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

Институт права
(наименование института полностью)
Кафедра «Конституционное и административное право»
(наименование)
40.05.01 Правовое обеспечение национальной безопасности
(код и наименование направления подготовки, специальности)
Государственно-правовая
(направленность (профиль) / специализации)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (ДИПЛОМНАЯ РАБОТА)

на тему «Информационные правонарушения как угроза национальной безопасности»

Обучающийся А.Ч. Нигматов _____
(Инициалы Фамилия) (личная подпись)

Руководитель к.ю.н., доцент А.А. Мусаткина
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2022

Аннотация

Тема работы: «Информационные правонарушения как угроза национальной безопасности».

Актуальность исследования. При рассмотрении проблемы информационных правонарушений будет проведен анализ воздействия информационных правонарушений на национальную безопасность государства. На сегодняшний день, информация – это данные, сообщения и сведения, для которой довольно часто требуется защита.

В силу происходящей в мире информатизации сегодня многое находится в непосредственной зависимости от информационной безопасности данных, систем, воздействующих на состояние защищенности государства, общества и личности, возможность управления объектами, которые создают непосредственную угрозу для государственной национальной безопасности.

Именно поэтому развитие информационной безопасности должно осуществляться также стремительно, как и развитие информационных технологий, что обусловлено тем, что информационная безопасность затрагивает такие сферы жизни общества, как социальную, техническую, научную, промышленную, военную, экологическую, экономическую, политическую и иные сферы.

Цель исследования – исследовать особенности информационных правонарушений как угрозы национальной безопасности РФ и способы предотвращения таких угроз.

Задачи исследования:

- изучить понятие и сущность информационной безопасности Российской Федерации,
- исследовать особенности правового обеспечения информационной безопасности,
- исследовать понятие и виды информационных правонарушений,

- выявить особенности развития российского законодательства в сфере регулирования информационных правонарушений,
- изучить особенности неправомерного воздействия на критическую информацию инфраструктуры Российской Федерации,
- изучить особенности нарушения правил хранения, обработки и передачи информационных сведений,
- исследовать особенности использования и распространения вредоносных компьютерных программ,
- провести анализ особенностей неправомерного доступа к информационным сведениям.

Структура исследования. Работа состоит из введения, трех глав, заключения, списка используемой литературы и используемых источников. Работа включает в себя 70 страниц, 1 таблица и 2 рисунка.

Оглавление

Введение

Актуальность исследования. При рассмотрении проблемы информационных правонарушений будет проведен анализ воздействия информационных правонарушений на национальную безопасность государства. На сегодняшний день, информация – это данные, сообщения и сведения, для которой довольно часто требуется защита.

В силу происходящей в мире информатизации сегодня многое находится в непосредственной зависимости от информационной безопасности данных, систем, воздействующих на состояние защищенности государства, общества и личности, возможность управления объектами, которые создают непосредственную угрозу для государственной национальной безопасности.

Как следует справедливо отметить, к такого рода объектам, прежде всего, относятся системы формирования общественного сознания, банковские системы, системы управления воздушным и наземным транспортом, атомные станции, системы хранения и обработки секретных информационных сведений, телекоммуникационные системы и так далее.

Именно поэтому развитие информационной безопасности должно осуществляться также стремительно, как и развитие информационных технологий, что обусловлено тем, что информационная безопасность затрагивает такие сферы жизни общества, как

- социальную,
- техническую,
- научную,
- промышленную,
- военную,
- экологическую,
- экономическую,

– политическую и иные сферы.

Степень изученности проблемы исследования. Теоретический анализ понятия и сущности информационной безопасности Российской Федерации был представлен в работах таких ученых, как В.А. Мазурова, В.В. Невинского, Д.С.-К. Велиева, О.В. Ясенева, А.Л. Сочкова, А.В. Дорожкина, В.Н. Ясенева и других ученых, которые в собственных научных трудах предпринимали попытки дать определение термину «информационная безопасность».

Сущность и структура информационной безопасности Российской Федерации рассматривалась в научных трудах А.Д. Чеснокова, Д. Устиновой, В.В. Невинского, В.А. Мазурова и других исследователей.

В работах К.Е. Израилова, В.В. Покусова, М.В. Буйневич, И.Н. Гайдаревой, Л.А. Витковой, Д.В. Сахарова, Э.В. Бириха, А.С. Карева и других ученых исследовались правовые особенности обеспечения информационной безопасности государства.

Объект исследования – общественные отношения, которые воздействуют на информационную безопасность.

Предмет исследования - совокупность правовых норм, которые направлены на предупреждение информационных правонарушений.

Цель исследования – исследовать особенности информационных правонарушений как угрозы национальной безопасности РФ и способы предотвращения таких угроз.

Задачи исследования:

– изучить понятие и сущность информационной безопасности Российской Федерации,
– исследовать особенности правового обеспечения информационной безопасности,
– исследовать понятие и виды информационных правонарушений,
– выявить особенности развития российского законодательства в сфере регулирования информационных правонарушений,

- изучить особенности неправомерного воздействия на критическую информацию инфраструктуры Российской Федерации,
- изучить особенности нарушения правил хранения, обработки и передачи информационных сведений,
- исследовать особенности использования и распространения вредоносных компьютерных программ,
- провести анализ особенностей неправомерного доступа к информационным сведениям.

Теоретической базой исследования стали работы российских и зарубежных ученых, материалы печатных изданий, монографии, интернет-источники, в которых затрагиваются вопросы исследования проблемы борьбы с информационными правонарушениями, выступающими угрозой для национальной безопасности государства.

Нормативно-правовой базой исследования стали Конституция РФ, федеральные законы и иные нормативно-правовые акты, которые направлены на регулирование и обеспечение информационной безопасности, регулирование информационных правонарушений в РФ.

Теоретическая значимость исследования обусловлена тем, что полученные результаты могут быть использованы для совершенствования правовых норм, направленных на предупреждение информационных правонарушений.

Структура исследования. Работа состоит из введения, трех глав, заключения, списка используемой (ых) литературы и (или) источников.

Во введении определена актуальность и степень изученности проблемы исследования, выделены объект, предмет, цель и задачи исследования, выделена теоретическая и нормативно-правовая база исследования, представлены данные о структуре исследования.

В первой главе «Теоретические основы нормативного регулирования информационных правонарушений» изучены понятие и сущность

информационной безопасности Российской Федерации; исследованы особенности правового обеспечения информационной безопасности.

Во второй главе «Социально-правовая характеристика информационных правонарушений» исследовано понятие и виды информационных правонарушений; выявлены особенности развития российского законодательства в сфере регулирования информационных правонарушений.

В третьей главе «Правовая характеристика информационных правонарушений как угрозы национальной безопасности» изучены особенности неправомерного воздействия на критическую информацию инфраструктуры Российской Федерации; изучены особенности нарушения правил хранения, обработки и передачи информационных сведений; исследованы особенности использования и распространения вредоносных компьютерных программ; проведен анализ особенностей неправомерного доступа к информационным сведениям.

В заключении приводятся краткие выводы, полученные по результатам проведенного исследования.

Список используемой литературы и используемых источников включает в себя 52 библиографических наименования.

Глава 1 Теоретические основы нормативного регулирования информационных правонарушений

1.1 Информационная безопасность РФ: понятие, сущность

Определение «информационной безопасности» было предложено в научных трудах В.А. Мазурова и В.В. Невинского, которые писали, что «информационная безопасность – это защищенность в области распространения, пользования, получения, распределения и выработки информационных данных, а также обеспечение их объективности, соблюдении гарантии тайны и секретности» [16, с. 59].

В научных трудах Д.С.-К. Велиева подчеркивается, что «информационная безопасность в широком понимании является состоянием, обеспечивающим непосредственную защиту государственных национальных интересов в информационном плане, которые определяются совокупностью таких элементов, как:

- личность,
- общество,
- государство» [3, с. 55].

О.В. Ясенев, А.Л. Сочков, А.В. Дорожкин, В.Н. Ясенев и другие исследователи отмечают, что под информационной безопасностью государства требуется понимать невозможность причинения вреда основным свойствам объекта безопасности, обусловленных информационной структурой и информационными сведениями [52, с. 34].

Сущностью информационной государственной безопасности считается формирование на территории государства активной защиты основных интересов, которые связаны с использованием ресурсов информационного характера.

В современных условиях комплексной задачей считается обеспечение информационной безопасности, что продиктовано многоплановостью и сложностью информационной среды.

В Российской Федерации анализ состояния информационной государственной безопасности, в первую очередь, требует реформирования и повышения эффективности в сфере организации обеспечения такого вида безопасности для формирования целостной системы обеспечения государственной информационной безопасности.

Как следует справедливо отметить, система обеспечения информационной безопасности, прежде всего, является составным элементом общей системы государственной национальной безопасности. Именно поэтому такая система предполагает совокупность органов власти, предприятий и управления, которые на основе правовых норм осуществляют деятельность по обеспечению информационной безопасности Российской Федерации.

Согласно научным воззрениям А.Д. Чеснокова, в структуре информационной безопасности государства могут быть выделены следующие основные элементы:

- финансовый элемент, который непосредственно охватывает системы обмена, финансовых расчетов, а также базы данных и информационные сети;
- экономический элемент, который включает в себя управленческие структуры и системы информационного и телекоммуникационного характера (системы принятия решений, управления, прогнозирования и т.п.);
- инфраструктурный элемент, который позволяет использовать информационные сведения без отрицательного влияния на систему и по назначению;
- состояние информации, затрудняющее или исключающее нарушение ее доступности, конфиденциальности и целостности;

– состояние защищенности информационного пространства, с помощью которого непосредственно осуществляется его развитие и становление в интересах субъектов хозяйствования, граждан и государства [51, с. 480].

В научных изысканиях Д. Устинова отмечалось, что на сегодняшний день основной характеристикой сущности и содержания системы информационной безопасности выступает свойство защищенности, которое подразумевает следующие основные виды защиты:

– пассивная защита;
– активная защита [32, с. 148].

Согласно первому виду защиты предполагается защита, обеспечивающая экономическое и общественное развитие. Основными направлениями в данном виде защиты информации считаются:

– международное сотрудничество;
– развитие ИТ-сектора;
– экономическое развитие;
– развитие онлайн-демократии;
– развитие культуры;
– свобода обращения информации.

Согласно второму виду защиты предполагается предотвращение несанкционированного доступа к сведениям информационного характера. Основными направлениями в данном виде защиты информации считаются:

– международные интересы;
– защита и эксплуатация объектов критической инфраструктуры;
– эксплуатация средств информационной безопасности;
– защита личных данных.

В системе обеспечения информационной безопасности важным аспектом выступает информационная безопасность личности, актуальность которой проявляется при длительном присутствии в виртуальном мире и при

спонтанном взаимодействии информационного характера [18, с. 69]. Необходимо отметить, что информационная безопасность личности включает в своей структуре такие направления, как:

- осуществление защиты здоровья в физическом и психологическом плане от воздействия негативного характера, которое может оказываться при использовании технологий информационного и коммуникационного характера;
- осуществление защиты от агрессивной внешней информации;
- осуществление защиты от заимствования результатов интеллектуальной собственности, представленной в электронном виде;
- обеспечение защиты от некачественной педагогической продукции, которая реализована на базе технологий информационного и коммуникационного характера и не отвечает эргономическим требованиям педагогики;
- осуществление защиты от информационных данных, оскорбляющих моральные чувства и ценности.

Выделим основные функции системы обеспечения государственной информационной безопасности:

- координирование деятельности органов государственной федеральной власти и иных органов, которые решают непосредственные задачи по обеспечению в государстве информационной безопасности;
- осуществление разработки правовой базы регулирования в системе обеспечения государственной информационной безопасности;
- инфраструктурное развитие, развитие средств информационного и телекоммуникационного характера, повышение на внешнем и внутреннем рынке их конкурентоспособности;
- осуществление контроля над деятельностью органов государственной федеральной власти и власти субъектов РФ,

комиссий межведомственного и государственного уровня, которые принимают непосредственное участие в решении основных задач по обеспечению в РФ государственной информационной безопасности;

- формирование ключевых условий для реализации прав объединений общественного характера, граждан на информационную деятельность, разрешенную российским законодательством;
- пресечение, выявление и предупреждение преступлений в информационной сфере, а также осуществление в этом области судебного производства;
- поддержания между потребностями государства, общества и граждан в свободном обмене информационными сведениями, ограничениями на распространение информации;
- осуществление в области обеспечения информационной государственной безопасности международного сотрудничества, а также представление нашего государства в организациях международного уровня;
- развитие и повышение эффективности системы подготовки кадров в сфере государственной информационной безопасности;
- оценка современного состояния государственной информационной безопасности, установление основных источников угроз внешнего и внутреннего характера, а также выявление и оценка основных направления нейтрализации, отражения и предупреждения таких угроз;
- контроль над использованием и созданием существующих средств информационной защиты с помощью обязательного лицензирования деятельности, сертификации средств информационной защиты;
- организация программ обеспечения государственной информационной безопасности на региональном и федеральном уровне, координация реализации таких программ;

– защита информационных ресурсов государства, в частности, в органах государственной власти субъектов РФ и органах федеральной власти, оборонно-промышленных комплексах;
– организация научных исследований прикладного и фундаментального характера в сфере обеспечения государственной информационной безопасности;
– разработка и проведение единой политики технического характера в сфере обеспечения государственной информационной безопасности.

Следовательно, согласно законодательным положениям, под информационной безопасностью принято понимать защищенность информационной общественной среды, которая реализуется в интересах человека, общества и всего государства.

Сущностью информационной государственной безопасности считается формирование на территории государства активной защиты основных интересов, которые связаны с использованием ресурсов информационного характера. В современных условиях комплексной задачей считается обеспечение информационной безопасности, что продиктовано многоплановостью и сложностью информационной среды.

1.2 Правовое обеспечение информационной безопасности

На сегодняшний день, компетенция государственных органов власти регионального и федерального уровня, других государственных органов, которые входят в систему обеспечения государственной информационной безопасности, определяются соответствующим правовым полем, которое включает в себя нормативно-правовые акты, федеральные законы и прочие законодательные акты.

Такое правовое поле направлено на координирование деятельности соответствующих органов, обеспечивающих государственную национальную безопасность.

В результате обеспечения информационной безопасности государство может противостоять информационной преступности, которая, как известно, отрицательно воздействует на информационное пространство. Методы и инструменты системы обеспечения информационной безопасности ориентированы, прежде всего, на осуществление противодействия оружию информационного характера [14, с. 38].

При этом, следует помнить о том, что защита информационной безопасности включает в себя меры, направленные на обеспечение информационной целостности и конфиденциальности информационных сведений при сохранении прав пользователей [11, с. 67].

Основными принципами обеспечения информационной безопасности:

- принцип благоразумности;
- принцип бесперебойности;
- принцип многоуровневой защиты;
- принцип прочности;
- принцип системности [2, с. 83].

Для обеспечения информационной безопасности на территории нашего государства на сегодняшний день сформировано соответствующее правовое поле.

Основными элементами, включенными в систему правового обеспечения информационной безопасности в Российской Федерации, являются:

- деятельность нормотворческого характера, направленная на формирование и совершенствование законодательства в сфере регулирования общественных отношений, непосредственно связанных с обеспечение информационной безопасности в государстве;

– деятельность правоприменительного и исполнительного характера, направленная на исполнение российского законодательства в сфере информатизации, информации, защиты информации государственными органами власти, гражданами, юридическими лицами и органами государственного управления [5, с. 177].

В системе обеспечения информационной безопасности государства деятельность нормотворческого характера, прежде всего, предполагает:

– осуществление разработки законодательных и нормативных актов, которые направлены на регулирование порядка и способов ликвидации основных последствий информационных угроз, реализации мер компенсационного характера, восстановления для субъектов ресурсов и их нарушенных прав;
– разработка механизма организационно-правового характера для осуществления анализа, оценки и сбора данных статистики, касающихся влияния информационных угроз на информационную безопасность государства, а также с учетом категорий информации оценки их последствий;
– формирование соответствующего правового статуса в системе информационной безопасности для всех субъектов и пользователей систем телекоммуникационного и информационного характера, определение ответственности для таких субъектов за обеспечение ими безопасности в информационном пространстве;
– формирование для обеспечения информационной безопасности государства соответствующих механизмов организационно-правового характера;
– оценка и анализ состояния действующего законодательства в сфере обеспечения информационной безопасности, а также разработка основных мероприятий по его совершенствованию и повышению его эффективности.

В свою очередь, деятельность правоприменительного и исполнительного характера предусматривает непосредственное осуществление разработки основных процедур для применения нормативно-правовых актов и российского законодательства к основным субъектам, которые при работе с закрытой информацией совершают преступные деяния, либо совершают правонарушения с применениям незащищенных информационных средств, нарушают регламент осуществления информационного взаимодействия.

Следует при этом подчеркнуть тот факт, что такая деятельность также затрагивает основные вопросы, связанные с разработкой составов преступных деяний с опорой на специфику ответственности дисциплинарного, административного, гражданского и уголовного характера, предусмотренную российским законодательством.

Необходимо отметить, что деятельность, которая ориентирована на осуществления правового обеспечения государственной информационной безопасности, прежде всего, должна выстраиваться на основе следующих фундаментальных правовых положений:

- неотвратимость наказания за совершенные преступные деяния;
- обеспечение необходимого баланса интересов для государства и его отдельных субъектов;
- соблюдение законности.

Как следует подчеркнуть, соблюдение законности в системе обеспечения информационной государственной безопасности должно включать в себя наличие нормативно-правовых актов и законов, а также непреклонное их исполнение в сфере информационной безопасности всеми субъектами права.

Выделим основные элементы нормативно-правовой и законодательной базы, направленной на регулирование системы обеспечения государственной информационной безопасности:

1. Законы Российской Федерации:

– Конституция РФ [13],
– Гражданский кодекс РФ [6],
– Федеральный закон от 27 мая 1996 г. № 57-ФЗ «О государственной охране» [46],
– Федеральный закон от 02 декабря 1990 г. № 395-1 «О банках и банковской деятельности» [49],
– Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» [37],
– Федеральный закон от 10 января 1996 г. № 5-ФЗ «О внешней разведке» [45],
– Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [35],
– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [38],
– Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» [36],
– Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» [9],
– Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» [42],
– Федеральный закон от 31 мая 1996 г. № 61-ФЗ «Об обороне» [43],
– Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» [47],
– Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности» и так далее [48].

2. Нормативно-правовые акты Президента РФ:

– Доктрина информационной безопасности Российской Федерации [26],
– Стратегия национальной безопасности Российской Федерации [25];
– Военная доктрина РФ [4],

– Указ Президента РФ от 7 августа 2004 г. № 1013 «Вопросы Федеральной службы охраны Российской Федерации» [28],
– Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» [29],
– Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении перечня должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне» [30],
– Указ Президента РФ от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации» [31],
– Указ Президента РФ от 6 октября 2004 г. № 1286 «Вопросы Межведомственной комиссии по защите государственной тайны» [27].

3. Нормативно-правовые акты Правительства РФ.
4. Уставы (конституции) субъектов РФ.
5. Законы субъектов РФ.
6. Ведомственные нормативные акты.

Таким образом, компетенция государственных органов власти регионального и федерального уровня, других государственных органов, которые входят в систему обеспечения государственной информационной безопасности, определяются соответствующим правовым полем, которое включает в себя нормативно-правовые акты, федеральные законы и прочие законодательные акты. Такое правовое поле направлено на координирование деятельности соответствующих органов, обеспечивающих государственную национальную безопасность.

Реализация основных механизмов, направленных на правовое обеспечение государственной информационной безопасности, в целом, должно опираться на информатизацию правовой сферы.

Исходя из проведенного анализа теоретических основ нормативного регулирования информационных правонарушений были получены следующие выводы.

Согласно законодательным положениям, под информационной безопасностью принято понимать защищенность информационной общественной среды, которая реализуется в интересах человека, общества и всего государства.

Было установлено, что сущностью информационной государственной безопасности считается формирование на территории государства активной защиты основных интересов, которые связаны с использованием ресурсов информационного характера.

В современных условиях комплексной задачей считается обеспечение информационной безопасности, что продиктовано многоплановостью и сложностью информационной среды.

Компетенция государственных органов власти регионального и федерального уровня, других государственных органов, которые входят в систему обеспечения государственной информационной безопасности, определяются соответствующим правовым полем, которое включает в себя нормативно-правовые акты, федеральные законы и прочие законодательные акты.

Такое правовое поле направлено на координирование деятельности соответствующих органов, обеспечивающих государственную национальную безопасность.

Реализация основных механизмов, направленных на правовое обеспечение государственной информационной безопасности, в целом, должно опираться на информатизацию правовой сферы.

Соблюдение законности в системе обеспечения информационной государственной безопасности должно включать в себя наличие нормативно-правовых актов и законов, а также непреклонное их исполнение в сфере информационной безопасности всеми субъектами права.

Деятельность, которая ориентирована на осуществления правового обеспечения государственной информационной безопасности, прежде всего, должна выстраиваться на основе следующих фундаментальных правовых положений:

- неотвратимость наказания за совершенные преступные деяния;
- обеспечение необходимого баланса интересов для государства и его отдельных субъектов;
- соблюдение законности.

Решение проблем в системе обеспечения информационной государственной безопасности, прежде всего, требует использование мер

- технического,
- программного,
- законодательного,
- организационного характера.

Такие меры непосредственно должны быть использоваться совместно.

Глава 2 Социально-правовая характеристика информационных правонарушений

2.1 Понятие информационных правонарушений и их виды

В сфере компьютерной информации, как следует справедливо подчеркнуть, лишь в 1996 г. были включены нормы о преступлениях, когда был принят УК РФ. Однако с течением времени наблюдается стремительное изменение криминальной ситуации в исследуемой области [8, с. 185].

Преступность в информационной среде, с одной стороны, обрела более профессиональный уровень. Так, ранее лишь отдельные личности занимались хакингом, а в настоящее время существует большое число организованных преступных группировок, которые занимаются информационными преступлениями.

В тоже время, на сегодняшний день наблюдается развитие и совершенствование различных программных инструментов, массовое распространение компьютерных сетей и компьютеров в мире, что, в свою очередь, приводит к тому, что специальное образование уже не требуется для совершения информационных правонарушений. Данная причина обусловливает повышение числа информационных правонарушений.

Компьютерная техника все чаще и чаще используется в преступном мире для совершения деяний преступного характера, которые непосредственно на авторские права, интересы государства, конституционные свободы и права человека, экономические интересы государства. Компьютерные технологии на сегодняшний день также используются для осуществления диверсий. Именно поэтому проблема анализа информационных правонарушений является весьма актуальной проблемой исследования на сегодняшний день.

Многие ученые стремились к введению в оборот конституционного, административного и уголовного права термина «информационные правонарушения». Остановимся на анализе некоторых понятий.

В научных исследованиях В.В. Крылова отмечалось, что «информационные правонарушения представляют собой деяния общественно-опасного характера, которые совершены в сфере правоотношений информационного характера и запрещены российским законодательством под угрозой наказания. Кроме того, необходимо отметить, что исследователь предлагает определение дефиниции «информационные правоотношения»» [15, с. 50]. В собственных трудах ученый пишет, что под информационными правоотношениями требуется понимать «отношения, которые формируются при создании и непосредственном использовании ресурсов информационного характера на базе распространения, создания, поиска, сбора, хранения, накопления, обработки и предоставления информации потребителю; использовании и создании информационных средств и технологий, защите прав субъектов и информации, которые участвуют в процессе информатизации и информационных процессах» [15, с. 50].

Следует отметить тот факт, что предлагаемая попытка стала в определении термина «информационные правонарушения». Однако предлагаемые исследователем идеи не получили в дальнейшем собственного развития. Направленностью данной идеи было исследование информационных компьютерных преступлений, именно поэтому в предлагаемом определении включены такие действия, как клевета, мошенничество, нарушение авторских прав, т.е. различные по природе правонарушения. Мы полагаем, что на сегодняшний день при определении термина «информационные правонарушения» такая группировка не целесообразна и не актуальна.

А.В. Суслопаров писал, что под информационными правонарушениями требуется понимать общественно опасные деяния противоправного

характера, которые непосредственный вред причиняют отношениям общественного характера, связанным с обеспечением информационной безопасности. При этом исследователь отмечает, что основным способом совершения информационных правонарушений считается информационное воздействие, в то время, как предметом информационных правонарушений выступает особый нематериальный объект – информация [19, с. 8].

Мы полагаем, что в предлагаемом определении присутствуют определенные пробелы и недостатки. Одним из недостатков предлагаемого ученым определения считается его избыточность. Так, под информационной безопасностью принято понимать «механизм защиты, который обеспечивает доступность, целостность и конфиденциальность информации» [7, с. 110]. Таким образом, в информационной среде оказание посягательств предполагает, прежде всего, информационное воздействие либо оказание влияния на информационные данные.

В предлагаемом определении можно выделить еще один недостаток, который связан с тем, что определение выходит за рамки традиционной концепции преступления как материальной вещи. В последние годы довольно часто информация в литературных источниках рассматривается в качестве предмета преступления. По нашему мнению, к данному положения нужно относиться критически, так как многие беспредметные преступления обретают предмет, который по сути является лишним. Прежде всего, это обусловлено тем, что многие годы практики и теоретики при квалификации преступлений обходились без него.

Согласно терминологическому определению, предлагаемому в трудах Л.Г. Устьева, «информационные правонарушения – это общественно опасные деяния, совершенные виновно, средством и предметом совершения которых выступает информация, которые запрещены российским законодательством» [33, с. 11].

Мы уже говорили ранее в исследовании о нежелательности использования в определении термина «информационные правонарушения»

понятия «предмет преступления». При этом, необходимо отметить, что весьма сомнительной считается необходимость включения информации в средства совершения исследуемой категории преступных деяний.

Информационные правонарушения, по мнению А.А. Турышева, представляют собой любые преступные деяния, в состав которых включена информация [22, с. 9]. Как заметно, в определении ученого отсутствует конкретизация признаков состава преступления, к которым должна относиться информация.

Следовательно, в современной науке было предпринято много попыток дать определение термину «информационные правонарушения» (таблица 1), однако единое и общепринятое определение так и не было выработано.

Таблица 1 – Подходы ученых к определению понятия «информационные правонарушения»

№	Автор	Определение
1	В.В. Крылов [15]	Информационные правонарушения представляют собой деяния общественно-опасного характера, которые совершены в сфере правоотношений информационного характера и запрещены российским законодательством под угрозой наказания. Кроме того, необходимо отметить, что исследователь предлагает определение дефиниции «информационные правоотношения».
2	А.В. Суслопаров [19]	Информационные правонарушения – это противоправные общественно опасные деяния, которые причиняют непосредственный вред отношениям общественного характера по обеспечению информационной безопасности.
3	Л.Г. Устьев [33]	Информационные правонарушения – это общественно опасные деяния, совершенные виновно, средством и предметом совершения которых выступает информация, которые запрещены российским законодательством
4	А.А. Турышев [22]	Информационные правонарушения представляют собой любые преступные деяния, в состав которых включена информация.

Представленные в таблице определения термина «информационные правонарушения» в качестве отправной точки, как следует справедливо отметить, используют термин «информация». В то же время, по нашему мнению, это весьма широкий термин, потому что может иметь непосредственное отношение к любым сведениям и данным вне зависимости

от носителя. В области информационной международной безопасности в Основах государственной политики РФ отмечается, что основной угрозой требуется считать использование технологий коммуникационного и информационного характера с вредоносными целями [24].

Таким образом, при выделении в качестве особой группы преступлений в основе выделения информационных правонарушений можно заложить использование информационных технологий, а также информационно-телекоммуникационных сетей.

Если обратиться к Федеральному закону «Об информации, информационных технологиях и защите информации» [38], то можно обнаружить, что в законодательном источнике отражено понятие «информационные технологии» и понятие «информационно-телекоммуникационные сети». Диспозиция закона гласит, что информационно-телекоммуникационные сети – это система технологического характера, у которой основной целью считается передача по линиям связи соответствующих информационных сведений, доступ к которым осуществляется с использованием средств вычислительной техники [Там же]. В то же время, информационные технологии – это процессы и методы предоставления, хранения, поиска, распространения, обработки и сбора информационных данных, а также способы их осуществления [Там же].

Таким образом, на основе рассмотренных подходов к определению термина «информационные правонарушения», можно предложить авторское определение данного понятия. Здесь и далее в работе под информационными правонарушениями мы будем понимать общественно опасные деяния, которые совершаются с использованием информационно-телекоммуникационных сетей, информационных средств и технологий, и которые запрещены российским законодательством, предусматривающим установление административной ответственности за их совершение.

Информационные правонарушения могут быть рассмотрены с позиции административно-правового регулирования. Так, информационное административное правонарушение представляет собой виновное и противоправное деяние деликтоспособного лицом, которое было общественно опасным, и совершено с применением информационных технологий и средств работы с информационными данными, совершено в информационной сфере в условиях информационной среды.

В системе информационных правонарушений административного характера ключевым отличительным признаком считается тот факт, что такое правонарушение, прежде всего, посягает на существующий порядок государственного управления в информационной области, т.е. установленный правопорядок в области обеспечения соответствующих свобод и прав гражданина и человека, нравственности и общественного порядка, безопасности в информационной области деятельности человека, определенного порядка государственной власти.

Правопорядок в информационной сфере формируется на основе Конституции Российской Федерации [13], российских федеральных законов и подзаконных актов РФ, непосредственно устанавливающих соответствующие обязанности и права основных субъектов информационной деятельности, в частности, в сфере использования, защиты, передачи и поиска соответствующих информационных систем.

Следует справедливо отметить, что в исследуемом противоправном деянии общественная опасность в большинстве случаях выражена размеров нематериального вреда, который был непосредственно причинен информационным интересам и ценностям государства, общества и личности. Необходимо указать на тот факт, что в зависимости от качества и количества причиненного информационным правонарушением вреда различают основные виды правонарушений, в том числе, административные информационные правонарушения отграничиваются от информационных правонарушений уголовной направленности.

Одним из признаков информационных административных правонарушений выступает противоправность. Так, данный признак подчеркивает направленность исследуемого общественно опасного деяния на нарушение правил поведения, установленных законодательными нормами. В категории информационных административных правонарушений, противоправный характер состоит в том, что довольно часто в нормах российского законодательства, предусматривающих наступление правовой ответственности, дается ссылка на конкретные правила обработки, использования и передачи сведений информационного характера.

Согласно диспозиции ст. 13.14 КоАП РФ [12], за разглашение информационных сведений с ограниченным доступом, т.е. нарушением преступным лицом установленного порядка обработки и соответствующего использования конкретной информации, составляющей тайну, который получил такой доступ к информационным сведениям в результате исполнения обязанностей профессионального или служебного характера.

В Федеральном законе «О коммерческой тайне» представлена дефиниция «разглашение информации, которая составляет коммерческую тайну». Согласно законодательному определению, представленному в п. 9 ст. 3 ФЗ «О коммерческой тайне», разглашение информации, составляющей коммерческую тайну, является бездействием / действием, в рамках которого третьим лицам становятся известны информационные сведения в любой возможной форме (письменная, устная и пр.), вопреки гражданско-правовому или трудовому договору или без согласия обладателей таких информационных сведений.

Объект посягательства в информационном административном правонарушении выделен в гл. 13 КоАП РФ [12], так законодательная диспозиция главы указывает на то, что объектом посягательства в исследуемой категории правонарушений являются отношения общественного характера в области информации и связи. В той же главе сказано, что видовыми (специальными) объектами информационного

административного правонарушения выступают общественные отношения в сфере:

- порядка распространения, предоставления, обработки информационных данных;
- архивного дела и статистики;
- использования средств массовой информации;
- порядка работы информации ограниченного доступа;
- информационной защиты;
- связи.

В Кодексе об административных правонарушениях [12] на сегодняшний день существует много статей, которые предусматривают наступление ответственности административного характера за осуществление виновным лицом информационных правонарушений сфере общественных отношений, связанных с информационной областью. В такого рода информационных правонарушениях общественные информационные отношения выступают специальным объектом, который, в свою очередь, соотноситься с иным родовым объектом. К примеру, отношения общественного характера в области:

- Ст. 19.7.3 «Непредставление информации в Банк России» КоАП РФ [12];
- Ст. 19.7 «Непредставление сведений (информации) КоАП РФ [12];
- Ст. 17.13 «Незаконное представление сведений о защищаемых лицах» КоАП РФ [12];
- Ст. 5.53 «Незаконные действия по получению и (или) распространению информации, составляющей кредитную историю» КоАП РФ [12];
- Ст. 15.22 «Нарушение ведения реестра владельца ценных бумаг» КоАП РФ [12];
- Ст. 15.21 «Неправомерное использование инсайдерской информации» КоАП РФ [12];

– Ст. 8.5 «Сокрытие или искажение экологической информации» КоАП РФ [12];
– Ст. 6.17 «Нарушение законодательства РФ о защите детей от информации, причиняющей вред их здоровью и (или) развитию» КоАП РФ [12];
– Ст. 20.23 «Нарушение правил производства, хранения, пролажи и приобретения специальных технических средств, предназначенных для негласного получения информации» КоАП РФ [12].

Исходя из проведенного анализа, предложено следующее определение термина «информационные правонарушения». Информационные правонарушения – это общественно опасные деяния, которые совершаются с использованием информационно-телекоммуникационных сетей, информационных средств и технологий, и которые запрещены российским законодательством, предусматривающим установление административной ответственности за их совершение.

2.2 Развитие российского законодательства в сфере регулирования информационных правонарушений

В 1970-е годы началось обширное распространение компактных компьютерных систем среди пользовательской аудитории, что, в конечном счете способствовало быстрому развитию технологий информационного характера, а также развитию способов их использования в преступной среде. В силу стремительного развития сети Интернет остро встал вопрос относительно создания и внедрения систем защиты, государственных серверов защиты информационных данных, направленных на ограничение доступа к сети [20, с. 128]. Создание такого рода систем, при этом, привело к повышению количества информационных правонарушений, что было обусловлено появлением профессионалов и схем взлома таких систем.

Инициативной группой Интерпола в начале 1990-х годов была осуществлена попытка формирования единой классификации информационных правонарушений, которая нашла в дальнейшем собственное отражение в Будапештской конвенции Совета Европы 2001 г.

В рамках настоящего исследования следует отметить, что страны G7 до сих пор предпринимают попытки для унификации уголовного законодательства в области предупреждения компьютерных преступлений.

Как следует отметить, волна информационных правонарушений не обошла и СССР, а в будущем и Российскую Федерацию. Волна преступлений в информационной среде способствовала выработке соответствующих решений относительно уголовного регулирования области использования и распространения технологий информационного характера.

В данном случае идет речь о разработке Закона РСФСР «Об ответственности за правонарушения при работе с информацией». В указанном нормативном источнике были выделены основания для уголовной, административной, гражданско-правовой и дисциплинарной ответственности за информационные правонарушения.

В то же время, как следует справедливо указать в рамках настоящего исследования, что из-за собственной недоработки закон так и не был принят. Российский законодатель в последующем принял более 600 правовых актов по вопросам осуществления регулирования информационно-телекоммуникационной области.

Российский сегмент мирового виртуального пространства начался 07 апреля 1994 г., когда был рожден Рунет. Именно с этого периода Россия стала официально признанной страной, которая была представлена в интернет среде. Процесс развития российского уголовного законодательства, направленного на регулирование и предупреждение информационных правонарушений, может прослеживаться через принятие основных законодательных источников:

– принятие Закона России о правовой охране программ для электронно-вычислительных машин и баз данных в 1992 г.;
– принятие Гражданского кодекса РФ, в котором содержатся некоторые нормы, которые связаны с компьютерной информацией;
– принятие Федерального закона об информации, информатизации и защите информации в 1995 г.

Рассматриваемый процесс нормотворчества закончился в 1996 г., когда был издан УК РФ, в который была включена отдельная глава, которая направлена на регулирование информационных правонарушений.

Что же касается административного регулирования информационных правонарушений, то основным законодательным актом, регламентирующим данную область, как уже ранее отмечалось в исследовании, выступает КоАП РФ [12].

Согласно проведенному аналитическому исследованию, установлено, что за 1994-2022 годы в Кодекс принимаются поправки каждые 10 дней (в среднем). Это свидетельствует о том, что наблюдается снижение срока, в рамках которого неизменным остается законодательный акт, т.е. снижается период стабильности.

В сфере регулирования информационных правонарушений также прослеживается аналогичная тенденция. Как следует подчеркнуть, выделенная тенденция обусловлена рядом причин: появление новых угроз и вызовов, формирование новых правоотношений, изменение основных норм отраслевого законодательства.

Вносимые в Кодекс изменения, как следует подчеркнуть, не подтверждены убедительными обоснованиями и критериями юридического научного характера. Такие изменения представлены субъективно, мало проработаны, что обусловливает разрушение логики построения Кодекса.

Мы уже раньше писали, что в гл. 13 КоАП РФ [12] выделена группа информационных правонарушений, но при этом в других главах Кодекса

также размещена значительная часть составов исследуемой категории правонарушений.

К примеру, в гл.13 ст. 13.25 КоАП РФ [12] и в гл. 15 ст. 15.19, 15.21 КоАП РФ [12] определена ответственность административного характера за правонарушения, которые связаны с информацией о деятельности юридического лица. В ст. 7.32.3, 7.31, 7.30, 8.28.1, 19.7.9, 19.7.7, 14.4.1, 13.19.1 КоАП РФ [12] предусматривается ответственность за непредставление сведений, или же за представление неактуальных, недостоверных или неполных сведений. Нарушения требований российского законодательства о предоставлении информации, обеспечении доступа к ней, хранении информации предусмотрены практически в каждой главе КоАП РФ [12].

Как и другие главы КоАП РФ [12] гл. 13 также подвергалась изменениям, однако часть статей рассматриваемой главы вообще не подвергались изменениям. Выделенное положение позволяет, с одной стороны, говорить об адекватности установленных законодательных мер ответственности за исследуемую категорию правонарушений.

С другой стороны, это свидетельствует о том, что такие нормы не работают. К примеру, в судебной практике использование ст. 13.24 «Повреждение телефонов-автоматов» КоАП РФ [12] практически не встречается, что обусловлено тем, что в результате развития сотовой связи их стали использовать мало, что, в конечном счете привело к снижению количества информационных правонарушений в данной сфере.

В процессе развития российского законодательства гл. 13 КоАП РФ [12] пополнялась новыми статьями. Актуальность их исследования, в первую очередь, обусловлена тем, что позволит выявить наиболее актуальные вопросы, которые государство и общество решает с помощью назначения ответственности административного характера. По сути, новые составы информационных правонарушений могут быть классифицированы следующим образом:

– юридическая ответственность за нарушение виновным лицом основных требований доступа к информационным данным, ее размещению и хранению, т.е. нарушение основных требований к соблюдению и установлению соответствующего правового режима в отношении какой-либо информации;
– защита содержательной стороны информации. Данная группа, как следует подчеркнуть, активно развивается.

Выделенные группы информационных правонарушений, в свою очередь, определяют ключевые векторы развития юридической ответственности в современной информационной среде. Именно поэтому, мы полагаем, требуется более подробно рассмотреть их.

Так, к первой группе могут быть отнесены довольно новые статьи Кодекса: 13.28 «Нарушение порядка предоставления информации о деятельности государственных органов и органов местного самоуправления» КоАП РФ [12] и 13.27 «Нарушение требований к организации доступа к информации о деятельности государственных органов и органов местного самоуправления и ее размещению в сети Интернет» КоАП РФ [12].

Согласно законодательным положениям ч. 1 ст. 13.27 КоАП РФ [12], устанавливается ответственность за нарушение основных требований к средствам обеспечения лингвистического, программного и технологического характера при пользовании официальными сайтами органов местного самоуправления и государственных органов.

В то же время ч. 2 ст. 13.27 КоАП РФ [12] предусматривает ответственность за выполнение обязанности по размещению в сети Интернет соответствующей информации о деятельности органов местного самоуправления и государственных органов. При этом, необходимо отметить тот факт, что с наступлением фактического ущерба не увязывается привлечение к ответственности, т.е. уже за факт совершенного правонарушения наступает ответственность административного характера.

Органы местного самоуправления и государственные органы, в согласовании с законодательными положениями ФЗ от 9.02.2009 г. №8-ФЗ, создают официальные сайты для размещения информации о собственной деятельности, на таких сайтах они указывают адреса электронной почты, чтобы пользователи могли направить соответствующий запрос. Правительством РФ установлены основные требования к средствам обеспечения пользования такими сайтами (лингвистические, программные и технологические средства).

Что же касается ст. 13.28 КоАП РФ [12], то можно проследить ее непосредственную связь со ст. 13.27 КоАП РФ [12]. Основной целью ч. 1 ст. 13.28 КоАП РФ [12] считается выполнение ключевых требований о предоставлении информационных сведений ограниченного доступа, а также соблюдении условий по предоставлению таких сведений, касающихся бесплатности и платности.

В ст. 21 ФЗ от 9.02.2009 г. №8-ФЗ определены виды информационных сведений о деятельности органов местного самоуправления и государственных органов. Выделим их:

- информация, которая устанавливает обязанности и права заинтересованного информационными сведениями пользователя. Такие обязанности и права устанавливаются российским законодательством;
- информация, которая передается в устной форме;
- информация, которая размещается в сети Интернет и в местах, отведенных для размещения соответствующей информации, органами местного самоуправления и государственными органами,
- прочая информация о деятельности органов местного самоуправления и государственных органов, установленная законом или муниципальными правовыми актами.

В ст. 22 ФЗ от 9.02.2009 г. №8-ФЗ определены условия регламентации порядка платы за предоставление соответствующих информационных

сведений о деятельности органов МСУ и государственных органов, а также выделены случаи предоставления такой платы.

Российский законодатель также ввел некоторые новые статьи и в другие главы КоАП РФ [12], которые затрагивают вопросы установления ответственности административного характера за нарушение установленного правового режима отдельных разновидностей информации.

Так, в ст. 5.53 КоАП РФ [12] регламентируется вопрос ответственности за получение, распространение информации, которая составляет кредитную историю.

В то же время в ст. 5.54 КоАП РФ [12] осуществляется регламентация вопроса ответственности за неисполнение обязанности по исправлению или проверки недостоверной информации в кредитной истории.

В тоже время, необходимо отметить, что российский законодатель уделил более пристальное внимание второй группе информационных отношений. Прежде всего, это связано с тем, что она касается содержательной стороны информационных сведений и распространением информации.

Необходимо отметить, что именно такие проблемы интересуют современное общество и государство.

На сегодняшний день на территории нашего государства вводятся запреты, на соблюдение таких запретов устанавливается ответственность юридического характера. В данном случае речь идет о запрете террористической, экстремистской информации и любой другой информации, запрещенной на территории нашего государства.

Ст. 13.15 «Злоупотребление свободой массовой информации» КоАП РФ [12] значительно подверглась изменениям, в частности:

- введение ч. 3 ст. 13.15 КоАП РФ [12], предусматривающей установление ответственности за осуществление незаконного распространения информации о несовершеннолетнем, который пострадал во время противоправных действий или бездействии,

нарушении требований, предусмотренных российских законодателем, к распространению таких информационных сведений (ФЗ от 5.04.2013 г. № 50-ФЗ)

- введение ч. 4 ст. 13.15 КоАП РФ [12], предусматривающей установление ответственности за публичное распространение сведений о днях воинской славы, памятных российских датах, выражающих явное неуважение к обществу (ФЗ от 5.05.2014 г. № 128-ФЗ);
- введение ч. 5 ст. 13.15 КоАП РФ [12], предусматривающей установление ответственности за распространение в СМИ, ИТС информационных сведений, которые включают в себя инструкции по самодельному изготовлению взрывных устройств и взрывчатых средств (ФЗ от 24.11.2014 г. № 370-ФЗ);
- введение ч. 6 ст. 13.15 КоАП РФ [12], предусматривающей установление ответственности административного характера за выпуск или производство продукции СМИ, содержащей призывы к осуществлению деятельности террористического характера, оправдание терроризма, призывы к экстремистской деятельности и т.д. (ФЗ от 2.05.2015 г. № 116-ФЗ);

Следует отметить, что по такой направленности близка ст. 20.29 КоАП РФ [12], предусматривающая установление ответственности административного характера за распространение и производство экстремистских материалов, но ответственность в рамках данной статьи наступает за массовое распространение материалов экстремистского характера, хранение и производство таких материалов для их дальнейшего массового распространения.

- введение ч. 7 ст. 13.15 КоАП РФ [12], предусматривающей установление ответственности за использование информационно-телекоммуникационных сетей и средств массовой информации для

разглашения основных сведений, которые составляют специально охраняемую законом или государственную тайну.

Ряд статей КоАП направлены на установление ответственности, обеспечивающей защиту детей от информации, причиняющей вред их здоровью и (или) развитию.

Так, Федеральным законом от 21июля 2011 г. №252-ФЗ была введена ст. 6.17 «Нарушение законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию», «установившая ответственность за нарушение установленных требований рас пространения среди детей информационной продукции, содержащей информацию, причиняющую вред их здоровью и (или) развитию» [12].

К этому же блоку статей следует отнести ст. 6.21 «Пропаганда нетрадиционных сексуальных отношений среди несовершеннолетних» КоАП, введенную Федеральным законом от 29 июня 2013 г. № 135-ФЗ.

За «пропаганду нетрадиционных сексуальных отношений среди несовершеннолетних (распространение информации, направленной на формирование у несовершеннолетних нетрадиционных сексуальных установок, привлекательности нетрадиционных сексуальных отношений, искаженного представления о социальной равноценности традиционных и нетрадиционных сексуальных отношений, либо навязывание информации о нетрадиционных сексуальных отношениях, вызывающей интерес к таким отношениям) установлен административный штраф» [12].

Если указанные действия совершены с применением средств массовой информации и (или) информационно-телекоммуникационных сетей (в том числе сети Интернет), то размер штрафа увеличивается. В отдельные части статьи выделены указанные действия, совершенные иностранным гражданином

Упомянутый Федеральный закон от 1 мая 2017 г. № 87-ФЗ дополнил КоАП ст. 13.36, устанавливающей «административную ответственность владельца аудиовизуального сервиса за нарушение установленного порядка

распространения среди детей информации, причиняющей вред их здоровью и (или) развитию» [12].

Еще одна вновь введенная статья КоАП (ст. 13.37) устанавливает «ответственность владельца аудиовизуального сервиса за распространение информации, содержащей публичные призывы к осуществлению террористической деятельности, материалов, публично оправдывающих терроризм, или других материалов, призывающих к осуществлению экстремистской деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности» [12].

Следовательно, на сегодняшний день можно обнаружить наличие однозначной и четкой тенденции в сфере установления соответствующей административной ответственности за распространение и содержание информационных сведений.

В силу чего, в настоящее время предлагается формирование Единого реестра доменных мен, указателей страниц веб-сайтов, сетевых адресов для реализации указанных мер правового регулирования. Благодаря созданию такого реестра можно идентифицировать веб-сайты, которые содержат информационные сведения, запрещенные на территории нашего государства.

Довольно длительное время, в основном, оператор связи выступал субъектом правоотношений информационного характера. В то же время, с течением временных изменений стало очевидно, что активное воздействие на распространение и доступ к информационным сведениям могут оказывать и иные субъекты. Именно поэтому российское законодательство было изменено, и уже ориентировалось на установление для такого рода лиц ответственности юридического характера.

Изменения российского законодательства, по сути, носили точечный характер в сфере установления юридической ответственности для конкретной категории субъектов, и их основных обязанностей.

При этом изменение российского законодательства было направлено на отдельную категорию субъектов, оказывающих непосредственное

воздействие на распространение и содержание информационных сведений в сети Интернет, обусловленные статусом таких субъектов либо характером их деятельности.

Выделенные обстоятельства способствовали выделению огромного числа субъектов, на которых была возложена обязанность по распространению / доступу информационных данных в Интернете, однако, таких субъектов можно не всегда отличить друг от друга в правоприменительной практике.

Наиболее актуальным остался вопрос о назначении правовой ответственности для таких субъектов. При этом, необходимо отметить, что решение выделенной проблемы в особенности актуально, когда идет речь о взаимодействии в сети Интернет, приводящем к нарушению основных норм законодательства РФ. К таким законодательным нормам, в первую очередь, требуется относить:

- осуществление мошенничества с использованием компьютерных информационных сведений;
- распространение, размещение и передача в сети Интернет материала с нарушением прав 3-х лиц;
- взломы пользовательских аккаунтов;
- доведение до всеобщего сведения информационных сведений, которые на территории Российской Федерации запрещены.

Специальный статус правового характера устанавливается в отношении субъектов, которые осуществляют техническую сторону отношений в сети Интернет.

Такого рода статус в нашей стране определяется, прежде всего, наличием у субъекта соответствующей ответственности и обязанностей за нарушения, совершенные другими лицами, а также условиями освобождения от такой юридической ответственности.

Исходя из анализа социально-правовой характеристикй информационных правонарушений, были получены следующие выводы.

Согласно законодательным положениям, под информационной безопасностью принято понимать защищенность информационной общественной среды, которая реализуется в интересах человека, общества и всего государства.

Было установлено, что сущностью информационной государственной безопасности считается формирование на территории государства активной защиты основных интересов, которые связаны с использованием ресурсов информационного характера.

На сегодняшний день можно обнаружить наличие однозначной и четкой тенденции в сфере установления соответствующей административной ответственности за распространение и содержание информационных сведений.

В силу чего, в настоящее время предлагается формирование Единого реестра доменных мен, указателей страниц веб-сайтов, сетевых адресов для реализации указанных мер правового регулирования. Благодаря созданию такого реестра можно идентифицировать веб-сайты, которые содержат информационные сведения, запрещенные на территории нашего государства.

Довольно длительное время, в основном, оператор связи выступал субъектом правоотношений информационного характера. В то же время, с течением временных изменений стало очевидно, что активное воздействие на распространение и доступ к информационным сведениям могут оказывать и иные субъекты. Именно поэтому российское законодательство было изменено, и уже ориентировалось на установление для такого рода лиц ответственности юридического характера.

Изменения российского законодательства, по сути, носили точечный характер в сфере установления юридической ответственности для конкретной категории субъектов, и их основных обязанностей.

При этом изменение российского законодательства было направлено на отдельную категорию субъектов, оказывающих непосредственное воздействие на распространение и содержание информационных сведений в

сети Интернет, обусловленные статусом таких субъектов либо характером их деятельности.

Выделенные обстоятельства способствовали выделению огромного числа субъектов, на которых была возложена обязанность по распространению / доступу информационных данных в Интернете, однако, таких субъектов можно не всегда отличить друг от друга в правоприменительной практике.

Наиболее актуальным остался вопрос о назначении правовой ответственности для таких субъектов. При этом, необходимо отметить, что решение выделенной проблемы в особенности актуально, когда идет речь о взаимодействии в сети Интернет, приводящем к нарушению основных норм законодательства РФ. К таким законодательным нормам, в первую очередь, требуется относить:

- осуществление мошенничества с использованием компьютерных информационных сведений;
- распространение, размещение и передача в сети Интернет материала с нарушением прав 3-х лиц;
- взломы пользовательских аккаунтов;
- доведение до всеобщего сведения информационных сведений, которые на территории Российской Федерации запрещены.

Специальный статус правового характера устанавливается в отношении субъектов, которые осуществляют техническую сторону отношений в сети Интернет.

Такого рода статус в нашей стране определяется, прежде всего, наличием у субъекта соответствующей ответственности и обязанностей за нарушения, совершенные другими лицами, а также условиями освобождения от такой юридической ответственности.

В настоящее время нормативная база международного уровня, затрагивающая регулирование правонарушений в информационной среде довольно далека от завершенности и полноты. На уровне ООН сегодня

отсутствует единое нормативное регулирование. Что же касается российского уголовного регулирования данной категории общественно-опасных деяний, то с принятием УК РФ в нем была выделена отдельная глава – гл. 28 УК РФ, затрагивающая вопросы регулирования информационных правонарушений, в рамках административного регулирования информационных правонарушений, то основным законодательным актом, регламентирующим данную область, как уже ранее отмечалось в исследовании, выступает КоАП РФ.

Анализ свидетельствует о том, что в настоящее время выделено множество субъектов, которые имеют обязанность по распространению, а также доступу в сети к соответствующим информационным данным, но таких субъектов не всегда можно в правоприменительной практике отличить друг от друга.

Именно поэтому, сегодня актуально определение ответственности такого рода субъектов, в частности, при осуществлении взаимодействия в сетевом пространстве, которое приводит к нарушению соответствующих норм законодательства РФ.

К таким нормам, требующим особенного регулирования, в первую очередь, относятся:

- осуществление мошенничества с использованием компьютерных информационных сведений;
- распространение, размещение и передача в сети Интернет материала с нарушением прав 3-х лиц;
- взломы пользовательских аккаунтов;
- доведение до всеобщего сведения информационных сведений, которые на территории Российской Федерации запрещены.

Глава 3 Правовая характеристика информационных правонарушений как угрозы национальной безопасности

3.1 Неправомерное воздействие на критическую информацию инфраструктуры РФ

Регулирование информационных правонарушений, связанных с неправомерным воздействием на критическую информацию инфраструктуры РФ осуществляется с использованием законодательных норм ст. 13.12.1 «Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры РФ» КоАП РФ [12].

В ч. 1 ст. 13.12.1 КоАП РФ [12] сказано, что за нарушение основных требований к созданию систем безопасности КИИ РФ и обеспечению их надлежащего функционирования, а также обеспечению безопасности значимых объектов КИИ РФ, подразумевает назначение административной ответственности в виде штрафа от 10 тысяч рублей до 50 тысяч рублей для должностных лиц; от 50 тысяч рублей до 100 тысяч рублей на юридических лиц.

В ч. 2 ст. 13.12.1 КоАП РФ [12] предусматривается наложение административного штрафа от 10 тысяч рублей до 50 тысяч рублей на должностных лиц; от 100 тысяч рублей до 500 тысяч рублей на юридических лиц за нарушение порядка информация о существующих компьютерных инцидентах, осуществление реагирования на них, принятия соответствующих мер по осуществлению ликвидации последствий информационных атак, которые были проведены в отношении значимых объектов КИИ.

Законодательная диспозиция ч. 3 ст. 13.12.1 КоАП РФ [12] указывает на то, что за нарушение порядка обмена информационными сведениями о компьютерных инцидентах между субъектами КИИ РФ, субъектами КИИ и уполномоченными органами иностранных государств, иностранными,

международными неправительственными и международными организациями, которые осуществляют деятельность в сфере реагирования на компьютерные инциденты, приводит к наложению штрафа от 20 тысяч рублей до 50 тысяч рублей на должностных лиц; от 100 тысяч рублей до 500 тысяч рублей на юридических лиц.

Еще одним нормативным документом, который регулирует данную категорию информационных правонарушений, считается Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ» [34].

В выделенном нормативном источнике сказано, что критическая информационная инфраструктура – это сети электросвязи и объекты КИИ, которые используются непосредственно для осуществления взаимодействия выделенных объектов.

При этом в указанном законодательном источнике сказано, что объекты критической информационной инфраструктуры включают в себя:

- автоматизированные системы, направленные на управления субъектами критической информационной инфраструктуры,
- информационно-телекоммуникационные средства,
- информационные системы.

Структура автоматизированных систем управления субъектов критической информационной инфраструктуры схематически представлена на рисунке 1.

Рисунок 1 – Структура автоматизированных систем управления субъектов критической информационной инфраструктуры

В процессе проведенного анализа было установлено, что категорирование объектов критической информационной инфраструктуры РФ на сегодняшний день осуществляется с опорой на экологическую, экономическую, социально-политическую значимость для обеспечения правопорядка, государственной безопасности, обороны государства и формирования соответствующего реестра значимых объектов критической информационной инфраструктуры.

В исследуемом законодательном источнике также представлено определение термина «компьютерный инцидент». Согласно предлагаемому определению, под компьютерным инцидентом требуется понимать факт прекращения или нарушения функционирования сети электросвязи, объекта критической информационной инфраструктуры, которые используются для осуществления организации взаимодействия такого рода объектов, либо же

нарушения безопасности информации, обрабатываемой таким объектом критической информационной инфраструктуры.

На основе изученной информации, можно прийти к выводу о том, что инцидент выступает фактом состояния работоспособности систем информационного характера, систем информационной защиты, информационных сетей.

Необходимо отметить, что в настоящее время законом утверждено наличие государственной системы ликвидации, предупреждения, обнаружения основных последствий от атак на российские информационные ресурсы. Необходимо отметить, что выделенная система – территориально разделенный единый комплекс ГосСОПКА. С 2013 г. ведется его созданием Федеральной службой безопасности России.

Также регулирование такого информационного правонарушения, как неправомерное воздействие на критическую информационную инфраструктуру РФ осуществляется нормами российского уголовного законодательства.

Согласно ч. 1 ст. 274.1 УК РФ, использование, распространение или создание соответствующей компьютерной информации или компьютерных программ, которые направлены на неправомерное воздействие на критическую инфраструктурную информацию России, в частности, для нейтрализации защитных средств таких информационных данных, либо копирования, модификации, блокирования или уничтожения такой информации наказываются принудительными работами до 5 лет.

При этом возможно ограничение свободы для виновного лица от 2-х до 5 лет со штрафом от 500 тыс. рублей до 1 млн. рублей. Штрафная санкция может быть определена и в размере заработной платы либо другого дохода осужденного виновного лица на срок от 1 года до 3-х лет.

При осуществлении неправомерного доступа к охраняемой информации, которая содержится в критической информационной инфраструктуре, в частности, с применением компьютерной информации или

компьютерных программ, направленных на осуществление такого воздействия, согласно ч. 2. ст. 274 УК РФ, приводит к уголовной ответственности в виде принудительных работ до 5 лет со штрафом от 500 тыс. рублей до 1 млн. рублей, либо в размере заработной платы и прочего дохода виновного осужденного лица от 1 до 3-х лет, с ограничением свободы до 2-х лет либо без ограничения; лишением свободы от 2-х до 6 лет со штрафом от 500 тыс. рублей до 1 млн. рублей или в размере заработной платы и прочего дохода за периол от 1 до 3 лет.

Согласно ч. 3 ст. 274.1 УК РФ, если нарушение правил эксплуатации средств передачи, обработки и хранения информационных сведений в критической информационной инфраструктуре, систем управления ей, правил доступа к информации повлекло причинение вреда критической информационной инфраструктуре, это наказывается принудительными работами до 5 лет, с лишением у виновного лица права заниматься определенной деятельностью или занимать определенные должности до 3-х лет, либо без такого лишения.

Кроме того, предусмотрена уголовная ответственность предусматривает лишение свободы до 6 лет с лишением права заниматься определенной деятельностью и занимать определенные должности до 3-х лет, либо без такого лишения.

3.2 Нарушение правил хранения, обработки и передачи информационных сведений

В ч. 3 ст. 13.25 КоАП РФ [12] предусматривается административная ответственность за неисполнение страховщиком обязанности по хранению документов и информационных данных, перечень которых отражен в страховом законодательстве, а также непринятие мер по обеспечению хранения информационных сведений, которые содержатся в

информационных системах, обеспечение и ведение сохранности которых предусмотрено российским страховым законодательством, в виде штрафа в размере от 20 тысяч рублей до 30 тысяч рублей – на должностных лиц; от 100 тысяч рублей до 200 тысяч рублей – на юридических лиц.

Регулирование такого вида информационного правонарушения, как нарушение правил эксплуатации средств хранения, обработки и передачи информационных сведений регулируется также законодательными положениями ст. 274 УК РФ.

Согласно ч. 1 ст. 274 УК РФ, нарушение таких правил предполагает нарушение правил эксплуатации средств передачи, обработки и хранения информационно-телекоммуникационных сетей, оборудования или охраняемой информации, правил доступа к информационно-телекоммуникационным сетям, которое способствовало копированию, модификации или уничтожению компьютерных информационных сведений, и причинило большой ущерб.

Уголовная ответственность за совершение такого преступления предполагает штраф до 500 тыс. рублей либо в размере заработной платы и прочего дохода виновного осужденного лица за период до 18 месяцев.

Также возможна ответственность в виде исправительных работ на срок от полугода до 1 года, ограничение свободы виновного лица до 2-х лет, принудительные работы до 2-х лет, или же лишение свободы виновного лица на аналогичный срок.

Если говорить о практическом применении законодательных норм ст. 274 УК РФ, то следует подчеркнуть тот факт, что на практике это достаточно сложно. Прежде всего, такие трудности обусловлены тем, что в законе отсутствуют четкие определения используемых терминов.

Именно поэтому при квалификации конкретных преступных действий происходят некоторые проблемы. В качестве примера можно рассмотреть тот факт, что в указанной законодательной норме отсутствует четкое определение средств хранения, передачи и обработки информационных

сведений. Кроме того нет определения того, что считать эксплуатацией таких средств.

Также следует подчеркнуть тот факт, что в законодательных нормах ст. 274 УК РФ содержится отсылка к законодательным нормам, которые не определены непосредственным образом в законе, а именно к правилам и инструкциям работы со средствами передачи, обработки или хранения информационно-телекоммуникационных средств и информационных данных.

Лишь на уровне нормативных подзаконных актов могут определяться и утверждаться такие соответствующие правила и инструкции. Именно поэтому в статистике МВД России прослеживаются сложности применения на практике данной законодательной нормы.

3.3 Использование и распространение вредоносных компьютерных программ

В законодательной диспозиции ч. 1 ст. 13.44 КоАП РФ [12] сказано, что при неисполнении владельцем, собственником технологической сети связи, оператором связи или организатором распространения информационных данных в сети Интернет, обязанности по использованию в ИТС сетевых адресов, программных и технических средств, которые функционируют в согласовании с установленными требованиями, национальной системы доменных имен приводит к наложению административного штрафа от 3 тысяч рублей до 5 тысяч рублей – на граждан; от 5 тысяч рублей до 10 тысяч рублей – на должностных лиц; от 10 тысяч рублей до 20 тысяч рублей – на индивидуальных предпринимателей; от 30 тысяч рублей до 50 тысяч рублей – на юридических лиц.

При этом, при повторном нарушении размер штрафа увеличивается: от 6 тысяч рублей до 10 тысяч рублей – на граждан; от 10 тысяч рублей до 20

тысяч рублей – на должностных лиц; от 20 тысяч рублей до 40 тысяч рублей – на индивидуальных предпринимателей; от 60 тысяч рублей до 100 тысяч рублей – на юридических лиц.

Как следует справедливо отметить, польза и вред от компьютерных программ, прежде всего, должен определяться не их основной способностью копировать, модифицировать, блокировать, уничтожать информационные сведения, а наличием основных принципов, которые схематически представлены на рисунке 2.

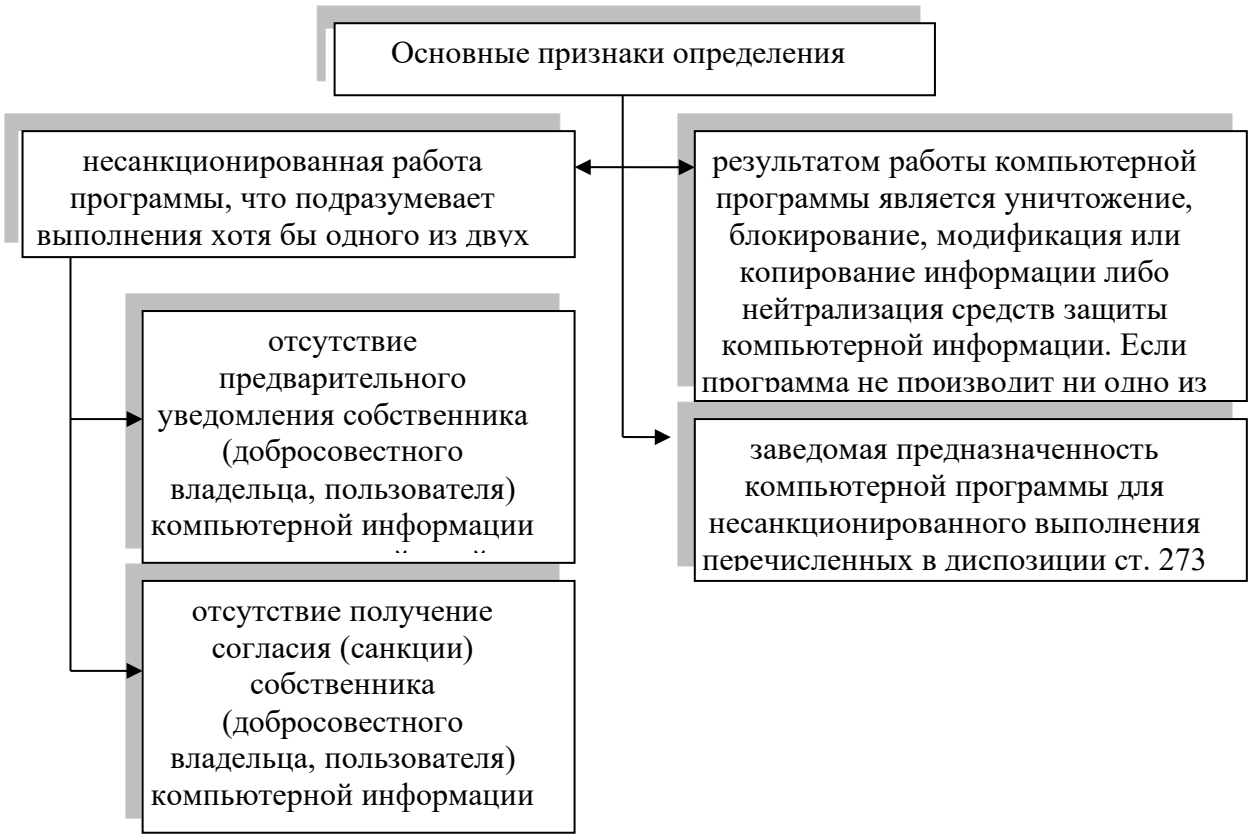

Рисунок 2 – Основные признаки определения вредоносности компьютерных программ

Использование и распространение вредоносных компьютерных программ регулируется также законодательными нормами ст. 273 УК РФ.

Согласно диспозиции ч. 1 ст. 273 УК РФ, данная категория информационных правонарушений подразумевает использование,

распространение или создание компьютерных информации или программ, которые своей целью имеют нейтрализацию средств защиты информации и осуществление несанкционированного копирования, модификации, блокирования или уничтожения информации.

Уголовная ответственность за такое преступление предусматривает ограничение свободы до 4-х лет, лишение свободы до 4-х лет со штрафом до 200 тыс. рублей, либо в размере заработной платы и прочего дохода до 18 месяцев; или же принудительные работы до 4-х лет.

В исследуемом Стандарте, как следует подчеркнуть, представлено определение термина «вредоносное программное обеспечение». Согласно предлагаемому определению, под вредоносным программным обеспечением требуется понимать компьютерную программу, целью которой считается нанесение ущерба или вреда пользователю информации, которая находится на средствах вычислительной техники.

При этом в определении дополняется тот факт, что нанесение вреда осуществляется с помощью осуществления несанкционированного копирования, нейтрализации, блокирования, модификации, уничтожения средств защиты, используемых на средствах вычислительной техники, либо для получения доступа к ресурсам вычислительного характера для их использования несанкционированным путем.

По ст. 273 УК РФ не должны квалифицироваться несанкционированное уничтожение, копирование, модификация, блокирование информационных сведений или нейтрализация средств защиты информации, если они произошли по ошибке пользователя / разработчика, либо если они произошли в результате непредвиденных результатов действия соответствующей компьютерной программы.

3.4 Неправомерный доступ к информационным сведениям

Незаконная деятельность в области защиты информационных сведений регулируется законодательными положениями ст. 13.13 КоАП РФ [12]. Так, согласно ч. 1 ст. 13.13 КоАП РФ [12] занятие видами деятельности в области информационной защиты (кроме защиты информации, которая составляет государственную тайну) без получения лицензии или разрешения в установленном порядке (если они обязательны в согласовании с законом), приводит к наступлению административной ответственности и наложению штрафа в размере от 500 рублей до 1 тысячи рублей с конфискацией / без конфискации средств информационной защиты - на граждан; от 2 тысяч рублей до 3 тысяч рублей с конфискацией / без конфискации средств - на должностных лиц; от 10 тысяч рублей до 20 тысяч рублей с конфискацией / без конфискации средств информационной защиты – на юридических лиц.

В тоже время в ч. 2 ст. 13.13 КоАП РФ [12] указано, что занятие видами деятельности, которая связана с защитой и использованием информации, составляющей государственную тайну, созданием средств, направленных на информационную защиту такой информации и т.д. без лицензии приводит к наступлению административной ответственности и наложению штрафа в размере от 4 тысяч рублей до 5 тысяч рублей - на должностных лиц; от 30 тысяч рублей до 40 тысяч рублей с конфискацией / без конфискации средств защиты– на юридических лиц.

На сегодняшний день, как следует подчеркнуть, достаточно широким является список правовых актов, которые охраняют компьютерную информацию. К ним, прежде всего, относятся:

- Конституция РФ [13];
- Трудовой кодекс РФ [21];
- Налоговый кодекс РФ [17];
- Гражданский кодекс РФ [6];
- Кодекс РФ об административных правонарушениях [12];

- Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» [49];
- Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» [47];
- Федеральный закон от 13 марта 2006 г. № 38-ФЗ «О рекламе» [40];
- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [35];
- Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» [42];
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [39];
- Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» [41];
- Закон от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» [10];
- Закон от 21 июля 1993 г. № 5485-1 «О государственной тайне» [9] и т.д.

Осуществление защиты соответствующих информационных сведений должно быть и от случаев изменения или искажения такой информации, и от случаев осуществления несанкционированного ознакомления с соответствующей информацией.

В первом случае говорится об изменении реквизитов, содержания соответствующей компьютерной информации; во втором случае – об ознакомлении с конфиденциальной информацией, информацией, которая составляет государственную или коммерческую тайну.

Оборот информации, в свою очередь, может быть ограничен, если такая информация носит «вредный» характер, т.е. способствует призыву к разжиганию религиозной розни, расовой ненависти, социальной ненависти, призыву к насилию и пр.

Определение термина доступ к информации было предложено в ФСТЭК России, согласно данному определению, доступ к информации

представляет собой возможность получения и использования такой информации [1].

Термин «доступ к информации» представлен и в Стандарте ФСБ России СТО ФСБ.КК 1-2018, где сказано, что доступ к информации представляет собой обработку или ознакомление с компьютерной информацией. В то же время в указанном Стандарте говорится, что обработка компьютерной информации – это совокупность операций, связанных с:

- совокупном и индивидуальном отображением компьютерной информации;
- модификацией и преобразованием информации;
- уничтожением информации;
- регистрацией информации;
- записью информации;
- передачей информации;
- приемом информации;
- выводом и вводом информации;
- хранением информации;
- накоплением информации;
- сбором информации [50].

С юридической точки зрения в научной литературе термин «неправомерный доступ» довольно часто эквивалентен термину «несанкционированный доступ». Кроме того, также в юридической литературе эквивалентны термины «несанкционированные действия» и «неправомерные воздействия».

Если провести анализ определений ФСТЭК России, то можно прийти к выводу, что под несанкционированными действиями или несанкционированным доступом требуется понимать доступ к информационным сведениям или совершение соответствующих действий с информационными сведениями, которые осуществляются с нарушением

установленных правил или прав доступа к ним либо действий с ними с использованием информационных средств и систем, аналогичных по характеристикам технического характера и собственному функциональному предназначению [1].

При этом в определениях ФСТЭК России сказано, что правила разграничения доступа к информационным сведениям – это совокупность правил, которые осуществляют регламентацию основных прав доступа субъекта к основным объектам такого доступа [Там же].

Исходя из проведенного анализа, можно резюмировать, что на сегодняшний день доступ к компьютерной информации требуется считать неправомерным доступом в следующих случаях:

- если у лица есть право на доступ к информационным сведениям, но лицо осуществляет такой доступ кроме соответствующего установленного порядка, т.е. с нарушением основных правил его защиты;
- если на доступ к таким информационным сведениям лицо не имеет права.

При этом, важно подчеркнуть, что в первом случае говорится о случаях, когда для неправомерного доступа к компьютерной информации используется служебное положение виновным лицом.

Несанкционированное ознакомление с информационными сведениями, которые обладают потенциальной или действительной ценностью, в конечном счете, может привести к потери основной ценности таких информационных сведений.

Исследовав правовую характеристику информационных правонарушений, как угрозы национальной безопасности, были получены следующие выводы.

Регулирование информационных правонарушений, связанных с неправомерным воздействием на критическую информацию инфраструктуры РФ осуществляется с использованием законодательных норм ст. 13.12.1

«Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры РФ» КоАП РФ.

Регулирование такого вида информационного правонарушения, как нарушение правил эксплуатации средств хранения, обработки и передачи информационных сведений регулируется также законодательными положениями уголовного и административного права.

В процессе проведенного анализа было установлено, что категорирование объектов критической информационной инфраструктуры РФ на сегодняшний день осуществляется с опорой на:

- экологическую,
- экономическую,
- социально-политическую значимость для обеспечения правопорядка,
- социально-политическую значимость для обеспечения государственной безопасности,
- социально-политическую значимость для обеспечения обороны государства,
- социально-политическую значимость для обеспечения формирования соответствующего реестра значимых объектов критической информационной инфраструктуры.

В процессе исследования было установлено, что в существующих нормах законодательства Российской Федерация на сегодняшний день отсутствует указание не операцию по ознакомлению с компьютерной информацией. В свою очередь, преступному лицу в некоторых случаях достаточно только прочитать или увидеть информационные сведения, чтобы использовать их без копирования в преступных целях в дальнейшем.

Исходя из проведенного анализа, можно резюмировать, что на сегодняшний день доступ к компьютерной информации требуется считать неправомерным доступом в следующих случаях:

– если у лица есть право на доступ к информационным сведениям, но лицо осуществляет такой доступ кроме соответствующего установленного порядка, т.е. с нарушением основных правил его защиты;
– если на доступ к таким информационным сведениям лицо не имеет права.

При этом, важно подчеркнуть, что в первом случае говорится о случаях, когда для неправомерного доступа к компьютерной информации используется служебное положение виновным лицом.

Несанкционированное ознакомление с информационными сведениями, которые обладают потенциальной или действительной ценностью, в конечном счете, может привести к потери основной ценности таких информационных сведений.

Заключение

Было установлено, что сущностью информационной государственной безопасности считается формирование на территории государства активной защиты основных интересов, которые связаны с использованием ресурсов информационного характера.

В современных условиях комплексной задачей считается обеспечение информационной безопасности, что продиктовано многоплановостью и сложностью информационной среды.

Компетенция государственных органов власти регионального и федерального уровня, других государственных органов, которые входят в систему обеспечения государственной информационной безопасности, определяются соответствующим правовым полем, которое включает в себя нормативно-правовые акты, федеральные законы и прочие законодательные акты.

Такое правовое поле направлено на координирование деятельности соответствующих органов, обеспечивающих государственную национальную безопасность.

Реализация основных механизмов, направленных на правовое обеспечение государственной информационной безопасности, в целом, должно опираться на информатизацию правовой сферы.

Соблюдение законности в системе обеспечения информационной государственной безопасности должно включать в себя наличие нормативно-правовых актов и законов, а также непреклонное их исполнение в сфере информационной безопасности всеми субъектами права.

Деятельность, которая ориентирована на осуществления правового обеспечения государственной информационной безопасности, прежде всего, должна выстраиваться на основе следующих фундаментальных правовых положений:

– неотвратимость наказания за совершенные преступные деяния;
– обеспечение необходимого баланса интересов для государства и его отдельных субъектов;
– соблюдение законности.

Решение проблем в системе обеспечения информационной государственной безопасности, прежде всего, требует использование мер

– технического,
– программного,
– законодательного,
– организационного характера.

Такие меры непосредственно должны быть использоваться совместно.

Согласно законодательным положениям, под информационной безопасностью принято понимать защищенность информационной общественной среды, которая реализуется в интересах человека, общества и всего государства.

Было установлено, что сущностью информационной государственной безопасности считается формирование на территории государства активной защиты основных интересов, которые связаны с использованием ресурсов информационного характера.

На сегодняшний день можно обнаружить наличие однозначной и четкой тенденции в сфере установления соответствующей административной ответственности за распространение и содержание информационных сведений.

В силу чего, в настоящее время предлагается формирование Единого реестра доменных мен, указателей страниц веб-сайтов, сетевых адресов для реализации указанных мер правового регулирования. Благодаря созданию такого реестра можно идентифицировать веб-сайты, которые содержат информационные сведения, запрещенные на территории нашего государства.

Довольно длительное время, в основном, оператор связи выступал субъектом правоотношений информационного характера. В то же время, с

течением временных изменений стало очевидно, что активное воздействие на распространение и доступ к информационным сведениям могут оказывать и иные субъекты. Именно поэтому российское законодательство было изменено, и уже ориентировалось на установление для такого рода лиц ответственности юридического характера.

Изменения российского законодательства, по сути, носили точечный характер в сфере установления юридической ответственности для конкретной категории субъектов, и их основных обязанностей.

При этом изменение российского законодательства было направлено на отдельную категорию субъектов, оказывающих непосредственное воздействие на распространение и содержание информационных сведений в сети Интернет, обусловленные статусом таких субъектов либо характером их деятельности.

Выделенные обстоятельства способствовали выделению огромного числа субъектов, на которых была возложена обязанность по распространению / доступу информационных данных в Интернете, однако, таких субъектов можно не всегда отличить друг от друга в правоприменительной практике.

Наиболее актуальным остался вопрос о назначении правовой ответственности для таких субъектов. При этом, необходимо отметить, что решение выделенной проблемы в особенности актуально, когда идет речь о взаимодействии в сети Интернет, приводящем к нарушению основных норм законодательства РФ. К таким законодательным нормам, в первую очередь, требуется относить:

- осуществление мошенничества с использованием компьютерных информационных сведений;
- распространение, размещение и передача в сети Интернет материала с нарушением прав 3-х лиц;
- взломы пользовательских аккаунтов;

– доведение до всеобщего сведения информационных сведений, которые на территории Российской Федерации запрещены.

Специальный статус правового характера устанавливается в отношении субъектов, которые осуществляют техническую сторону отношений в сети Интернет.

Такого рода статус в нашей стране определяется, прежде всего, наличием у субъекта соответствующей ответственности и обязанностей за нарушения, совершенные другими лицами, а также условиями освобождения от такой юридической ответственности.

В настоящее время нормативная база международного уровня, затрагивающая регулирование правонарушений в информационной среде довольно далека от завершенности и полноты. На уровне ООН сегодня отсутствует единое нормативное регулирование. Что же касается российского уголовного регулирования данной категории общественно-опасных деяний, то с принятием УК РФ в нем была выделена отдельная глава – гл. 28 УК РФ, затрагивающая вопросы регулирования информационных правонарушений, в рамках административного регулирования информационных правонарушений, то основным законодательным актом, регламентирующим данную область, как уже ранее отмечалось в исследовании, выступает КоАП РФ.

Анализ свидетельствует о том, что в настоящее время выделено множество субъектов, которые имеют обязанность по распространению, а также доступу в сети к соответствующим информационным данным, но таких субъектов не всегда можно в правоприменительной практике отличить друг от друга.

Именно поэтому, сегодня актуально определение ответственности такого рода субъектов, в частности, при осуществлении взаимодействия в сетевом пространстве, которое приводит к нарушению соответствующих норм законодательства РФ.

К таким нормам, требующим особенного регулирования, в первую очередь, относятся:

- осуществление мошенничества с использованием компьютерных информационных сведений;
- распространение, размещение и передача в сети Интернет материала с нарушением прав 3-х лиц;
- взломы пользовательских аккаунтов;
- доведение до всеобщего сведения информационных сведений, которые на территории Российской Федерации запрещены.

Регулирование информационных правонарушений, связанных с неправомерным воздействием на критическую информацию инфраструктуры РФ осуществляется с использованием законодательных норм ст. 13.12.1 «Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры РФ» КоАП РФ.

Регулирование такого вида информационного правонарушения, как нарушение правил эксплуатации средств хранения, обработки и передачи информационных сведений регулируется также законодательными положениями уголовного и административного права.

В процессе проведенного анализа было установлено, что категорирование объектов критической информационной инфраструктуры РФ на сегодняшний день осуществляется с опорой на экологическую, экономическую, социально-политическую значимость для обеспечения правопорядка, государственной безопасности, обороны государства и формирования соответствующего реестра значимых объектов критической информационной инфраструктуры.

В процессе исследования было установлено, что в существующих нормах законодательства Российской Федерация на сегодняшний день отсутствует указание не операцию по ознакомлению с компьютерной информацией. В свою очередь, преступному лицу в некоторых случаях

достаточно только прочитать или увидеть информационные сведения, чтобы использовать их без копирования в преступных целях в дальнейшем.

Исходя из проведенного анализа, можно резюмировать, что на сегодняшний день доступ к компьютерной информации требуется считать неправомерным доступом в следующих случаях:

- если у лица есть право на доступ к информационным сведениям, но лицо осуществляет такой доступ кроме соответствующего установленного порядка, т.е. с нарушением основных правил его защиты;
- если на доступ к таким информационным сведениям лицо не имеет права.

При этом, важно подчеркнуть, что в первом случае говорится о случаях, когда для неправомерного доступа к компьютерной информации используется служебное положение виновным лицом.

Несанкционированное ознакомление с информационными сведениями, которые обладают потенциальной или действительной ценностью, в конечном счете, может привести к потери основной ценности таких информационных сведений.

Список используемой литературы и используемых источников

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 [Электронный ресурс]. URL: https://fstec.ru/component/attachments/download/289

2. Буйневич М.В., Покусов В.В., Израилов К.Е. Способ визуализации модулей системы обеспечения информационной безопасности // Научноаналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2018. № 3. С. 81-91.

3. Велиева Д.С-К. Деятельность органов государственной власти по охране окружающей среды и обеспечению экологической безопасности: проблемы законодательного определения // Алтайский вестник государственной и муниципальной службы. 2008. №2. С. 55-57.

4. Военная доктрина Российской Федерации (утв. Президентом РФ 25.12.2014 № Пр-2976) // Российская газета от 30 декабря 2014 г. № 298.

5. Гайдарева И.Н. Правовое обеспечение информационной безопасности в России // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2009. №1. С. 174-180.

6. Гражданский кодекс РФ. Ч. 4. от 18 декабря 2006 г. № 230-ФЗ (с изменениями и дополнениями) // Собрание законодательства РФ от 25.12.2006, № 52. ст. 5496.

7. Гребеньков А.А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава // Lex Russica. 2018. №4 (137). С. 108-120.

8. Гребеньков А.А. Преступность в сфере высоких технологий: исторический аспект// Известия Юго-Западного государственного университета. Серия «История и право». 2012. № 1-1. С. 184—188.

9. Закон РФ от 21 июля 1993 г. № 5485-I «О государственной тайне» (с изменениями и дополнениями) // Российская газета от 21 сентября 1993 г. № 182.

10. Закон РФ от 27 декабря 1991 г. № 2124-I «О средствах массовой информации» // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации от 13 февраля 1992 г. № 7 ст. 300.

11. Карев А.С., Бирих Э.В., Сахаров Д.В., Виткова Л.А. Проблемы информационной безопасности в интернете вещей // В сборнике: Интернет вещей и 5G. 2016. С. 66-70.

12. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства Российской Федерации от 7 января 2002 г. N 1 (часть I) ст. 1.

13. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Российская газета от 4 июля 2020 г. № 144.

14. Красов А.В., Штеренберг С.И., Фахрутдинов Р.М., Рыжаков Д.В., Пестов И.Е. Анализ информационной безопасности предприятия на основе сбора данных пользователей с открытых ресурсов и мониторинга информационных ресурсов с использованием машинного обучения // TComm: Телекоммуникации и транспорт. 2018. Т. 12. № 10. С. 36-40.

15. Крылов В.В. Основы криминологической теории расследования преступлений в сфере информации. М. : МГУ, 1998. 50 с.

16. Мазуров В.А., Невинский В.В. Понятие и принципы информационной безопасности // Известия АлтГУ. 2003. №2. С. 057-063.

17. Налоговый кодекс Российской Федерации от 31 июля 1998 г. № 146-ФЗ. Часть первая. // Собрание законодательства Российской Федерации от 3 августа 1998 г. № 31 ст. 3824.

18. Роберт И.В. Информационная безопасность личности // Труды международного симпозиума «Надёжность и качество». 2018. Т. 1. С. 68- 71.

19. Суслопаров А. В. Информационные преступления: автореф. дис. … канд. юрид. наук. Красноярск, 2008. 22 с.

20. Трофимова, А. Ю. История развития уголовного законодательства в части регламентации оснований ответственности за преступления в сфере компьютерной информации // Молодой ученый. 2021. № 53 (395). С. 128-129.

21. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ // Собрание законодательства Российской Федерации от 7 января 2002 г. № 1 (часть I) ст. 3.

22. Турышев А. А. Информация как признак составов преступлений в сфере экономической деятельности: автореф. дис. … канд. юрид. наук. Омск, 2006. 24 с.

23. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации от 17 июня 1996 г. № 25 ст. 2954.

24. Указ Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // URL: https://www.consultant.ru/document/cons_doc_LAW_381999/

25. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации от 5 июля 2021 г. № 27 (часть II) ст. 5351.

26. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» //

Собрание законодательства Российской Федерации от 12 декабря 2016 г. № 50 ст. 7074.

27. Указ Президента РФ от 6 октября 2004 г. № 1286 «Вопросы Межведомственной комиссии по защите государственной тайны» (с изменениями и дополнениями) // Собрание законодательства Российской Федерации от 11 октября 2004 г. № 41 ст. 4024.

28. Указ Президента РФ от 7 августа 2004 г. № 1013 «Вопросы Федеральной службы охраны Российской Федерации» (с изменениями и дополнениями) // Собрание законодательства Российской Федерации от 9 августа 2004 г. № 32 ст. 3314.

29. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями и дополнениями) // Собрание законодательства Российской Федерации от 10 марта 1997 г. № 10, ст. 1127.

30. Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне» (с изменениями и дополнениями) // Собрание законодательства Российской Федерации от 4 декабря 1995 г. № 49 ст. 4775.

31. Указ Президента РФ от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации» (с изменениями и дополнениями) // Собрание актов Президента и Правительства Российской Федерации от 25 января 1994 г., № 4, ст. 305.

32. Устинов Д. Сущность информационной безопасности // Международный журнал гуманитарных и естественных наук. 2017. № 12. С. 146-151.

33. Устьев Л. Г. Уголовная ответственность за коррупционные информационные преступления: автореф. дис. … канд. юрид. наук. Тамбов, 2010. С. 11.

34. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» //

Собрание законодательства Российской Федерации от 31 июля 2017 г. № 31 (часть I) ст. 4736.

35. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ (последняя редакция) // Собрание законодательства Российской Федерации от 11 апреля 2011 г. № 15 ст. 2036.

36. Федеральный закон «О полиции» от 07.02.2011 № 3-ФЗ (последняя редакция) // Собрание законодательства Российской Федерации от 14 февраля 2011 г. № 7 ст. 900

37. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» (с изменениями и дополнениями) // Собрание законодательства Российской Федерации от 3 января 2011 г. № 1 ст. 2.

38. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3448.

39. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрании законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3451.

40. Федеральный закон от 13 марта 2006 г. № 38-ФЗ «О рекламе» // Собрание законодательства Российской Федерации от 20 марта 2006 г. № 12 ст. 1232.

41. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» // Собрание законодательства Российской Федерации от 9 августа 2004 г. № 32 ст. 3283.

42. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ (последняя редакция) // Собрание законодательства Российской Федерации от 14 июля 2003 г. № 28 ст. 2895.

43. Федеральный закон от 31 мая 1996 г. № 61-ФЗ «Об обороне» (с изменениями и дополнениями) // Собрание законодательства Российской Федерации от 3 июня 1996 г. № 23 ст. 2750.

44. Федеральный закон от 27 мая 1996 г. № 57-ФЗ «О государственной охране» (с изменениями и дополнениями) // Собрание законодательства Российской Федерации, 27 мая 1996 г., № 22, ст. 2594.

45. Федеральный закон от 10 января 1996 г. № 5-ФЗ «О внешней разведке» (с изменениями и дополнениями) // Собрание законодательства Российской Федерации от 15 января 1996 г., № 3. ст. 143.

46. Федеральный закон от 27 мая 1996 г. № 57-ФЗ «О государственной охране» (с изменениями и дополнениями) // Собрание законодательства Российской Федерации, 27 мая 1996 г., № 22, ст. 2594.

47. Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ (последняя редакция) // Собрание законодательства Российской Федерации от 14 августа 1995 г. № 33 ст. 3349.

48. Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности» (с изменениями и дополнениями) // Собрание законодательства Российской Федерации от 10 апреля 1995 г. № 15 ст. 1269.

49. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 № 395-1 (последняя редакция) // Ведомости съезда народных депутатов РСФСР от 6 декабря 1990 г. № 27 ст. 357.

50. Федеральная служба безопасности Российской Федерации. Стандарт СТО.ФСБ.КК 1-2018 «Компьютерная экспертиза. Термины и определения», Москва, 12 ноября 2018 г. № 33 [Электронный ресурс]. URL: http://www.fsb.ru/files/fsbdoc/normakt/standart_sto_2018.doc

51. Чесноков А.Д. Информационная безопасность // Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022. С. 478-489.

52. Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Информационная безопасность: учеб. Пособие, под общ. ред. В.Н. Ясенева. / Нижний Новгород: Нижегородский гос. ун-т им. Н.И. Лобачевского, 2017. 198 с.