на которой реализовано общественно опасное деяние и наступили последствия образующие объективную сторону преступления. Применение данного принципа к главе 28 УК РФ затруднительно, т.к. они могут находится на значительном удалении друг от друга.

Выходом из сложившейся ситуации может служить расстановка приоритетов. Рассмотрим понятие время совершения преступления, к которому относится общественно опасное действие (бездействие) независимо от времени наступления общественно опасных последствий [Молодкин, с. 43-48]. В результате можно сделать вывод о расстановке приоритетов, а именно моменте совершения общественно опасного деяния без последствий, категории «место» и «время» неразрывно связаны. Таким образом «местом совершения преступления», следует считать место совершения общественно опасного деяния [Арямов, с. 254-261].

В данном подходе есть и негативная составляющая, так при наступлении общественно опасных последствий на территории Российской Федерации, в ситуации, когда общественно опасное деяние осуществлено на территории иностранного государства, местом совершения преступления должна быть признана иностранная территория.

Вместе с тем, существует и противоположная точка зрения, при которой общественно опасные последствия затрагивающие интересы Российской Федерации должны квалифицироваться в уголовно-правовом порядке отечественного права.

Некоторые ученые выделяют подход, при котором местом совершения преступления с материальным составом следует считать место наступления общественно опасных последствий, а в случаях с формальным – место совершения деяния.

Подводя итоги, местом совершения преступления в цифровом пространстве следует признавать место сетевого соединения с информационной сетью и вводом команд с последующей реализацией преступных действий. В случаи затрагивания национальных интересов, противоправную деятельность следует квалифицировать в соответствии с законодательством Российской Федерации, вне зависимости от места совершения общественно опасного деяния.

1.2. Понятие и признаки преступлений, совершаемых с использованием информационных технологий.

Современные способы коммуникации с использованием цифрового пространства позволяют не только исключить физический контакт, но и создать дополнительные защитные барьеры на пути идентификации личности.

Наиболее распространёнными способами сокрытия информации о личности, а также параметров используемого устройства в сети «Интернет», является подмена IP-адреса. С использованием протоколов соединения [Каримов, с. 51 - 54]:

1. Virtual Private Network (VPN) «Виртуальная частная сеть» [Методические рекомендации № 2003/46, с. 7];
2. The Onion Router (TOR) – реализация второго и третьего поколения т.н. луковой маршрутизации [Перов, с. 10-13];
3. Invisible Internet Project (I2P) «Невидимый интернет» [Ляпидов, с. 19-21], можно имитировать физическое нахождение в любой точке мира.

Наиболее характерными признаками преступлений в сфере компьютерной информации [Грачева, с. 145-159], являются:

1. Международный характер правовых взаимоотношений;
2. Отсутствие физического контакта между лицом осуществляющим противоправное деяние и жертвой преступного посягательства;
3. Латентный характер, ввиду имиджевого ущерба компаниям;
4. Локализация выявленных угроз информационной безопасности, создает предпосылки к совершенствованию механизмов и способов преодоления средств защиты;
5. Отсутствие видимых проявлений преступных действий, как следствие сложность выявления вредоносного программного обеспечения.

В целях совершенствования правовых механизма необходимо выработать единую международную терминологию, как следствие и спектр уголовно-наказуемых деяний.

Проведем анализ двух наиболее популярных в научных кругах понятий «информационные технологии» и «компьютерная информация».

В федеральном законе закреплено понятие «информационные технологии» к которому относятся процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [Федеральный закон № 149-ФЗ, с. 11-12].

Впервые упоминание о информационных технологиях встретилось в научных трудах В.М. Глушкова, рассматриваемое как способ работы с информацией, в частности [Глушков, с. 15]:

1. Способ и средство сбора информации;
2. Обработка информации;
3. Обмен информации в целях проведения анализа и получения новой информации.

Примечание ст. 272 УК РФ приводит понятие «компьютерная информация» - это сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [Уголовный кодекс Российской Федерации № 63-ФЗ, с. 245]. Таким образом компьютерная информация является составной частью информационных технологий, однако разделение данных понятий затрудняет понимание их содержания.

В приведенных понятиях разграничение происходит на основе анализа норм отечественной правовой системы, что позволяет разграничивать преступления совершенные в цифровом пространстве от иных деяний [Голованова, с. 176].

Для определения тяжести преступления, в первую очередь необходимо определить объект преступного посягательства [Винокуров, с. 71 - 79]. Условно разделим на вертикальное и горизонтальное деление «По горизонтали»: общие, родовые, видовые и непосредственные объекты. По вертикали происходит разделение «по горизонтали» — это определение основного и дополнительного объекта преступления.

В качестве объекта преступления выступает определенное благо (интерес), повреждение которого образует социальную сущность данного преступления и в целях защиты которого издана уголовно-правовая норма или группа уголовно-правовых норм, предусматривающих ответственность за его нарушение.

В главе 28 УК РФ прямым объектом признаются общественные отношения в информационной сфере, обеспечивающих состояние защищенности личности, общества и страны от информационных угроз. Объектами преступления в сфере компьютерных технологий следует считать следующее:

1. Информацию;
2. Объекты информационных технологий;
3. Компьютерную информацию;
4. Информационные системы;
5. Сайты;
6. Сети связи;
7. Информационные технологии;
8. Деятельность субъектов, связанную с формированием и обработкой информации.

В случаях отсутствии указанного специального объекта преступного посягательства к рассматриваемым составам следует отнести те деяния, в которых использование информационных технологий является способом осуществления преступления, т.к. на наш взгляд, само по себя деяние значительно шире, чем просто средство совершения преступления.

Исследование объективной стороны преступлений, рассмотренных правоотношений, позволяет выделить наиболее характерные признаки. В совокупности с проведенным анализом норм, содержащихся в главе 28 УК РФ, позволяет говорить о том, что деяния совершаются путем активных действий. На что нам прямо указывают используемые формулировки, как «создание», «распространение», «использование», указывающие на альтернативный характер деяния. Встречаются случаи когда нарушение правил эксплуатации

средств хранения (обработки) или передачи охраняемой компьютерной информации либо информационных сетей и оконечного оборудования, в т.ч. правил доступа к информационно-телекоммуникационным сетям, может быть совершено также путем бездействия С учетом данного подхода составы сформулированные в ст.ст. 272 и 274 УК РФ, являются материальными, с указанием на наступление негативных последствий, в виде: «уничтожение или блокирование, модификация либо копирование электронной информации», однако эти последствия альтернативны. В случаи совершения одного из перечисленных последствий, образуется состав уголовного правонарушения. Таким образом, в процессе доказывания необходимо установить причину, которая привела к наступлению общественно опасных последствий. С точки зрения нашего подхода, абстрактный способ изложения объективной стороны составов преступления и альтернативная диспозиция являются обоснованными шагами законодателя в виду многоаспектности рассматриваемых нами дел.

Факультативным признаком объективной стороны, является способ совершения преступления. В этой связи преступления, объединенные главой 28 УК РФ, содержат все необходимые элементы в основной характеристике деяния, как обязательности признака объективной стороны. Следовательно «только тогда способ совершения преступления, когда он сливается с деяниями (действиями или бездействием)», таким образом способ совершения преступления с использованием информационных технологий должен быть описан в уголовном законе с помощью слов «посредством», «путем», «с использованием», «с применением» и т.п.

Многообразие способов совершения общественно опасного деяния принуждает нас к широкому пониманию, чем само деяние. Совершение действия возможно посредством совершения определенных действий (например совершение акта), однако при этом способ не всегда является показателем объективной стороны состава преступления и может быть полностью не отражен в законодательной конструкции состава. Этот способ также нельзя назвать преступным поведением человека в целом, но и основной поступок здесь

не входит в состав преступления. Однако они являются частью целого – в преступное поведение).

Рассмотрим определение Зуйкова Г.Г., предложившего понимать под способом комплекс объективно и субъективно детерминированных, причинно-следственных действий злоумышленника в процессе подготовки к преступлению и сокрытия преступления, сопряженных с использованием условий мест и времени, орудий и средств. Таким образом они соответствуют объему преступного замысла и достижению поставленной цели [Зайков, с. 217].

Неразрывность применения указанным способом общественно опасных действий - орудий и средств, используемых для совершения преступления, очевидна. Кандидат юридических наук Яшковой С.А. в научных трудах выражал точку зрения, что средство совершения преступлений является не только в форме вещей материального мира (например, в форме предметов), но еще и в форме приемов, методик и способов совершения преступления, где в качестве орудий преступления выступают предметы материального мира [Яшков, с. 169].

В результате проведенного анализа способ в рассматриваемых нами действиях может быть отражен в диспозициях статьи, а также являться обязательным признаком (оказывающим влияние на состав преступления), может быть и должен быть учтен при индивидуальной квалификации преступления, может и должен быть учтён при индивидуализации наказания.

Следовательно, информационные программы (скрипты), с использованием которых совершалось общественно опасное деяние, оказываются средствами осуществления преступления, а используемое при этом устройства (материальные объекты) являются орудием. Таким образом вышеперечисленные элементы являются способом совершения преступления.

Помимо всего прочего, в качестве средства сокрытия совершенного правонарушения так же можно использовать различные программные комплексы и ухищрения цифрового пространства, в том числе для облегчения совершения преступления. В данном случае речь идет о создании

с использованием информационных технологий различных материальных предметов, а также уничтожение «цифровых» отпечатков, либо механическое уничтожение материальных носителей информации.

Особенности субъективных признаков рассматриваемых составов преступлений позволяют выделить некоторые особенности, такие как использование правонарушителем служебного положения (ч.°3 ст.°272 УК°РФ).

Под использованием служебного положения, предусмотренным в диспозиции ч.°3°ст.°272 УК°РФ, понимаются возможность беспрепятственного доступа к компьютерной информации, возникшей в связи с выполняемым характером работ (по различным основаниям, как устным так и письменным соглашениям) или используемого влияния по службе на лица, имеющих такой доступ (в данном случаи субъектом является работник). В основном деяния совершаются с умышленной формой вины, при этом специальные признаки квалификации для данных составов законодатель не устанавливает.

В унификации терминологии целесообразней употреблять термин «преступления, совершенные с использованием цифровых технологий», включающий кроме преступлений, также и преступления, совершенные с использованием информационных технологий.

С учетом того, что в рассматриваемой нами главе уголовного кодекса уже есть «некомпьютерные» статьи уголовного закона, которые фактически совершаются с помощью IT-технологий.

Таким образом, считаем целесообразным к преступлениям, совершенным с использованием информационно-телекоммуникационных технологий относить общественно опасные деяния, направленные на нанесения вреда общественным интересам в сфере безопасности цифровых технологий, а также создающих угрозу наступления негативных последствий, в т.ч. иные запрещённые уголовным законом деяния.

Особое внимание обращаем на то обстоятельство, что таким не считается деяние, например, когда происходит хищение компьютера с целью дальнейшей

реализации, поскольку компьютерная технология, вложенная в устройство, выражается лишь в качестве объекта преступного посягательства. Критерии отнесения преступления в данную группу должно обладать признаками направленности, которые предполагают наличие совокупности средств и способов. Таким образом подразумевается, что лицу необходимо обладать материальным цифровым устройством, используемого для достижения преступного умысла.

Исходя из вышесказанного мы считаем, что понятие «преступления, совершенные с использованием цифровых технологий» достаточно полно раскрывает все перечисленные нами понятия, характеризующие рассматриваемую группы преступных деяний. Термин, используемый нами необходимо трактовать в самом широком смысле – это использование в преступной деятельности неограниченных информационных ресурсов, способов и технологий. В условиях современного мира, новации в области информационных технологий постоянно модернизируются, что подталкивает преступные элементы к своевременному адаптированию и изощренным формам деятельности, связанных с посяганием на различные виды общественных отношений, ответственность за которые установлена различными разделами и главами уголовного закона. Необходимо применение одного обобщающего понятия для обозначения данной совокупности преступлений, которые являются преступлениями в сфере информационных технологий. На наш взгляд выбранная нами терминология базируется еще и на том, что она содержит законодательное отражение и позволяет избежать искажений при толковании. Таким образом, рассмотренные позиции позволяют сделать вывод:

1.°Рассматриваемые понятия объединенные группой преступного посягательства, содержащиеся в главе 28 УК РФ, до любых преступлений против личности, совершенные с использованием любых технических устройств. В большинстве случаев указывающих на двойственную природу рассматриваемых преступлений.

Выделяют основные группы:

-°противоправные деяния, за которые предусмотрена ответственность в сфере компьютерной информации закрепленная главой 28 УК РФ.

-°иные уголовно наказуемые деяния, где дополнительным объектом выступает нарушение безопасности в IT-сфере.

-°действия, с использованием информационных технологий являются способом совершения преступлений, где в качестве основного объекта противоправного посягательства выступают другие общественные отношения.

Выделенные группы противоправных деяний, совершаемы с использование цифровых технологий или с использованием информационно-телекоммуникационной сети «Интернет», а также посягательство предоставляет угрозу общественным отношениям, где при совершении противоправного деяния использовались цифровые технологии, то они выражают способ совершения преступления.

2.°Учеными-правоведами выделяются наиболее характерные особенности [Голованов, с. 216]:

-°межгосударственный характер взаимодействия среди субъектов (Трансграничность).

-°значительное удаление между субъектом и объектом преступного посягательства.

-°использование материальных специализированных средств.

-°использование специализированных цифровых программных комплексов.

-°латентный характер преступлений, на фоне репутационных рисков и сложностью механизмов выявления.

3. В условиях современного общества, с учетом темпов развития цифровых технологий совершение преступлений в цифровой среде становится наиболее популярным, что подтверждается рассмотренной статистикой опубликованной в ГИАЦ УМВД России. Способность быстрого охвата большой аудитории потенциальных жертв дополнительно создает предпосылки для популяризации хакерской аудитории и достижения

преступных целей, представляется необходимым включение в качестве квалифицирующих признаков совершение преступления «с использованием цифровых или информационно-телекоиммунизационных сетей» в подавляющее большинство статей УК РФ, применимо к составам преступлений, где такой способ является физически возможным.

1.3. Классификация киберпреступлений по российскому уголовному законодательству.

В процессе используя комплексного подхода к расследованию преступлений, совершенных с использованием информационных технологий, необходимо выделить такой метод как - структурирование сведения по различным основаниям, в связи с чем рассмотрим некоторые критерии классификации [Кадников, с. 5-16]:

1.°По степени опасности в однородном составе.

2.°По отдельным элементам состава преступления (объект, объективная сторона, субъект и субъективная сторона).

3.°По содержанию и степени общественной опасности (ст.°15 УК РФ).

Рассматриваемые классификации должны отражать социальное содержание по различным основаниям деления уголовных дел, а также способствовать в оценке совершенных противоправных деяний.

В качестве примера можно привести классификацию преступлений, которая необходима для составления общих принципов понимания об изучаемой группе случаев; характеристики отдельных объектов из различной совокупности случаев; дифференцированные критерии при соотнесении отдельных видов и рядов случаев и на этом основании выделение определенных закономерности такой соотнесенности; построение прогнозов возможности развития противоправных явлений в определенном направлении, с целью своевременного регулирования правоотношений.

В свою очередь, классификация заключается в том, чтобы помочь правильно соотнести и оценить рассматриваемые преступления, а также облегчить процесс их квалификации [Чуманов, с. 134].

Однако преступления, которые совершаются с использованием современных информационных технологий, довольно сложно выделить в рамках определенных групп. Это происходит потому, что в настоящее время на рынке существует огромное количество разнообразных цифровых устройств, которые позволяют совершать преступления с их помощью.

Выделяя критерии классификации компьютерных преступлений, необходимо рассмотреть международную практику отражения типов киберпреступности, содержащуюся в докладе Управления ООН по борьбе с наркопреступностью и киберпреступлениями, к которым относится:

1.°Компьютерное мошенничество или подлог.

2.°Компьютерные преступления, связанные с использованием персональных данных.

3.°Распространение или контроль распространения спама.

4.°Компьютерные преступления, касающиеся авторских прав или товарных знаков.

5.°Деяния, предполагающие использование компьютера в целях причинения личного вреда.

6.°Деяния, предполагающие использование компьютера в целях завлечения детей и груминга.

Например, в юридической литературе можно встретить различные позиции. В соответствии с Конвенцией Совета Европы о киберпреступлении 2001 г. выделяют несколько групп преступлений [Чуманов, с. 141]:

1.°В данном случае речь идет о компьютерных преступлениях, которые включают в себя незаконный доступ, перехваты, вмешательство в данные, а также в саму систему.

2.°Совершение преступлений на основе использования компьютера: цифровая кража сведений о реквизитах банковских карт, мошенничество и тд.

3.°При совершении преступлений, в которых компьютер является интеллектуальным средством: распространение на сайтах детской порнографии; информации о национальной, расовой, религиозной вражде.

Рассматривая научные труды Рассолова И.М., в которых он делит рассматриваемые нами деяния, как на «преступления в сфере компьютерной техники», так и на «кибернетические правонарушения». Сфера компьютерных преступлений требует правового закрепления в УК РФ, а кибернетические

уголовно правовые деяния подпадают под квалификацию иных статей [Рассолова, с. 61].

Главный вывод, который следует сделать по отношению к рассматриваемым уголовно наказуемым деяниям [Кузнецов, с. 94]:

1. Можно выделить несколько классификаций киберпреступлений:

-°на основании системы УК РФ: преступления, которые непосредственно связаны с использованием информационных технологий; преступления, при совершении которых компьютерные технологии значительно облегчают противоправную деятельность, являясь способом совершения преступления.

-°по объекту преступного посягательства, в качестве которого выступают общественные отношения в информационной сфере, обеспечивающие состояние защищенность персональной информации, государства и общества от угроз в цифровом пространстве, где опасности выступают в качестве основного объекта преступления; то по объекту преступления, в котором общественные отношения в информационной сфере, обеспечивающих состояние защищенности личности, общества и государственности от информационных угроз выступают в качестве дополнительного или факультатива.

-°преступления совершаются с использованием IT-технологий (в зависимости от специального упоминания в диспозициях). Преступления, которые могут быть совершены с помощью современных информационных технологий (с отражением в диспозиция), являются преступлениями, которые не содержат такого способа совершения деяния.

-°также можно выделить несколько основных видов преступлений, к ним относятся по степени общественной опасности (по степени опасности в составе однородного состава): основные составы преступлений, где использование цифровые технологии является обязательным признаком состава преступления; квалифицированные составы преступлений, где использование информационных технологий не является обязательным признаком состава преступления; «нейтральные» к этому признаку преступления;

2.°В ходе анализа классификаций по различным основаниям необходимо отметить, что большинство противоправных деяний рассматриваемых за пределами главы 28 УК РФ, могут быть совершены посредством использования материальных предметов цифрового пространства [Далгалы, с. 19-21].

С учетом темпов роста преступлений в цифровом пространстве, в том числе в рамах главы 28 УК РФ, целесообразно рассмотреть возможность внести в ст. 63 УК РФ дополнение: использование средств массовой информации, информационных систем, электронных либо информационно-телекоммуникационных сетей, в т.ч. сети «Интернет», что поможет учитывать данное обстоятельство при назначении наказания.

1.4. Зарубежный опыт противодействия киберпреступлениям.

В современных условиях стремительного развития цифровых технологий каждое государство стремиться к регулированию общественные отношения в рассматриваемой сфере. Как мы уже говорили отличительной особенностью является трансграничный характер. В связи с этим наиболее целесообразно рассмотрение зарубежного опыта противодействия киберпреступности, в ходе анализа которого прослеживается стремление к единой юрисдикции государств и противодействие киберпреступности. Анализ зарубежных примеров позволит выявить общие тенденции развития противодействия в мировом пространстве.

В рассматриваемых нормах ООН, существует два категория киберпреступлений.

1) Нечто вроде «киберпреступления» в узком смысле: любое противоправно-преступное деяние, осуществляемое с помощью электронных операций, целью которого является преодолением защиты компьютерных систем и обрабатываемых ими информационных данных.

2) Если говорить о киберпреступлении в широком смысле – это любое противоправное деяние, которое совершается посредством и в связи с компьютерной системой или сетью.

В любом случае, государства стремятся отразить в национальном законодательстве аналогичные преступления. Согласно данным, опубликованным в официальном журнале Совета Европы, первые нормативные акты Совета Европы, посвященные вопросам регулирования киберпреступности – это Рекомендация № 2 Комитета Министров стран-членами Совета Европы «О преступлениях, связанных со компьютерами», а также Отчет европейского комитета по проблемам преступности о преступлениях, совершенных на компьютерах. Изучив указанные законодательные акты, можно сделать вывод, что отчет разделяет все преступления, содержит два перечня преступлений - минимально необходимые к включению в национальный закон и дополнительные преступления [Далгалы, с. 34-37].

В указанную группу входят:

-°компьютерное мошенничество.

-°компьютерный сбой.

-°несанкционированный доступ и перехват.

-°несанкционированное воспроизведение компьютерной программы, охраняемой авторским правом.

-°компьютерный взлом и т.д.

Следующим документом является Конвенция Совета Европы по борьбе с преступностью в сфере компьютерной информации. Данные акты содержат состав по четырем основным группам, в соответствие с объектом посягательства:

-°преступления в сфере конфиденциальности, целостности и доступности компьютерных баз и систем.

-°нарушения в работе компьютеров, которые были обнаружены.

-°содержание данных.

-°преступления, связанные с нарушением авторского и смежных прав.

В результате анализа данного акта, приходим к выводу о том, что Конвенция содержит только общие правила регламентации ответственности за преступления с применением IT-сфере. В свою очередь, Российская Федерация не подписала данный документ. Данный отказ связан с тем, что в пункте о том, что «сторона имеет право без согласия другой стороны получать через компьютерные системы на своей территории доступ к хранящимся там компьютерным данным или получить их». Данное положение, как представляется, дает возможность давать полномочия, которые могут быть нанесены ущерб суверенитету государства.

При этом России было дано согласие на ратификацию Соглашения о сотрудничестве государств - участников СНГ по борьбе против преступлений в сфере компьютерной информации. Данное соглашение было подписано рядом государств: Азербайджанской Республики, Республикой Армения, Республик Беларусь, Республик Казахстан, Кыргызская Республика, Республик Молдова, Республик Таджикстан, Республик Узбекистан и Украиной [Голованов, с.194-201].

Список деяний, которые должны быть криминизированы в странах, приведен в ст. 3 данного документа

а) Противоправный доступ к защищаемым государством компьютерным данным и системам, если это деяние повлекло за собой уничтожение, блокирование, модификацию или копирование информации, нарушение работы ЭВМ или их сети;

б) Создание, внедрение в систему и распространение вредоносных программ;

в) А также нарушение правил эксплуатации ЭВМ, системы эмснрой или их сети лицом, имеющим доступ в ЭВМ, системе эмснрой и их сети, повлекшее уничтожение, блокровку или модификацию охраняемой законом информацииЭВМ, если это деяние причинил существенный вред или тяжкие последствия.

г) Присвоение авторства за нарушение авторских прав или же нанесение ущерба – это не что иное, как незаконное использование программ для ЭВМ или базы данных, являющихся объектами авторской собственности.

Если рассматривать законодательство государств участников, то можно заметить различия в наименовании данных преступлений [Голованов, с.203-206].

Раздел 16 Уголовного кодекса Украины содержит статью 16 «Преступления в области применения электронных вычислительных машин (компьютеров), средств и компьютерных сетей и сетей электросвязи»

Киберпреступность в Азербайджане – глава 30.

Преступления, которые были совершены в Армении, содержатся во главе 24 «Преступление против безопасности компьютерных данных».

Указом Президента Республики Беларусь от 30.12.2015 № 548 «О внесении изменений в Указ Президента Республики Беларусь от 29 декабря 2015 года № 549" данная группа была переименована. Закон Казахстана содержит главу 7 «Уголовно-правовые правонарушения в сфере информатизации и связи».

Кыргызская Республика объединила рассматриваемые правонарушения в главу 42 Уголовного кодекса – «Преступления против информационной безопасности».

«УК республики Молдавия» (УРМ) называет действия, совершенные в сфере электросвязи, Информационными преступлениями и преступлениями в области электросвязи

В Уголовном кодексе Таджикистана преступления данной группы отражены в главе 28 « Преступления против информационной безопасности».

Закон в Узбекистане содержит главу «Преступления в сфере информационных технологий».

По нашему мнению, данные составы преступлений полностью соответствуют требованиям законодательства стран-участниц, отражая специфику использования информационных систем в специальных нормах, а также в иных составах преступлений.

Однако в отличие от указанных нами стран (в т.ч. Российской Федерации) некоторые страны, вследствие своего высокого уровня развития цифровых технологий (США, Японии, страны Евросоюза) начали разработку правовых норм борьбы с компьютерными преступлениями намного раньше других. А вот в этой области лидируют США. Исследователи подчеркивают, что в законодательстве США закреплены такие действия:

–°Компьютерный взлом;

–°«Несанкционированное» использование правительственного компьютера.

–°Повреждение либо же нарушения государственного компьютерного оборудования;

–°Мошенничеством с использованием компьютера.

–°Обман при продаже компьютерных паролей;

–° Угрозы, шантаж с помощью компьютера;

–°Торговля краденными или поддельными устройствами доступа, с помощью которых можно получить деньги, товары или услуги;

–°Умышленное повреждение оборудования, линий и систем связи.

–°Передача информации, передаваемой по телеграфу, с помощью перехвата и разглашения.

Не смотря на такое детальное урегулирование деяний, государство испытывает затруднения (как и другие государства) в случае, если посягательство совершается за пределами страны.

Стоит отметить, что признаки деяний в странах разных правовых систем (романо-германской и англо-саксонской) немного отличаются по содержанию этих формулировок. Особенность прецедентного права заключается в признании признака состава по конкретному факту (например, в зависимости от конкретного случая), что приводит к наличию абстрактных правовых формулировок и возможности широкого толкования этих признаков. А также особенность заключается в полном отсутствии в национальном законодательстве конкретных составах правонарушения. Кроме того, как правило, в Великобритании ответственность за совершение подобных преступлений возлагается на различные нормативные акты – законы о неправомерном использовании компьютера, закон об электронном сообщении, а также Закон об электронной защите персональных данных и др. Анализ названных нормативных актов показывает, что компьютерная информация в одних ситуациях выступает объектом преступления.

Партнеры РФ, с целью закрепления в нормах уголовного закона цифровой терминологии стремятся к закреплению в них четких и однозначных формулировок. При этом все без исключения государства при формулировании конструкции норм стремятся к определенной унификации в определении общих признаков, что позволяет говорить об их ответственности за схожие деяния. Этот факт подтверждает факт употребления в нормах единоообразных формулировок: так, например статья о «компьютерном саботаже» в Уголовном кодексе Республики Беларусь, Республике Армения, Кыргызской Республики.

Но не все страны романо-германского союза выделяют собственно киберпреступления. Однако в Уголовном кодексе ФРГ нет специальной главы,

но есть отдельные составы преступления: «Изменения данных» (§303б), «Компьютерный саботажник» (§203а), «Компьютерное мошенничество». УК Нидерландов также не содержит отдельной специальной статьи, отражающей преступления, совершенные с помощью цифровых технологий, в зависимости от существующего родового объекта преступного посягательств.

Данный вопрос имеет не только практическое значение, также связан с необходимостью закрепления в законодательстве специальных статей, и является вопросом о том, как отразить в национальном законе такой квалифицирующий признак, как использование информационных технологий для облегчения совершения преступления. При этом анализ нормативных актов зарубежных стран показывает, что чаще всего подобный способ присутствует в составах деяний, устанавливаемых ответственностью за хищение.

Здесь мы приводим нормы, которые содержатся в ст. 212 УК Республики Беларусь «Хищение путем использования компьютерной техники», которая предусматривает ответственность за хищение имущества посредством изменения информации, обрабатываемой в компьютерной системы, хранящейся на машинных носителя или передаваемой по сетям передачи данные, либо введение в компьютерную систему ложной информации. В Уголовном кодексе Республики Армения приводится аналогичная статья 181 «Хищение, совершенное при помощи компьютерной техники» [Абдулвалиев, с.123-130].

С помощью специальных норм законодательства ФРГ - "компьютерное мошенничество" (§ 203а) - "Действие, направленное на получение для себя или третьего лица противоправно имущественной выгоды от действий, направленных на обработку данных компьютера посредством составления неправильных программ, а также нарушение правил эксплуатации компьютера. В соответствии с нормами уголовного законодательства Японии, Швеции, Польши и других стран, такие нормы нашли свое отражение в Уголовном кодексе Японии, Швеции, Польши и других европейских стран.

Конечно же мы считаем, что применение цифровых технологий в качестве способа совершения преступлений должно отвечать современным реалиям.

Из анализа зарубежных законов можно сделать следующие выводы:

-°Не секрет, что в современном мире существует множество способов и методов борьбы с киберпреступностью, однако достичь положительного результата возможно только при соблюдении единообразного подхода, использовании в законодательном порядке схожих формулировок. Кроме того все без исключения государства, при формулировке конструкций норм, стремятся к определенной унификации в выделении общих признаков, что дает возможность говорить об ответственности за схожие деяния Но сейчас законодательство стран имеет различные по содержанию нормы и способы их отражения в уголовном законодательстве.

-°Для стран англо-саксонской правовой системы характерна особенность, что часто используются абстрактные формулировки, которые не всегда понятны для неподготовленного человека. Отличается от других тем, что отсутствует в национальном законодательстве конкретный состав правонарушения, а регулирование осуществляется путем обращения в каждом конкретном случае к различным нормативно-правовым актам.

-°Для стран романо-германской системы характерна особенность, что чаще всего содержатся специальные составы преступления, которые определяют их по основному объекту преступных посягательств, но есть и исключения. В то же время общественную жизнь в сфере цифровых технологий можно рассматривать как дополнительный объект посягательства, а специальные нормы закона не могут быть использованы в качестве основы для регулирования общественных отношений в этой сфере. Таким образом в законодательстве многих стран содержатся специальные главы, которые содержат специальные составы преступления, где использование цифровых технологий является способом совершения преступлений.

ГЛАВА 2. ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.

2.1. Неправомерный доступ к компьютерной информации.

Во времена цифровой эпохи прослеживаются такие процессы, как развитие и совершенствование, что выражается в изменении технологического уклада. Все более конкретно прослеживаются контуры информационного общества с его основными технологическими укладом и техникой, а информация считается самым важным ресурсом, новые информационные и телекоммуникационных технологии и техника становятся базовыми, а информация считается наиболее важным ресурсом.

Исследователи считают, что мировая информационная система начала формироваться в 2002 году, когда компьютеры и пользователи Интернета стали настолько значимыми для экономики, что она стала приспосабливаться под соответствующий спрос на цифровые продукты.

В наше время компьютер является не только рабочим инструментом, но и способом проведения досуга. В качестве информационного контента потребляется цифровая информация, которая передается и получает с помощью специальных технических устройств. Тем не менее преступления все еще имеют место быть, они также используют «инструменты, которые используются при проникновении в сети, взломе и модификации программного обеспечения», а также «инструменты, используемые для взлома и модификации программного обеспечения, незаконно полученного или заблокированного» [Уголовное право России, с. 211-219].

С этим связано всё более важное место в системе уголовной ответственности за компьютерную информацию занимает уголовно-правовая охрана информации.

Согласно статье 272 Уголовного кодекса РФ, за неправомерный доступ к компьютерной информации предусматривается уголовная ответственность. Данная законодательная новелла действует в редакции Федерального закона от 07 декабря 2011 года № 420-ФЗ, который внес ряд существенных изменений

в состав этого состава правонарушения и существенно изменил его структуру, когда законодатель фактически отказался от таких слов, как «машинный носитель», «ЭВМ», «сеть ЭВМ».

Однако такой ответ был вполне закономерен и оправдан с точки зрения современного научного познания, так как понятийно-категориальный аппарат к тому времени значительно изменился, а понятие электронно-вычислительной машинки оказалось устарелым и не соответствующим современным научным представлениям. Сегодня все эти понятия, как и ранее, объединены термином «компьютерная информация».

Но в уголовно-правовой литературе, как и в других областях знания, нет единого подхода к пониманию объекта данного преступления. Есть и другие авторы. Они пишут о том, что видовым для такого случая является «безопасность охраняемой законом компьютерно-информационной системы, обеспечиваемой правомерным доступом к ней».

Иные авторы называют этот видовой объект данного преступления общественными отношениями «обеспечивающими защиту компьютерной информации», а также «основным и единственным объектом данной группы преступлений». Третья группа считает предметом преступления «общественные отношения в области охраны компьютерной информации».

С точки зрения определения объекта преступления по ст. 272 УК РФ они не отличаются от формулировок других статей, определяющих компьютерную информацию [Ляпидов, с. 89].

Согласно примечанию 1 к ст. 272 УК РФ, под компьютерной информацией понимаются сведения, полученные в результате обработки информации, представленной в форме электрических сигналов, независимо от способов ее хранения, обработки и передачи.

В некоторых работах критикуется данное определение. Помимо этого, уточняется неясность смысла термина «электрический сигнал» и возникает множество проблем при применении его к правоотношениям. В тот же момент записи и чтения информация, хранящаяся на оптических дисках, является

компьютерной информацией, поскольку она находится «в форме электрических сигналов» в операционной памяти обрабатывающего информацию устройства, а во время хранения этих дисков (или накопителей подобного рода) — нет.

Однако в судебной практике не возникает проблем в оценке компьютерной информации. Такие сведения могут иметь самую разную форму – от информации о правах доступа, до сайтов с информацией о компьютерных системах и программном обеспечении.

Таким образом, в данном случае компьютерная информация является предметом рассмотрения данного уголовного дела.

А между тем существует точка зрения о том, что объектом данного преступления является «электронно-вычислительная машина как комплекс информационных средств, физическая среда и непосредственно хранящая информацию (носитель°информации)». А вот с этим утверждением согласиться нельзя – ведь ни о каких носителях информации в статье 272 УК РФ речи не идет. Под признаком состава правонарушения является компьютерная информация, которую используют в качестве орудия совершения преступления. Так, например, некоторые авторы указывают на то, что компьютерная информация в структуре составов преступлений может быть как предметом, так и способом совершения преступления. Исходя из этого вывода мы считаем его ошибочным. Ведь он основывается не только на неправильной оценке объекта нападения (что само по себе уже ошибка), но и на ложном понимании предмета преступления, которое заключается в том, что именно наносит вред объекту нападения (что само по себе уже нарушение). При совершении определенных действий в отношении компьютерной информации, согласно статье 272 УК РФ, ответственность наступает. Как и во всех других случаях с данной проблемой, она является предметом преступления [Степанов-Егиянц, с. 67-74].

Охрана закона – это неотъемлемое свойство компьютерной информации, которая входит в состав рассматриваемого состава преступления, что закреплено в статье 272 УК РФ. По мнению некоторых авторов, этот знак является

специальным режимом ее правовой защиты. Подразумевается соответствующий статус информации, позволяющий относить информацию к государственной, коммерческой, банковской и налоговой тайне либо к персональным данным.

Ст. 5 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и об защите информации», гласит: «Информация в зависимости от категории доступа делится на общедоступную, а именно на информацию, доступ к которой ограничен федеральным законом (информация ограниченного доступа), и информацию, доступ к которой ограничен федеральным законом (информация неограниченного доступа). В данном случае речь идет о том, что в компьютерной информации содержится информация, которая не является общедоступной. А это, в свою очередь, лишь о компьютерной информации ограниченного доступа

При этом следует отметить тот факт, что анализ судебной практики о преступлениях, предусмотренных статьей 272 УК РФ, позволяет прийти в выводу о том, что одним из условий, подлежащих установлению по уголовному дела, является правовая охрана соответствующей компьютерной системы. Судам приходится руководствоваться Федеральным законом от 26.07.2006 № 149–ФЗ «Об информации, информационных технологиях и о защите информации» и специальными нормативно-правовыми актами, защищающими эту информацию В частности, Федеральный закон от 29.07.2004 №°98-ФЗ «О коммерческой тайне», ГК РФ (часть четвертая) от 18.12.2006 №°230–ФЗ и т. д.

В данном случае, объективная сторона данного состава преступления представлена неправомерным доступом к компьютерной информации. Если вы имеете возможность получить доступ к информации или же вам предоставляется возможность использовать информацию, то это всегда активный шаг, который выражается в возможности получения информации и возможности её использования. В литературе отмечается, что под доступом к компьютерной информации следует понимать «получение лицом возможности воздействия на компьютерную информацию путем чтения,

записи или исполнения им в компьютере машинных команд». Этот доступ должен быть незаконным, т. е. у виновника не должно быть необходимого разрешения законного владельца информации.

Подобные ситуации возникают при использовании специальных вредоносных программ для подбора аутентичных пар логин пароль и нейтрализация средств защиты компьютерной информации. В случае совершения подобных действий, необходимо получить дополнительную квалификацию по ст.°273 УК РФ.

По конструктивной стороне неправомерный доступ к компьютерной информации является материальным составом, т.е. состав, где криминообразующим признаком являются последствия В ст.°272 УК РФ перечислены следующие последствия [Бриллиантов, с. 34-36]:

1. Заражение информацией. Это результат воздействия информации, исключающей её дальнейшую обработку и распространение. При этом удаление информации происходит посредством её уничтожения. В дальнейшем значение для квалификации не имеет.

Судебная практика показывает, что в качестве примера можно привести осуждение М., по ст. 272 УК РФ. В соответствии с текстом судебного приговора, подсудимая, не имея законных оснований для доступа к сайту юридического лица, с незаконным использованием известных ей в силу занимаемой должности в данной организации логина и пароля от компьютера, с использованием своего ноутбука и сетей «Интернет» осуществила доступ к административной панели сайта, суд признал, что М. нарушила закон о защите информации.

2. У меня есть блокиратор информации. Причиной является воздействие на компьютерную информацию, которое приводит к невозможности осуществления необходимых операций над компьютерной информацией полностью или в требуемых условиях, т. е., совершение действий, приводящих к ограничении или закрытию доступа законных пользователей к компьютерному оборудованию и расположенным на нём ресурсам, намеренное затруднение доступа законных пользователей к компьютерному оборудованию

и находящимися на нём ресурсам, направленное ограничение или закрытие доступа законных пользователей к компьютер При этом компьютерная информация, которая была заблокирована, не имеет никакого значения.

Из практики можно привести такой пример. М., для того чтобы получить возможность использования на данной игре нелицензионных игровых приложений и использовать специальные познания при их использовании на данной игровой приставке, производитель внес несанкционированные им изменения в ПО игровой приставки. М. В результате замены оригинального компонента ПО и внедрения в электронную схему игровой приставки постороннего устройства, предназначенного для обхода программно-аппаратурной защиты игровых приставок иностранной коммерческой фирмы, что в совокупности привело к тому факту, что отключилась программная защита с использованием нелицензионных копий программного продукта и появилась возможность использовать В этом случае виновник заблокировал компьютерную информацию.

3. К понятию модификация информационной системы, принято относить изменение данных о компьютере и его параметрах, а также в баз данных.

Как известно из вышесказанного, М. изменил сроки и классы подписки на принадлежащей ему смарт-картой спутникового телевидения с истекшими срокам подписок, посредством несанкционированного использования программ, предназначенных для модификации хранящейся в памяти смарт-карты информации. В соответствии с этим, суд квалифицировал данное деяние по ч.°2 ст.°272 Уголовного кодекса РФ как модификацию компьютерной информации и признал виновником М.

4. Копирование информации с компьютера включает, в себя что компьютерная информация воспроизводится на другом носителе с сохранением исходной информации (первоначальной информации), а также дублирование ее на другой носитель без изменений первоначальной информации.

Так сотрудник салона мобильной связи и имеющий возможность доступа в компьютерную информацию по персональным данным клиентов посредством

своего мобильного телефона передал К. файл со сведениями об датах и времени телефонных соединений, номерах входящих и исходящих соединений и текстовых сообщений абонента сотовой связи. Однако если бы они не нарушили тайну связи и не допустили несанкционированного доступа к информации компьютера, то их действия были бы квалифицированы как нарушение тайны переписки, телефонных переговоров, почтовых и телеграфных сообщений (ст. 138 УК).

С субъективной стороны данного состава преступления, как и в других случаях, нет ни малейшего намека на умысел. Согласно действующему законодательству, судебные органы при вынесении приговора указывают не только на намерение, но и на его реализацию, как правило, в форме прямого умысла. По мнению ученых, такое преступление может быть совершено в форме легкомыслия. Но это не нашло отражения в судебной практике. На основании изученных судебных приговоров судами было установлено понимание факта незаконной деятельности по доступу к компьютерной информации у обвиняемых и их намерение на совершение действий, которые входят в состав объективной стороны состава преступления. С этой точки зрения следует сделать вывод, что объективную сторону данного состава преступления составляет только прямой умысел [Антонов, с. 541].

Стоит отметить, что данный случай является самым распространенным среди всех преступлений в сфере компьютерной информации. Скорее всего причиной этого является то, что понятие «компьютерная информация» существует как минимум во всех областях телекоммуникационных системах, а возможно даже в компьютерных программах и баз данных.

2.2. Создание, использование и распространение вредоносных компьютерных программ.

Первоначальный текст редакции статьи 273 Уголовного кодекса РФ, введен в 1996 году, где термин «ЭВМ» является устаревшей, узконаправленной и узкой специализацией; он не соответствует современным технологическим укладом. В соответствии с Федеральным законом от 07 декабря 2011 года № 420-ФЗ «О внесение изменений в УК РФ и отдельные законодательные акты Российской Федерации», статья, которая ранее была принята в редакции Федерального закона от 07 декабря 2011 года № 421-ФЗ «О внесении изменений в УК РФ и отдельные законодательные акты претерпевали бурное развитие.

Принадлежащие к данной группе преступлений относятся к сфере компьютерной информации, а именно к отношениям в сфере компьютерной информации. Одним из основных объектов преступления по ст.°273 УК РФ является «безопасность компьютерных программ и средств защиты компьютеров», а именно право на их использование. К предмету рассматриваемого состава правонарушения относятся программы, которые содержат компьютерную информацию. С другой стороны, для обозначения вредоносных компьютерных программ (скриптов) используются привычные всем гражданам слова – вирус, либо троян, однако такой раздел вирусологии предусматривает широкий спектр различных программных уязвимостей, одной из наиболее активно развивающихся фирм по выявлению компьютерных атак является лаборатория Касперского и Group-IB.

Правоприменительная практика судов также использует различные обозначения вредительских компьютерно-информационных программ. Однако в данном случае это название является типом (видом) компьютерных программ Специалисты отмечают, что наиболее часто встречающимися вредными компьютерными программами являются компьютерные вирусы, черве и сканирующие программы, обходчики средств безопасности, программы управления потоками компьютерной информации. Данный факт вполне оправдан законодателем. Он имеет право использовать в своей речи обобщенный

термин «компьютерные программы», который охватывает все компьютерные программы и всю компьютерно-информационную информацию, обладающую определенной вредоносностью.

С учетом положений статьи 1261 ГК РФ, программа для ЭВМ (компьютерная программа) является представленной в объективной форме совокупностью информационными командами, предназначенными для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки компьютерной программы, и порождаемые ею негативные процессы [Гражданско-правовое регулирование договорных отношений в сфере телекоммуникационных услуг, с. 176].

На основании этого обстоятельства и примечания 1 к ст. 272 УК, предметом преступления является «иная компьютерная информация», содержание которого раскрывается в примечании.

Нет, конечно, в компьютерных программах и в информации, которую они содержат могут быть вирусы или вредители, но только те, которые являются вредоносными. Указание на вредность отсутствует в тексте ст.°273 УК РФ. Этот знак присутствует только в названии статьи. При этом в тексте статьи данный термин раскрывается через указание на назначение компьютерной программы для несанкционированного уничтожения, блокада, модификации, копирования, нейтрализации средств защиты компьютерной информации.

Несмотря на то, что в ст.°273, в отличие от ст.°272 УК РФ нет упоминания об «охраняемой законом» компьютерной информации, которая наносит вред компьютеру, в статье есть указание на «охраняемость законом» компьютера. Значит, что компьютерные вирусы опасны сами по себе, без привязки к какой-либо конкретной компьютерной информации. Однако в некоторых случаях суды, принимая решение, все-таки определяют характер компьютерной информации, которую причинили вред. К примеру, часто встречается «конфиденциальная закодированная информация о зарегистрированных учетных записях различных сервисов сети Интернет».

В других случаях суды не указывают конкретную компьютерную информацию, ограничиваются указанием на «чужую компьютерную информации». С точки зрения юридической оценки характера компьютерной информации, которая причиняется данным преступлением, это не имеет никакого значения. Однако, если в результате совершения таких деяний злоумышленник получит возможность доступа к электронной переписке потерпевшего, то ему необходимо дополнительно квалифицировать содеянную по ст. 138 УК РФ. Нередко бывает так что действия, описанные в статье 273 УК РФ дополняется статьей 272, при наличии к тому основания.

Стоит отметить, что вместо «охраняемости законом» законодатель употребляет термин «несанкционированности» доступа к компьютерной информации и средствам защиты ее. «Непосредственность» – в данном случае отсутствие разрешения со стороны законного пользователя компьютера.

Как известно в научной литературе встречаются мнения о том, что предметом преступления, кроме компьютерных программ и компьютерной информации, являются ещё и средства защиты компьютерной информации. В данном случае мы считаем, что такой подход неверный, так как не соответствует понятию преступления. Если же говорить о буквальном и логическом толковании диспозиции ст.°273 УК РФ, то можно сделать вывод, что средства защиты компьютерных программ не являются составной частью преступления, в отношении которого совершается деяние. Подлежащие действию деяния заключаются в том числе в компьютерных программах и информации, которая является предметом преступления. По признакам предмета преступления, которые определяют это свойство объекта (вредоносность), средства защиты компьютерной информации относятся к предмету преступления. Таким образом, если компьютерная программа и компьютерные данные предназначены для нейтрализации соответствующих средств защиты или же они могут образовывать рассматриваемый состав преступления, то действия с этими предметами могут быть квалифицированы

как преступление. Кроме того, нет необходимости в нейтрализации указанных средств защиты – достаточно факта их назначения [Русскевич, с. 44].

Тем не менее при рассмотрении вопроса о средствах защиты компьютерной информации следует обратить особое внимание на то обстоятельство, что это понятие является свойством объекта преступления и должно быть рассмотрено в контексте рассмотрения вопроса о средствах защиты компьютерной информации

При этом законодатель не дает определение понятия «средств защиты компьютерной информации». В соответствии со ст. 16 Федерального Закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и об защите информации», защита информации представляет собой принятие правовых, организаторских и технических мер. В соответствии с этим, средства защиты компьютерной информации можно разделить по правовым, организационным и техническим. Конечно же, нет никаких сомнений в том, что правовая и организационная защита не может быть признаком вредоносной компьютерной программы, ведь в силу своей технической природы такая программа физически не способна причинить физический вред. Но это только технический вред. Потому что, согласно статье 273 УК РФ, средства защиты компьютерной информации должны рассматриваться только с позиции технической безопасности.

Однако авторы не отрицают, что к средствам защиты компьютерной информации относится техническая, криптографическая или программная защита такой информации, а также средства контроля эффективности такой защиты.

В судебной практике наиболее распространена оценка действий, направленных на подавление (нейтрализация) именно средств программной защиты, например, антивирусных программ.

Некоторые ученые считают, что термин «нейтрализация» не имеет единого смысла и не устоялся в русском языке. Однако, к этому понятию некоторые авторы относят полное или частично разрушение защитных систем компьютеров

без возможности их восстановления либо иное перекрытие защитной системы компьютера. По нашему мнению, в данном случае уместно использовать слово «подавление». Снижение, вплоть до полного исключения, влияния какого-либо. Под воздействием средств защиты и подавления вредной компьютерной программы (программы — наивысшего уровня) вредоносная компьютерная программа (компьютер-наивысшего уровня) подавляет эту защиту, разрушается ее, создает критическую уязвимость для злоумышленника, дает ему возможность получить доступ к компьютерной информации. Такими являются такие процессы и обозначают соответствующую “нейтрализации”, упомянутую законодателем в ст. 273 УК РФ. С нашей точки зрения, это абсолютно бессмысленно – менять терминологию и заменять слово «нейтрализация» на другой термин более подходящий, емкий и содержательный, так как в правоприменительной практике не возникают проблем с толкованием данного понятия.

При этом конструкция составов преступления позволяет отнести его к формальным, поскольку не предполагает наличия общественно опасных последствий. За это ответственность наступает в соответствии с соответствующим деянием в отношении вредоносных компьютерных программ или компьютерной информации [1].

Субъективную сторону преступления, предусмотренного ст. 272 УК РФ, представляют три альтернативных действия – создание, распространение и использование. Данный термин встречается довольно часто в Уголовном кодексе РФ. Он является общеупотребимым и не вызывает затруднений в его оценке в рамках правоприменительной практики.

В частности, судами не устанавливаются все технические обстоятельства, характеризующие особенности изготовления вредоносной компьютерной программы или компьютерной информации; не затрагиваются технические аспекты, связанные с использованием соответствующего языка программирования, последовательность кодов (сигналов) и сигналов и т.д. Так как же все-таки судам интересны технические инструменты для создания

вредительской электронной системы? Например, такие как компьютерная техника (например, ноутбуки, модемы, сети «Интернет» и т.д.), а также техническая информация (например, компьютеры). Например, Асбестовский городской Суд в одном из приговоров установил, что виновный создал веб приложение, внешне похожее на дизайн интернет-сайта.

В данном случае под созданием понимается создание вредоносной компьютерной программы или компьютерной информации. В частности, приговором Прикубанского городского суда города Краснодара установлено, что виновный присоединил к чековому принтеру одного из банкоматов, сетевой концентратор. В данном случае под использованием понимается использование вредоносной компьютерной программы или компьютерной информации

Распространение также не вызывает затруднений в толковании и оценке. В некоторых случаях суды указывают, что «по смыслу закона, распространение вредоносных компьютерных программ означает предоставление доступа к воспроизведенной в любом материальном виде компьютерной программе, в том числе сетевым и иным способом, а также путем продажи, прокаты, сдачи внаем, предоставления безвозмездно или за плату, аренды, передачи в аренду, передачи в залог, передачи в доверительное управление, передачи в залог по договору и т.д.

В научной литературе высказывается мнение о том, что необходимо включить в объективную сторону состава рассматриваемого правонарушения действия, составляющего приобретение вредоносных компьютеров и компьютерной информации. Такая теория объясняет это тем, что «подавляющее большинство преступников, которые используют вредоносную компьютерную программу, не являются ее создателями, а приобретают ее для преступных целей у представителей хакерской группы, на хакерских сайтах и веб - страницах, путем обмена через электронные доски объявлений либо хакерские форумы».

Несмотря на это сегодня покупка зараженных компьютерных программ или компьютерная информация уже является составной частью преступления

и не подлежит уголовной ответственности. А между тем эти действия сами по себе не представляют никакой общественной опасности, поскольку еще не означили применения или распространения. Здесь же расширение субъективной стороны правонарушения, которое было совершено по ст.°273 УК РФ нецелесообразно.

Если покупка вредоносных компьютерных программ или компьютерной информации совершается для последующего их использования, то содеянного можно было бы квалифицировать как подготовку к преступлению И хотя статья 30 УК РФ предусматривает ответственность только за приготовление преступления небольшой или средней тяжести (ч. 2 ст. 30 УК РФ), но поскольку ч. 2 ст. 30 УКРФ запрещает привлечение к уголовной ответственности за приготовлением к преступлению небольшой или средней тяжести, то и говорить в данном случае об уголовной ответственности не приходится. Для того чтобы приобрести вредную компьютерную программу, а также информацию в целях ее последующего распространения с целью причинения тяжких телесных повреждений (ч. 3 ст. 272 УК РФ), необходимо довести дело до конца по не зависящим от виновного обстоятельствам, т.е. довести его до конца по не зависящим от него причинам

Субъективная сторона рассматриваемого правонарушения характеризуется прямым умыслом. В данном случае имеется прямой умысел, который заключается в том, что компьютерная программа или информация предназначена для несанкционированного уничтожения, блокирования и модификации компьютерной информации или нейтрализации средств защиты компьютерных информации.

В этом вопросе правоприменительная практика уделяет особое внимание. На суде суд подчеркивает, что обвиняемый осознает назначение данной программы или компьютерной информации. Описывают как бы «лицо» в прямом смысле слова, то есть оно имеет прямой умысел.

Кроме того, в приговоре Свердловского районного суд г. Костромы в качестве характеристики объективной стороны преступления сказано:

«в соответствии с заранее обдуманным намерением, направленным на нейтрализацию средств защиты компьютерной информации, сознательно зная незаконный характер своих действий, заведомо понимая незаконный характер своих действий, заведомо сознавая незаконный характер своих действий, умышленно зная незаконный характер своих действий, сознательно желая нейтрализовать средства защиты компьютерной информации.

2.3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Техническое оборудование в виде компьютеров и связи на основе информационно-телекомуникационных сетей является необходимым для информационного общества в целом и цифровой экономики в частности, так как оно позволяет осуществлять связь с помощью современных технологий. Обеспечение стабильной работы этого оборудования – залог стабильности экономических и социальных процессов, основывающихся на информационно-цифровых принципах Все действия по работе с цифровой системой должны быть согласованы с локальными нормативно-правовыми документами (локальными нормативными актами), содержащими правила работы в данной сфере, регулирующие обязанности ответственных лиц и определенные запреты.

Преступление по статье°274 является защитой компьютерной информации в соответствии с правилами о защите информации от неправомерных действий, которые совершаются с нарушением определенных правил [Абдулвалиев, с. 217].

Согласно Федеральному закону от 07 декабря 2011 года № 420-ФЗ «О внесение изменений в Уголовный кодекс Российской Федерации» данная статья была значительно изменена Федеральным законом от 07 декабря 2011 года № 421-ФЗ «О внесении изменений в УК РФ и отдельные законодательные акты Российской Федерации». Согласно статьи 271 УК РФ, в данной статье законодатель отказался от понятия «ЭВМ», «систем» и «информации» в пользу актуального понятийно-категорийного аппарата.

Как и все действия, предусмотренные гл. 28 УКРФ, нарушение правил эксплуатации средств хранения, обработке или передачи электронной информации и информационно-телекоммуникационной сети (ИТС) посягает на общественные отношения в области компьютерной информации.

Такое представление об объекте правонарушения не соответствует действительности. В данном случае речь идет о средствах обработки

или передачи охраняемой компьютерной информации (компьютерной техники) или информационно-телекоммуникационных сетей и оконечного оборудования. В соответствии с пп. «а» пп. «б» ст. 274 УК РФ, в диспозиции ст.°274 УК РФ содержатся данные термины, но в данном случае необходимо различать понятие предмета правонарушения и средств правонарушения Как известно, в уголовно-правовой науке догматичным является соотношение данных понятий: «предмета — это то, что подвергается преступлению для нанесения вреда объекту посягательств; орудия и средства — при помощи(посредством) чего преступление совершается». По логике и при прямом толковании признаков преступления, предусмотренного статьей 274 УК РФ, очевиден тот факт, что средства хранения, обработки или транспортировки охраняемой компьютерной информации, информационно- телекоммуникационные сети и оконечное оборудование – это то, с помощью чего происходит вред, а непосредственные изменения (следствия) происходят.

Как уже говорилось ранее, предметом рассматриваемого состава правонарушения является именно электронно-вычислительная машина или компьютерная информация (понятие и специфику компьютерной информации, как предмета преступлений, предусмотренных гл. 28 УК РФ.

При этом, если говорить об объективной стороне, то она заключается в нарушении правил эксплуатации и правил доступа. С учетом этого положения в статье 274 УК РФ содержится бланкетная диспозиция Эти правила содержатся в различных нормативных актах. Авторы указывают на то обстоятельство, что в таких актах могут быть федеральные законы, постановления Правительства Российской Федерации или правила, инструкции, предписания, к примеру, такие как Общероссийские Временные санитарные нормы и правила для вычислительного центра, паспорта качества, технические описания и инструкции по эксплуатации, а также инструкции по применению компьютерных программ.

Так, например, в литературе высказывается мнение о том, что основная проблемой применения ст.°274 УК РФ является отсутствие какой-то системы

правил и инструкций в этой сфере, а также процедуры их принятия и довода до исполнителей.

С другой стороны, согласно действующему законодательству, в правоприменительной деятельности по данной категории дел должны быть установлены нормативно-правовой акт, регламентирующий те или иные вопросы работы со средством хранения, обработки или передачи охраняемой информации, информационно-телекоммуникационных сетей и оконечного оборудования. По своей юридической природе такие нормативно-правовые акты являются локальными. А также есть упоминания в судебной практике об аттестате соответствия автоматической системы в защищенном исполнении, Аттестованном удостоверении о соответствии автоматизированной системы в защищённом исполнении, Инструкции по защите информационной информации при ее автоматизации в защищённом исполнении и др. Данные нормативно-правовые акты были приняты на уровне предприятия и регулируют правила доступа к компьютерной информации, которая обрабатывается в служебно-вычислительной системе.

Нарушением является нарушение нормы права, регулирующей данное поведение субъекта. На основании этого приговора в приговоре нужно отразить пункт правил, противоречащий действию или бездействию.

На данный момент диспозиция ст.°274 УК РФ содержит в себе средства совершения преступления. К ним относятся средства хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекомуникационные сети и оконечное оборудование.

На законодательном уровне понятие средств хранения, обработки или передачи охраняемых компьютерных данных не закреплено. По этому поводу существует множество определений этого слова, которые можно найти в различных научных трудах. По мнению некоторых авторов, средства хранения данных и другие информационно-телекоммуникационные устройства являются составной частью компьютеров и иных информационно-телекоммуникационных устройств. Третьи утверждают, что такими средствами

являются любые электронные (цифровые)устройства, способные работать с различными данными, и электронные (машинные) носители информации. При рассмотрении дел в судах, связанных с использованием вычислительной техники, часто используется термин «использование вычислительных мощностей неиспользуемого компьютера».

Основное отличие этих определений заключается в том, что они содержат суть рассматриваемых средств хранения данных, обработки или передачи компьютерной информации и имеют отличия друг от друга незначительно.

Исходя из этого можно сделать вывод о том, что существующее понятие средств хранения, обработки либо транспортировки компьютера является достаточно емким и позволяет отнести его к самому разнообразному компьютерному оборудованию [Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, с. 9].

Это важно подчеркнуть, что законодатель не случайно в диспозиция ст. 274 УК РФ включил обязательный признак компьютерной информации – охран способность закона. Этот факт говорит о том, что для хранения и обработки данных необходимо использовать только защищенные компьютерные системы. Здесь может оказаться информация о частной жизни человека (например его имя, адрес, телефон), а также сведения о государственной, коммерческой, банковской, налоговой, семейной или иной охраняемой законом тайне.

Например, в качестве примера из судебной практики можно привести решение Саровского городского суда Нижегородской области по делу об административном правонарушении, согласно которому виновный использовал служебные вычислительные сети предприятия, предназначенные для обработки секретной информации уровня конфиденциальности «для служебного пользования», «персональные данные» и «коммерческая тайна».

В данном случае, в процессе производства по уголовному делу необходимо установить вид компьютерной информации и определить нормативно-правовой акт, который охраняет данную информацию.

Согласно пп.°2 п.2 ст.2 Федерального закона от 27.07. 2006 № 149-ФЗ «Об информации, информационных технологиях и об защите информации" информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по сетям связи информации, доступ к которой осуществляется посредством использования средств вычислительной техники.

Самая распространенная в России информационно-телекоммуникационная сеть – это сеть «Интернет». Однако существует еще и другие (например, Единая система электросвязи РФ, сети связи Министерства обороны России) Здесь речь идет о том, что в данной судебной практике использовались служебные вычислительные сети одного из Федеральных государственных унитарных предприятий [Русскевич, с. 90].

Подразумевается и законодательная дефиниция, которая включает в себя понятие «оконечное оборудование». Статья 2 Федерального закона от 07.07 2003 № 126-ФЗ "О связи" гласит: Пользовательское оборудование (оконечное оборудование), которое находится в пользовании абонентов или предназначено для таких целей, является техническим средством для передачи и (или) приема сигнала электросвязи по линиям связи, которые находятся в пользовании абонентов или предназначены для таких целей.

По делам, в которых фигурирует оконное оборудование, правоприменительная практика складывается из производства административных правонарушений, предусмотренных ст. 13 КоАП РФ [Русскевич, с. 90], и гражданских дел. При рассмотрении данного вопроса, к виду оконечного оборудования правоприменителей относят также и такие устройства как телевизор, TV-тюнер, роутер, модем, телефон, абонентская станция цифровых радиосистем беспроводного подключения. По данным судебных актов, в указанных судебных актах указывается факт подключения данного оборудования к информационно- телекоммуникационной сети «Интернет»

или другого доступа к услугам связи. Таким образом, под понятие оконечного оборудования входят почти любые технические средства и устройства, отвечающие критериям Федерального закона от 07.07.2003 № 126-ФЗ «О связи».

В соответствии с конструкцией состава уголовного преступления, предусмотренного ст. 274 УК РФ [Тимошенко, с. 38], материальный состав преступления заключается в том, что он предполагает два следствия, имеющих значение именно в своей совокупности – это материальное и процессуальное.

1) Разрушение и удаление компьютерных данных, а также модификация или копирование компьютерной информации.

2) Крупный ущерб.

В рамках рассмотрения состава преступления, предусмотренного статьей 272 УК РФ, были приведены особенности последствий в виде уничтожения, блокирования или модификации компьютерной информации. С учетом вышесказанного, нет никакой специфики в данном составе преступлений

Применительно к понятию «большой ущерб» необходимо отметить следующее. Статья 272 УК РФ гласит: «Крупным считается нанесенный крупный материальный ущерб, превышающий 1 млн рублей». Исходя из этого факта следует предположить то обстоятельство, что законодательный орган определил формальные критерии данного последствия, которое можно было бы отнести в разряд формально-определенного вида. При применении новой редакции УК РФ в отношении последствий данного состава преступления используется термин «значительный ущерб», который является оценочным [Бриллиантов, с. 261].

В судебной системе существует практика отнесения крупного ущерба к категории оценочной. Не менее примечательным является Апелляционное постановление Мосгорсуда, в котором суд процитировал мнение прокурора, внесшего апелляционное представление. В нем суд указал, что размер ущерба, нанесенного обществу, превышает один миллион рублей. Моральный, материальный, а также ущерб деловому имиджу могут

быть причинены в результате нарушения режима секретности, нарушения правил охраны труда, нарушения правил эксплуатации оборудования, нарушения правил техники безопасности. Исходя из нашего мнения, данный способ правоприменителя противоречит законодательному подходу, изложенному в примечании 2 к ст.272 УК РФ, согласно которой единственный критерии для определения степени тяжести вреда - это его объем - более одного миллиона рублей. Негативное мнение основывается на расширительном толковании уголовного законодательства и нарушает принцип законности.

При этом ч.°2 ст.°274-й статьи предусматривает ответственность за совершение преступления, при котором наступает угроза его совершения. Это не только показатель, но и оценка, которая должна быть проведена с учетом всех обстоятельств.

Московский областной суд рассмотрел уголовное дело по обвинению лица в преступлении, предусмотренном ч. 1 ст. 274 Уголовно-процессуального кодекса РФ, и вынес постановление о прекращении уголовного дела, где учтя все обстоятельства совершенного деяния, оценил возможные последствия совершенного деяния, которые могут быть связаны с восстановлением доступа к базам данных и проведением комплекса мероприятий по восстановлению доступа к базам данных. Общую сумму ущерба, нанесённого пострадавшему, составил 1°155°600 рублей.

С учетом этого обстоятельства, квалификация рассматриваемого преступления должна быть проведена с учетом всех последствий, указанных в диспозиции статьи 274 УК РФ. Однако, по мнению некоторых авторов, в данном случае речь идет о субъективной стороне преступления, где говорится о форме вины, но это объясняется тем, что в тексте статьи нет прямой ссылки на форму вины, в связи с чем мнения ученых разделились. По мнению других, умысел может быть как прямой, так и косвенный; третьи же утверждают, что такое преступление возможно только по неосторожности. На основании этого подхода делается вывод о том, что лица, которые нарушили требования правил эксплуатации средств хранения, обработки или передачи охраняемых

компьютерных данных, либо информационно-телекоммуникационных сетях и оконечного оборудования, а равно правила доступа к информационно-телекоммуникационным сетям могут неправильно оценить риски уничтожения, блокирования, модификации либо копирования [Голованова, с. 194].

Правоотношения по рассматриваемой категории дел имеют достаточно сложную правовую конструкцию, мы считаем необходимым подчеркнуть возможность неосторожной формы вины в случае совершения правонарушения или преступления. Здесь законодателем был использован юридический подход, который позволил ему сконструировать данный состав правонарушения – отсутствие указания на форму вины. По этой причине, состав правонарушения предполагает возможность совершения данного преступления в состоянии невменяемости.

В данном случае мотив и цель преступления не имеют никакого значения.

Негативная судебная практика по данной категории дел отсутствует. Существую единичные случаи, когда виновные лица привлекаются к уголовной ответственности Можно объяснить и этим – это обусловлено конструкцией объективной стороны состава преступления по статье 274 УК РФ, определяющей обязанность обязательного характера причинения ущерба в виде уничтожения, блокирования или модификации компьютерной информации, а также крупного ущерба. Примером может послужить дело, связанное с использованием вычислительных возможностей компьютерного оборудования и служебной электронной вычислительной сети для майнинга (майнинга) криптовалюты. Но обстоятельства дела таковы что они являются работниками одной федеральной государственной организации. В нарушение правил эксплуатации средств хранения и обработки информации они установили на компьютеры этого предприятия специальное программное обеспечение, которое внесло изменения в имеющуюся компьютерную информацию, которая содержала персональные данные, коммерчекую и государственную тайну. Оно использовалось для вычисления криптовалютаю во время ночного времени и давало им возможность избежать ответственности за содеянное. Необходимость

в проведении внеочередной повторной аттестационной проверки системы защиты в защищенном исполнении возникла вследствие необходимости проведения внеочередной повторной аттестации автоматизированной системы защиты в защищенном исполнении. В результате предприятие понесло убытки в размере 1°140°157 руб., что составляет крупный ущерб, в результате виновные понесли уголовное наказание.

Другой случай связан с копированием одним работником фирмы на флешь носитель информации о гражданах данной фирмы, содержащей их персональные данные. Нарушение было совершено в нарушение соглашения о сохранении служебной, коммерческой и личной тайны и должностной инструкции ведущего системного администратора. Сумма ущерба, причиненного юридическому лицу вследствие устранения негативных последствий совершенного деяния, составила 1°155°600 рублей (крупнейший ущерб). Лица, которые совершили это преступление были освобождены от уголовной ответственности в связи с истечение сроков давности.

В литературных изданиях выражается мнение о рассматриваемой возможности декриминализации данного состава преступления. Фактически действия, связанные с нарушением правил обработки компьютерной информации либо информационно-телекоммуникационных сетей не представляют общественной опасности. Однако порождаемые негативные последствия в виде нанесения ущерба создают необходимость для уголовно-правовой защиты интересов потерпевшего. Таким образом, декриминализация рассматриваемого преступления является преждевременной и недостаточно обоснованной.

2.4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

В рассматриваемой нами гл. 28 УК РФ на основании законодательной нормы № 194-ФЗ от 26.07.2017 «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»» была дополнена ст. 274.1, предусматривающей уголовную ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации [Евдокимов, с. 78].

Как отмечали авторы проекта указанного Федерального закона, «учитывая необходимость повышенной уголовно-правовой защиты безопасности критической ин формационной инфраструктуры Российской Федерации, целесообразно выделение составов посягательств на критическую информационную инфраструктуру Российской Федерации в отдельную статью» [Русскевич, с. 101].

Как уже говорилось ранее, данный состав преступления имеет новое свойство – критическая информационно-коммуникативная инфраструктура Российской Федерации. Понятие критической информационной инфраструктуры РФ содержится в Федеральном законе от 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации». Рассматриваемая правовая норма подразумевает под критической информационной инфраструктуру критического информационного пространства (критическая информационная инфраструктура), а также сети электросвязи, используемые при организации взаимодействия таких объектов. Но при этом объекты критической информационной инфраструктуры – информатизация субъектов критической информационной инфраструктуры и их информационное обеспечение (информационное обеспечение). Существующие субъекты критической информационной инфраструктуры – федеральные органы исполнительной власти, государственные учреждения,

российские юридические лица, а также индивидуальные предприниматели, которым на праве собственности принадлежит информационная система, информационно-телекоммуникационные сеть, автоматизированная система управления, функционирующая в сфере здравоохранения, науки, транспорта [Галахова, с. 311].

Но в данном случае это не так уж и сложно понять – ведь слово «дефиниция» имеет довольно витиеватый смысл, который заключается в том, что оно определяет понятие через повторение одних и тех же (или близких по значению и смыслу) слов Если же термин «критическая информационная инфраструктура» имеет место быть, то он должен быть описан через объекты и субъекты критической информации, что не соответствует действительности.

Научно-популярная литература содержит примеры критической информационной структуры: информационно – телекоммуникационные сети государственных органов, а также информационно - телекоммуникационные сети и автоматизированные системы управления технологического процесса, функционирующие в оборонной промышленности; в области здравоохранения, транспорта, связи.

В судебной практике встречаются случаи, когда объектом критической информационной структуры признаются сайты, размещенные в информационно°-°телекоммуникационной сети «Интернет». При оценке данных сайтов с точки зрения Федерального закона от 26.07.2018 N2 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» суд отметил, что эти электронные ресурсы являются «электронной информационной системой взаимодействия, Роскомнадзора Российской Федерации с телекоммуникационными операторами» [Боровиков, с. 218].

Но в соответствии с Федеральным законом от 26.07.2017 N 2 187-ФЗ «О безопасности критичной информационной инфраструктуры Российской Федерации» реестр значимых объектов критической информационной

инфраструктуры необходимо вести на основании данных о значимых объектах критической информационной инфраструктуры. Как предполагается, в данный реестр будут включены сведения об объекту и субъекте критической информационной инфраструктуры (критической информационной инфраструктуры), о взаимодействии значимого объекта критической информатизации и сетей электросвязи и т.д. В этой связи в качестве одного признака объекта критической информационной инфраструктуры можно указать включение данного объекта в вышеназванном реестре. Но сейчас реестр значимых объектов критической информационной инфраструктуры пока что не создан. Отсутствие в реестре такого реестра затрудняет квалификацию, оставляя право отнесения соответствующего ресурса к объектам критической информационной инфраструктуре на усмотрение правоприменителя [Боровиков, с. 220].

Так, предметом рассматриваемого правонарушения является критическая информационная структура РФ как совокупность соответствующих ей субъектов (критическая информация). С точки зрения юридической стороны состав преступления, предусмотренного ч. 1 ст. 274 УК РФ, аналогичен составу преступления, предусмотренного ч. 1 статьи 273 УК РФ. Также здесь говорится на совершение деяния, которое заключается в создании, распространении и (или) использовании компьютерных программ либо иной компьютерной информации. Это средство предназначено для уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты указанной информации. Неправомерное воздействие на критическую информационную инфраструктуру Российской федерации осуществляется посредством специальных средств, которые имеют название «критическая информационная инфраструктура» [Галахова, с. 316].

Согласно ч.°2 ст.°274.1 ГУК РФ, «объективная сторона» состава преступления в отношении лиц, которые являются потерпевшими по делу, почти тождественна «объективной стороне» состава преступления, предусмотренного ч.°1 ст.°272°УК°РФ. В данном случае речь идет о неправомерном доступе

к защищаемой компьютерной информации. Отличается только то, что эта информация содержится в критической информационной структуре России и вред, как следствие, причиняется именно критической информационной структуры РФ.

С точки зрения юридической стороны состав преступления, предусмотренного ч.°3 статьи°274.1 УК РФ аналогичен составу преступления, предусмотренного ч.°1 статьи°274 УК РФ. На данный момент штраф за нарушение правил эксплуатации средств хранения, переработки или передачи охраняемой компьютерной информации либо правила доступа к информации, информационным систем, информационно-телекоммуникационным°сетям, автоматизированным системам управления и сетям электросвязи. Отличием также является то, что данные объекты относятся к критической информационной инфраструктуре РФ С этим связано и последствие, которое заключается в нанесении ущерба критической информационной инфраструктуре РФ.

Фактически ст. 274.1 Уголовного Кодекса Российской Федерации является специальной по отношению к ст.272, 273, 274. Исходя из вышесказанного можно сделать вывод о том, что наиболее подходящей с точки зрения юридической техники является конструирование состава преступлений по ст. 272-274 УК РФ, с учетом включения в него квалифицирующих признаков, относящихся к совершению данного деяния в отношении объектов критической информационной инфраструктуры. Действительно данный метод позволил бы исключить проблемы определения конкуренции правовых норм, а также с возможным применением двойной ответственности. [Чуманов, с. 131].

Субъективная сторона каждого состава преступления имеет свои особенности. В данной статье необходимо наличие прямого умысла; в этой же статье – либо прямой, либо косвенный умысел; в этой же статье°–°либо неосторожность, либо прямой умысел.

В литературе можно встретить мнение о том, что состав преступления по статье 274.1 УК РФ является «мертворожденной» нормой. Как правило,

в подобных случаях авторы ссылаются на небольшое количество лиц, привлекаемых к уголовной ответсвенности, и отмечают отсутствие разъяснений Пленума ВС России по всем преступлениям в сфере компьютерной техники.

И действительно, правоприменительная деятельность не отличается многообразием и разнообразием. Только на одном из них мы можем найти информацию о том, что в каком-то случае была проведена проверка.

Одно преступление связано со специализированным сайтом, размещенным в виде сайта на информационно-телекоммуникационной сети «Интернет». На данный момент этот сервис предназначен для нагрузочного тестирования интернет ресурсов посредством отправки большого количества HTTP-запросов А это значит что в данном случае виновный отправил эти запросы на сайты, которые суд счел объектами критической информационной структуры В течение восьми минут на данные объекты было направлено значительное количество HTTP-запрос, что могло привести к невозможности получить доступ к информации, размещенной на указанных веб-сайтах, для других лиц или информационных систем (например, заблокировать информацию). Лицо было освобождено от уголовной ответственности за активное раскаяние.

Следующее уголовное дело было возбуждено по факту использования вредоносных компьютерных программ, которые были использованы для обнаружения открытых портов; нейтрализации средств защиты компьютера с помощью перебора логина и пароля; создания и модификации компьютерной информации с использованием вредоносной компьютерной программы. По результатам проведенного расследования, виновные получили удаленный доступ к компьютерам одного крупного акционерного общества, являющегося субъектом оборонной промышленности. Судебная инстанция установила, что вред выразился в модификации компьютерной техники и воздействий на компьютерную технику и технику, следствием чего явилась невозможность осуществления требуемых операций над компьютерной информацией полностью или в требуемой степени. Данные меры были предприняты для ограничения и закрытия доступа к компьютеру, находящемуся на нем,

а также к хранящейся на нем информации. В отношении фигурантов дела было вынесено обвинительное заключение по ч. 4 ст. 274.1 УК РФ.

На основании анализа проблем классификации уголовных дел по компьютерным преступлениям можно сделать вывод, что сложность имеет относительную новизну рассматриваемых деяний и связана с их высокой сложностью. В большинстве своем, все они были подвергнуты существенным изменениям за последние несколько лет. Для того чтобы избежать путаницы, законодатель отказался от некоторых уже привычных понятий и стал использовать более современную терминологическую базу, отвечающую современным требованиям в области науки и техники [Тимошенко, с. 47].

При этом правоприменительная практика в сфере компьютерной информации осложняется тем, что правоотношения, связанные с компьютерной техникой, регулируются отдельными нормативно-правовыми актам, которые регулярно меняются и дополняются. Вместе с тем правоприменительная деятельность по данным категориям споров становиться всё менее разнообразной и более распространенной, что безусловно улучшит защиту отношений в сфере компьютерной информации.

ЗАКЛЮЧЕНИЕ

Законодательные новеллы и статистические сведения свидетельствуют о теоритическом и практическом совершенствовании механизмов, не только выявления, но и привлечения к уголовной ответственности, а также повышении межотраслевого взаимодействия правоохранительных органов с техническими специалистами в области информационных технологий.

«Цифровое пространство» имеет ряд особенностей таких как трансграничность и отсутствие государственно-властного элемента. Рассмотрены различные подходы к месту совершения преступлений, наиболее обоснованным считается по месту совершения действий (бездействий) содержащих все признаки состава преступления.

В результате рассмотренных признаков преступлений, совершаемых с использованием информационных технологий и проведенного сравнительно-правового анализа понятий «информационные технологии» и «компьютерная информация» пришли к выводу о необходимости введения понятия «преступления совершаемые с использованием информационных технологий», включающие в себя помимо преступлений предусмотренных главой 28 УК РФ более широкий спектр правонарушений совершаемых с помощью информационных технологий.

Используя комплексный подход к преступлениям в сфере компьютерной информации нами приведена, классификация киберпреступлений по способу совершения деяния; по объекту преступного посягательства; по характеру и степени общественной опасности; по группа общественных отношений. В результате чего пришли к выводу о необходимости внесения дополнений в ст. 63 УК РФ о использовании информационно-телекоммуникационной сети «Интернет».

Проанализирован зарубежный опыт противодействия преступлениям в сфере компьютерной информации представителей романо-германской и англо-саксонской правовой системы. Активные меры по совершенствованию механизмов регулирования данной сферы прослеживаются повсеместно,

однако без единого международного подхода весьма затруднителен. В связи с чем необходима унификация понятий. Выделения общих признаков преступлений и уход от абстрактных формулировок свойственных англо-саксонской правовой системе значительно способствовало бы совершенствованию правовых механизмов.

Отечественная правовая система активно развивается в сфере противодействия компьютерным преступлениям, однако в настоящее время не все проблемные вопросы при квалификации преступлений решены.

В ходе анализа судебной практики в сфере неправомерного доступа к компьютерной информации выявлено, что обстоятельством подлежащим установлению является правовая охрана соответствующей компьютерной информации, где именно «активные» действия порождают уголовный состав, при наличии определенного намерения, которое реализуется, как правило, в форме прямого умысла.

При анализе понятийного аппарата ст. 273 УК РФ «создание, использование и распространение вредоносных компьютерных программ», понятие именно «вредоносной» компьютерной программы законодательного отражения не нашло, как и понятие «средства защиты компьютерной информации». Таким образом законодатель отдает приоритет не «охраняемости законом», а «несанкционированности» доступа к компьютерной информации.

Применительно к ст. 274 УК РФ «нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно°-°телекоммуникационных сетей» характерно законодательное отсутствие единой системы правил и инструкций в данной области, а также процедуры применения и доведения до исполнителей. Наличие отдельного признака – ущерба свыше одного миллиона рублей, в судебной практике носит оценочный характер и включает в себя в т.ч. угрозу их наступления, что порождает различные споры.

Выделение отдельного признака – «критическая инфраструктура», в ст. 274.1 УК РФ «неправомерное воздействие на критическую

информационную инфраструктуру Российской Федерации», не в полной мере отражает сущность термина, а лишь приводит общее понимание объектов. При наличии такого подхода, наиболее целесообразно разработать реестр объектов. Специфичность нормы, затрудняет правоприменительную практику, как следствие и совершенствование уголовно-правовых механизмов.

Цифровизация общества наступает интенсивными темпами, что порождает новые вызовы перед международно-правовым и отечественным законодательством, консолидация и унификация международных правовых подходов способствовала бы выработке эффективных механизмов правового регулирования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Книжные издания

Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (с изм. и доп., вступ. в силу с 01.07.2021) // Правовая система «КонсультантПлюс».

Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации Решение Высшего Евразийского экономического совета от 11.12.2020 № 12 "О Стратегических направлениях развития евразийской экономической интеграции до 2025 года

Уголовно-юрисдикционная деятельность в условиях цифровизации: монография / Н.А. Голованова, А.А. Гравина, О.А. Зайцев и др. М.: ИЗиСП, КОНТРАКТ, 2019. с. 212.

Гражданско-правовое регулирование договорных отношений в сфере телекоммуникационных услуг: Монография. Кузнецова О.А. Гражданско-правовое регулирование договорных отношений в сфере телекоммуникационных услуг: монография. М.: Юстицинформ, 2018. с. 208

Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования: монография / [А. Ф. Абдулвалиев и др.; под науч. ред. проф. Е. В. Смахтина, проф. Р. Д. Шарапова, доц. В. И. Морозова] Министерство науки и высшего образования Российской Федерации, Тюменский государственный университет, Институт государства и права. - Тюмень: Издательство Тюменского государственного университета, 2021. - 376 с.

Тимошенко Ю.А. Место совершения преступления: уголовно-правовой и процессуальный аспекты // Законность. 2015. N 7. с. 543.

Молодкин В.М. Статья 157 УК РФ: к вопросу о времени совершения преступления // Вестник исполнительного производства. 2019. № 3. с. 617.

Уголовное право России. Общая и Особенная части: учебник / А.А. Арямов, Т.Б. Басова, Е.В. Благов и др.; отв. ред. Ю.В. Грачева, А.И. Чучаев. М.: КОНТРАКТ, 2017. 384 с.

Каримов В.Х. Актуальные вопросы борьбы с преступлениями, совершаемыми с использованием систем анонимизации пользователей в сети Интернет // Российский следователь. 2018. № 6. с. 311.

Конфиденциальность и защита информации при телемедицинских консультациях. Методические рекомендации № 2003/46

Перов В.А. О криминалистической методике выявления преступлений, совершаемых с использованием криптовалюты, и расследовании соответствующих уголовных дел // Российский следователь. 2020. № 12. с. 117.

Грачева Ю.В., Коробеев А.И., Маликов С.В., Чучаев А.И. Уголовно-правовые риски в сфере цифровых технологий: проблемы и предложения // Lex russica. 2020. № 1. с. 259.

Глушков В.М., Амосов Н.М., Артеменко И.А. Энциклопедия кибернетики. Киев, 1974. с. 451.

Винокуров В.Н. Объект преступления и предмет уголовно-правового регулирования // Современное право. 2020. № 5. с. 71 - 79.

Кадников Н. Г. Классификация преступлений по уголовному праву России. М.: Юрид. изд-во МВД РФ, 2000. с. 5-16.

Чуманов Е. В. Гносеологическая функция классификации в российском праве // Науч. тр. филиала МГЮА в г. Кирове. № 10. Киров, 2005. с. 163.

Пастухов П.С. «Электронные доказательства» в нормативной системе уголовно-процессуальных доказательств / под ред. О.А. Кузнецовой, В.Г. Голубцова, Г.Я. Борисевич, Л.В. Боровых, Ю.В. Васильевой, С.Г. 66 Михайлова, С.Б. Полякова, А.С. Телегина, Т.В. Шершень // Пермский юридический альманах. Ежегодный научный журнал. 2019. № 1. с. 707.

Далгалы Т.А. Киберкриминология: вызовы XXI века // Российская юстиция. 2020. № 10. с. 12.

Уголовное право России. Общая и Особенная части: учебник / А.А. Арямов, Т.Б. Басова, Е.В. Благов и др.; отв. ред. Ю.В. Грачева, А.И. Чучаев. М.: КОНТРАКТ, 2017. 384 с.

Оценочные признаки в Уголовном кодексе Российской Федерации: научное и судебное толкование: научно-практическое пособие / Ю.И. Антонов, В.Б. Боровиков, А.В. Галахова и др.; под ред. А.В. Галаховой. М.: Норма, 2014. 736 с.

Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации

Русскевич Е.А. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ): вопросы квалификации // Уголовное право. 2020. № 5. с. 94 - 104.

Евдокимов К.Н. Особенности субъективной стороны состава преступления при нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) // Мировой судья. 2019. № 6.

Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ.

Методические рекомендации по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса

Электронные издания

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Правовая система «КонсультантПлюс».

Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрат» // Правовая система «КонсультантПлюс».

Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев

значимости объектов критической информационной инфраструктуры» // Правовая система «КонсультантПлюс».

Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // URL.: https://www.kremlin.ru/acts/bank/41919. (дата обращения: 01.11.2021).

Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // URL.: https://www.kremlin.ru/acts/bank/41460.

Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Правовая система «КонсультантПлюс».

Уголовное право России. Общая и Особенная части: Учебник // Правовая система «КонсультантПлюс».

Ляпидов К.В. Анализ и предложения к действующему Федеральному закону № 187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-коммуникационных сетях» // Правовая система «КонсультантПлюс».

Приказ ФСБ России от 19.06.2019 № 282, «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры РФ» // Правовая система «КонсультантПлюс».

Приказ ФСБ России от 06.05.2019 № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» // Правовая система «КонсультантПлюс».

Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» // Правовая система «КонсультантПлюс».

Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему» // Правовая система «КонсультантПлюс».