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

Институт финансов, экономики и управления
(наименование института полностью)

Департамент магистратуры (бизнес-программ)
(наименование)

38.04.02 Менеджмент
(код и наименование направления подготовки)

Государственное и муниципальное управление
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему: «Правовое обеспечение и управление информационной безопасностью в Российской Федерации».

Студент М.С. Валенцев
(И.О. Фамилия) (личная подпись)

Научный руководитель д.ю.н., профессор Д.А. Липинский
(ученая степень, звание, И.О. Фамилия)

Тольятти 2021

Оглавление

Введение

Вступление общественности в информационную составляющую, основанную на достижениях новейших технологий, требует незамедлительного устранения угроз, касающихся безопасности информации. Исполнение цели, основанной на контроле и защите информации, обеспечивают структурные государственные органы межведомственного управления. На протяжении последних десятилетий, многими странами мира были утверждены документы концептуальной, доктринальной и программной направленности, которые основаны на защите информационных систем во всех сферах жизни общества.

На сегодняшний момент обеспечить правовое обеспечение в сфере защиты информации позволит введение современных концепций, которые направлены на усиление информационной безопасности. Благодаря правовому обеспечению, происходит пересмотр следующих разновидностей законодательных норм:

- Нормы, обладающие декларативной направленностью,
- Нормы, имеющие неоднозначное объяснение,
- Нормы, не соответствующие темпу времени,
- Нормы, которые не отражают реальность происходящего. В данной разновидности норм принимают активное участие заинтересованные органы, в лице федерального органа власти субъектов РФ, а также СМИ и общественность.

Актуальность исследования – в настоящее время мир столкнулся с множеством глобальных угроз в области информации. Хакерские атаки проводятся против крупных производственных мощностей государств, в том числе нефтедобывающих, энергетических, ядерных производств. В прессе постоянно встает вопрос о вмешательстве в выборы в различных государствах. Поэтому информационной безопасности в нашей стране, как и во всем мире, требуется уделить особое внимание. Крупный шаг к этому -

принятие Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ. С учетом того, что закон принят недавно – еще отсутствует твердая правоприменительная практика его исполнения. Также многие его аспекты слабо изучены в научной и практической среде. Поэтому актуальность работы состоит в глубоком анализе информационной безопасности и ее управления в Российской Федерации с учетом анализа самых последний изменений законодательства и тенденций всемирного прогресса в сфере информационных технологий.

Степень разработанности темы – на сегодняшний момент данная тема разработана мало, так как в последнее время в мире произошли сильнейшей изменения в рамках информационной безопасности, глобализации угроз. Разработаны и приняты новые нормативно-правовые акты.

Цель исследования работы – проанализировать нормативные акты и работы других авторов, касающиеся правового обеспечения РФ и управления в сфере обеспечения безопасности информации, а также рассмотреть основные тенденции по ее развитию.

Задачи исследования:

- Проанализировать и раскрыть суть понятия «информационная безопасность», представленное в действующем законодательстве РФ;
- Рассмотреть нормы правового регулирования, которые направлены на осуществление безопасности в сфере информации;
- Отыскать роль безопасности в сфере информации в разделе национальной безопасности РФ;
- Проанализировать основные угрозы и опасности, оказывающие воздействие на безопасность информации;

- Отыскать и отметить вероятность улучшения норм правового обеспечения, которые направлены на обеспечение безопасности в сфере информации;
- Провести исследования действующего законодательства в сфере защиты критической информационной инфраструктуры РФ.
- Осуществить категорирование объекта КИИ согласно примеру информационной системы здравоохранения.

Методология исследования - основана на совокупности различных методик современной науки, к которым относятся общефилософские, общенаучные, правовые и специальные.

Теоретическая и эмпирическая база исследования - в процессе исследования данной работы, были проанализированы нормы правового обеспечения, которые непосредственно влияют на сферу обеспечения защищенности информации РФ, а также на коллективные труды, научную литературу и статьи, посвященные обеспечению защищенности информации. Среди проанализированных работ, следует отметить труды М. В. Демьянец, В. М. Жеребина, Г. П. Жигулина, В. Н. Снеткова, Л. К. Терещенко. Нормативную базу исследования составляют, прежде всего, Конституция Российской Федерации; федеральные законы; В качестве эмпирического материала использовались постановления и определения Конституционного Суда Российской Федерации, постановления и определения Верховного Суда Российской Федерации, официальные статистические данные, а также информация сети Интернет, затрагивающие различные аспекты исследуемой проблематики.

Новизна исследования заключается в том, что в рамках работы:

- Найдены возможности улучшения норм правового обеспечения безопасности в сфере информации Российской Федерации;
- Исследовано действующее законодательство в сфере защиты критической информационной инфраструктуры РФ;

– Проанализирована с точки зрения закона о КИИ ГИС здравоохранения, проведены мероприятия по категорированию и передача сведений во ФСТЭК.

Объект исследования работы – общественные отношения, направленные на правовое регулирование и обеспечение безопасности в сфере информации, которые относятся к информационным процессам.

Предмет исследования работы – инструменты регулирования правовых отношений, обеспечивающие информационную защиту.

Апробация исследования заключается в том, что был полностью подготовлен пакет документации по классификации объекта КИИ, проведено категорировании ГИС на примере здравоохранения. Также в ходе прохождения практики у ИП Карыпова А.П. была изучена работа предпринимателя, пересмотрена его деятельность. В результате предприниматель решил сменить форму собственности и заняться работой в сфере защиты информации, в том числе с применением закона о КИИ РФ. Опубликована научная статья.

Положения выносимые не защиту:

– Изложить понятие «национальная безопасность» так: «это комплекс условий, который обеспечивают защиту от угроз внутреннего и внешнего типа, имеющих значение в существовании и развитии государства и его интересов»;
– Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ – большой шаг вперед в сфере защиты критически важных информационных систем в сфере информационной безопасности;
– Определены ключевые направления информационно-технических угроз в РФ.

Работа состоит из введения, 3-х основных разделов и заключения.

В первой главе рассмотрено как формировалась правовая база информационной безопасности Российской Федерации, дано теоретическое обоснование необходимости правого обеспечении информационной безопасности, рассмотрена роль информационной безопасности в системе национальной безопасности Российской Федерации, рассмотрено нормативно-правовое регулирование информационной безопасности в системе права Российской Федерации.

Во второй главе рассмотрены ключевые нюансы информационной безопасности в Российской Федерации, рассмотрены и составлены ключевые угрозы информационно-технического направления, проведен анализ дальнейшего развития правовых норм необходимых для обеспечения информационной безопасности РФ.

В третьей главе рассмотрен Федеральный закон Российской Федерации о критической информационной инфраструктуре, проанализировано смежное законодательство по вопросам КИИ, на примере объекта здравоохранения сделан пакет документов для согласования категории ГИС.

1 Формирование правовой базы информационной безопасности Российской федерации

1.1 Теоретическое обоснование необходимости правового обеспечения информационной безопасности Российской Федерации

Информация выступает в качестве основного продукта постиндустриального общества, которая характеризуется в лице всемирного признака общественного развития. Переход от индустриального общества к постиндустриальному начался еще в середине XX века.

В 60-70-х гг. сформировалось огромное разнообразие всевозможных концепций, направленных на постиндустриальное общество, согласно которым общественное развитие поступательной направленности основано благодаря профессиональному и отраслевому разделению труда. Важнейшими составляющими в постиндустриальном обществе является сфера услуг, наука и образование [21].

Сущность постиндустриальной общественности раскрывается в следующем, что в тот момент, когда государством достигнут определенный экономический баланс, то на первое место выходят материальные блага, которые направлены на всестороннее развитие личности, а вовсе не экономические права [23,4].

Можно сделать вывод, что этап развития мирового сообщества направлен на увеличение значимости информационной сферы в жизни общества.

Проанализировав действующее законодательство, можно сказать о том, что определение «информация» употребляется достаточно часто в нормах правового обеспечения, обладающие комплексным характером, которые затрагивают различные сферы жизни общества.

В Федеральном законе РФ от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации» представлено опреде-

ление «информации», которое характеризуется совокупностью сведений или данных, не зависящая от формы выражения.

Многие ученые определяют понятие «информация» в качестве данных, касающихся окружающего мира и происходящих в нем процессах, воспринимающихся людьми и специальным оборудованием. Сведения выступают в роли познания в различных областях и представления о чем-либо» [30,172].

Стоит отметить следующее, что информация может обладать различным социально значимым характером, в том числе может, как приносить пользу обществу, так и оказывать негативное воздействие на государство и общественность.

В современном мире информация выступает в роли ресурса, наравне с трудовым, материальным и энергетическим ресурсами, что в свою очередь означает, что осуществление переработки ресурсов в сфере информации происходит схожим образом с материальным видом ресурсов.

Переходный период Российского государства характеризуется сменой методов производственной деятельности, мировоззрения общественности и всемирных взаимоотношений. Показатель развития общественного пространства в сфере информации в значительной степени оказывает влияние на экономическую составляющую, общественность, оборону, политическую сферу, от чего в большинстве случаев зависит отношение людей, организация общественных движений, а также достижение социальной защищенности и стабильности внутри государства [28,40].

В 80-х гг. XX в. в исследованиях Е. Масуда и Дж.Нейсбит, касающихся развития общественности в сфере информации, происходит становление концепции, которое направлено на совершенствование постиндустриального общества. Исследования отражают реальный показатель развития производственной деятельности, а также уровень распределения и использования информации в общественности [21].

Некоторые ученые ставят на одну ступень определения «постиндустриального общества» и «информационного общества». Это не совсем пра-

вильно.

Невозможно не отметить мнение ученого Попова В.В., которое заключается в следующем: «функционирование постиндустриального общества происходит благодаря предоставлению сферы услуг, а информационная разновидность общества определяется развитием потоков информации, которые совершенствуются с помощью различных научных методов» [34, 70].

Сетевая разновидность структуры общества представляет собой важнейшую составляющую модели информационной системы, в состав которой входит большое разнообразие вычислительных сетей. Формирование информационной модели взаимосвязано с переменами качественной и принципиальной разновидности в сферах жизни общества, что в свою очередь, способствует созданию единого пространства в обществе. Важнейшей стратегической задачей является правильный выбор вида политики в сфере информации [26,28].

За счет совершенствования телекоммуникационных технологий происходит процесс развития информационного общества. Благодаря данному развитию, во-первых, большинство компаний и предприятий используют в своей работе персональные компьютеры, которые подключены к трансграничным информационным сетям, во-вторых, каждая семья имеет у себя в собственности техническое устройство.

Процесс развития техники позволяет выявить новые формы и совершенствовать действующие сферы деятельности, которые неразрывно связаны с применением информационных сетей. В современном мире каждый человек должен вовремя получать актуальную и доступную информацию, а также осуществлять общение с другими людьми, вне зависимости от места проживания.

Коммуникационный процесс позволяет установить взаимодействие между различными социальными сферами. Именно поэтому, коммуникационный процесс основополагающее значение в процессе совершенствования общества в сфере информации. Проводниками в процессе осуществления

политических решений в обществе выступают Интернет и СМИ. Информация, которая транслируется благодаря Интернету и СМИ, играет немаловажную роль в процессе оказания манипуляций с сознанием общества, которые позволяют достичь политические и коммерческие цели государства.

«Стратегия развития информационного общества в Российской Федерации», которая была утверждена Президентом РФ 07.02.2008 г. № Пр-212 отражает следующее, что «Информационное общество в РФ отличается высоким показателем развития информационных и телекоммуникационных технологий, а также их активным использованием гражданами, бизнесом и органами государственной власти».

На сегодняшний день созданы условия, направленные на организацию и использование технологической, информационной и коммуникационной инфраструктуры, которые развиваются системно. Данные условия развиваются в комплексе и удовлетворяют потребности каждого человека проживающего на территории РФ, а также способны создать предпосылки, необходимые для расширения границ и совершенствования информационной среды.

Системы в сфере хозяйства, которые существуют на данный момент, преобразуются в экономическую сферу жизни общества. Благодаря переходу к постиндустриальному обществу достигается значительное усиление значения интеллектуальной составляющей в производстве [17,17].

С помощью интенсивного уровня совершенствования, которое затрагивает многие сферы жизни общества, происходит изменение системных связей и системных информационных потоков.

Преобразования, затрагивающие общественность и коммуникационные технологии, вносят актуальность информационному праву и духовной составляющей безопасности в системе информации [37,3].

Усиление значимости роли информационных технологий, их непосредственному участию во все сферы жизнедеятельности, происходит возрастание роли информационных технологий, которые обладают немаловаж-

ным значением в жизнедеятельности многих государственных институтов.

Определение информационной безопасности стоит рассмотреть с разных сторон.

Узаконенное понятие информационной безопасности отражено в Доктрине информационной безопасности РФ, которая была утверждена Президентом РФ 09.09.2000 г. № Пр-1895. Согласно определению, отраженному в Доктрине, информационная безопасность обеспечивает защиту национальных интересов в информационной сфере, которая определяется балансом совокупности интересов государства, общественности и каждого человека.

Проанализировав высказывания, которые были предложены научными исследователями, информационная безопасность характеризуется в виде состояния защищенности национальных интересов в информационной сфере.

Ученым Терещенко Л.К. были выдвинуто конкретное определение информационной безопасности, которое заключалось в следующем: «информационная безопасность – это оказание защиты национальных интересов РФ в информационной сфере, основанная на совокупности информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования, которые возникают в общественных отношениях [23,158].

Многие исследователи дают объяснение данному обстоятельству через наличие основных опасностей, другими словами, относят информационную безопасность в качестве состояния защищенности национальных интересов в информационной сфере от угроз, возникающих как внутри, так и снаружи. Один из подходов был предложен учеными технического профиля. Они рассматривают информационную безопасность в качестве деятельности, направленной на защиту свойств информации и информационной инфраструктуры техническими и организационными мерами, основываясь на положениях государственных стандартов [38,6].

Целесообразно проанализировать понятие «информационная безопасность» через возможность субъектов правоотношений выполнять следую-

щие действия, направленные на информационную сферу, а именно обеспечение функционированя, защита и развитие.

Существуют множество научных понятий информационной безопасности, например, широкое понятие: «информационная безопасность характеризуется состоянием защищенности национальных интересов в информационной сфере от внутренних и внешних угроз, которое включает в себя широкий ассортимент направлений деятельности, направленных на противоборство и защиту персональных данных». Узкое понятие информационной безопасности: «Это деятельность, обеспечивающая защиту свойств информационных систем» [38,6].

В данном случае, целесообразно разграничить понятия «информационной безопасности РФ», «безопасности информационной сферы» и «защиты информации и информационной структуры».

На сегодняшний день существуют несколько подходов, суть которых состоит в обеспечении безопасности в информационной системе. Одним из подходов является осуществление доступности информации, а другим – дозирование информации и контроль ее доступности.

Несколько лет назад в нашей стране вопрос, касающийся правового обеспечения информационной безопасности, даже не рассматривался. На сегодняшний день информационная безопасность обрела свое назначение в рамках обеспечения национальной безопасности РФ по следующим основаниям:

– Развитие информационного обеспечения является одной из основных причин, оказывающих поддержание безопасности в сфере информации на довольно высоком уровне. В ходе исследования удалось выявить, что процесс развития информационной среды играет немаловажную роль в общественном развитии и развитии каждого человека. Благодаря этому возникает необходимость в обеспечении правовой защиты и защиты информационной среды;

– Усиление положения информационных систем в глобализационных условиях. Информация по праву достойна, выступать в качестве продукта и объекта труда, основного богатства страны и стратегического национального ресурса;
– Обретение значимости силового и информационного фактора в политической сфере общества, которая выражается в возможности эксплуатации интеллектуального потенциала других стран, внедрении духовных и идейных ценностей, культуры, языка, возможности тормозить духовно-культурное развитие других стран, трансформации духовно-нравственных устоев [29,30].

Следует отметить прямую взаимосвязь, возникшую между научно-техническим прогрессом и информационной безопасностью человека. Процесс развития техники и науки способствует повышению значения безопасности в сфере информации.

Критические компоненты, при воздействии на них может спровоцировать возникновению следующих обстоятельств:

– Возникновение глобальный аварий;
– Дезорганизация государственного и военного управления, финансовых систем, научных центров;
– Спровоцировать военные конфликты.

Многие сферы жизни, касающиеся государства, общественности и человека уже невозможно представить без достижений в сфере научно-технического прогресса, которые буквально за несколько лет смогли проникнуть с них настолько, что их уже без них эти сферы представить невозможно.

Благодаря возрастанию роли информационных систем, XXI в. стали именовать веком информации. Существенное значение в котором должно играть право и организационно-техническая составляющая.

1.2 Информационная безопасность в системе национальной безопасности Российской Федерации

Основной составляющей в государственном управлении является законодательное обеспечение в сфере информационной безопасности. Определение «безопасность», которое отражено в действующем законодательстве РФ, научных трудах и СМИ, рассматривается с разных точек зрения.

Безопасность может быть обеспечена различным сферам, например, экономике, финансам, экологии, информации, энергии и т.д. Посягательство на данные сферы может спровоцировать преобразование государственного устройства.

В Федеральном законе Российской Федерации от 28.12.2010 г. № 390-ФЗ «О безопасности» нет определения безопасности, несмотря на это в законе отражена суть деятельности, исходя из обеспечения, к которым относится:

- Рассмотрение основных угроз безопасности, а также предложение мер по их устранению;
- Определение направлений в государственной политике;
- Стратегический вид планирования, который направлен на оказание безопасности;
- Формирование правового регулирования в сфере обеспечения информации;
- Разработка и применение комплекса оперативных и долговременных мер по выявлению, предупреждению и устранению угроз безопасности, локализации и нейтрализации последствий их проявления;
- Использование экономических методов, которые направлены обеспечение информации;
- Применение современных разновидностей вооружений, к которым относится военная техника и техника специального назна-

чения, позволяющая обеспечить безопасность;

- Осуществление научных исследований, касающихся организации безопасности;
- Осуществление контроля, направленного на деятельность государственных органов власти, органов местного управления в сфере безопасности;
- Финансирование сферы обеспечения безопасности;
- Контроль расходов в сфере безопасности;
- Сотрудничество на мировом уровне, направленное на обеспечение безопасности;
- Организации других мер, направленных на обеспечение безопасности.

В действующая Конституции РФ, которая была принята в 1993 году, определение «безопасность» отражено в следующих статьях:

- ч. 5 ст. 13 - «Запрещается создание и деятельность общественных объединений, цели или действия которых направлены на подрыв безопасности государства»;
- ч. 3 ст. 37 - «Каждый имеет право на труд в условиях, отвечающих требованиям безопасности»;
- ч. 3 ст. 55 и ч. 1 ст. 56 – данные статьи отражают условия допустимости ограничения прав и свобод человека, в которые включена безопасность государства и граждан;
- п. «м» ст.71 - определяет безопасность к ведению РФ;
- п. «б» и «д» ст. 72 - закрепляют за совместным ведением Российской Федерации и ее субъектов обеспечение общественной и экологической безопасности;
- ч. 2 ст. 74 - в данной статье предусмотрена при необходимости обеспечения информации, возможность ограничения перемещения товаров и услуг в РФ;

– ч. 1 ст. 82 - при вступлении в должность Президент РФ приносит присягу, в которой обязуется защищать безопасность государства;
– п. «ж» ст. 83 -закрепляет полномочия главы государства по формированию и руководству Советом Безопасности РФ, статус которого определяется Федеральным законом Российской Федерации от 28.12.2010 г. № 390-ФЗ «О безопасности»;
– п. «д» ч. 1 ст. 114 - относит к ведению Правительства Российской Федерации обеспечение государственной безопасности [1,4398].

На основе анализа статей Конституции РФ, определение «безопасность» изложено в разных значениях. На сегодняшний день, можно выделить три уровня теоретического и методологического знания о безопасности:

– Философия безопасности;
– Специальная теория безопасности;
– Теория национальной безопасности.

С помощью философии безопасности происходит создание и сохранение субъектом условий собственного существования, с помощью которых происходит процесс соблюдения интересов, реализация выдвинутых целей и задач, в основании которых лежат его ценности, которые обусловлены различным уровнем значимости, необходимых для самореализации личности.

Специальная теория безопасности служит для раскрытия способов, позволяющих обеспечить информацией личность, общество и природу, которая касается множества социальных систем.

Общая теория национальной безопасности позволяет произвести объединение таких разновидностей наук, как политические, экономические, прикладные, социальные, логические, которые направлена на исследование средств в области обеспечения безопасности государства, общественности и человека в условиях комплексного воздействия внешних и внутренних фак-

торов различного характера. К задачам общей теории национальной безопасности относятся:

- Анализ научных трудов и работ;
- Решение методических задач;
- Правовая организация;
- Рассмотрение понятий фундаментального характера;
- Разработка концептуальных понятий и т.д.

Проанализировав сферу безопасности, которое взяло свое начало еще в 90-х годах прошлого столетия, это дало толчок к теоретическому развитию сферы безопасности, которое выступает в качестве методологической базы, позволяющей решить задачи в правовой, организационной и правоприменительной сфере.

В научных работах наибольшую популярность обрели концепции, касающиеся национальной безопасности [27,30].

Как уже было сказано, повышение роли информационных систем обусловлено общественному прогрессу и научно-технической революции. Благодаря этому, информацию стали рассматривать в виде основного компонента интеллектуальной и материальной деятельности людей. В связи с данными изменениями, правовая политика стала своей целью видеть реализацию национальных интересов, что в свою очередь предполагает:

- Соблюдать конституционные права и свободы, которые затрагивают доступ к информации, содержащей культурные и научные достижения страны;
- Обеспечить правовое регулирование государственной политики в сфере информации, которое направлено на предоставление актуальной информации и обеспечение доступа граждан к информационными ресурсам, располагающимся в открытом доступе;
- Оказать содействие в развитии информационных технологий;
- Накопить, сохранить и эффективно использовать современные информационные ресурсы;

– Обеспечить безопасность информационных ресурсов от несанкционированного доступа к ним;
– Не допустить противоправную деятельность в отношении информационного пространства и т.д. [28,41]

На сегодняшний день в РФ происходит правовое обеспечение национальной безопасности, которое основано на взаимодействии основных норм правого обеспечения, содержащих юридические принципы, которые своей целью ставят управление общественными отношениями в сфере обеспечения национальной безопасности для их упорядочения, безопасности и развития в соответствии с гражданскими потребностями [27,29].

Юридическая литература излагает, что между государственной деятельностью и национальной безопасностью существует неразрывная связь. Совершая упор на государственный аппарат и органы власти, государство способно оказать защиту населения, а также создать благоприятные условия для проживания граждан. Социальные силы не способны выполнить данную задачу.

Национальная безопасность относиться как к юридической, так и к политологической категории. Для политики, направленной на сферу национальной безопасности характерно широкое разнообразие видов и форм, также она способна в своей деятельности использовать следующие виды средств, к которым относятся военные, экономические, политические, экологические и т.д. [31,47]

Цель судебных органов состоит в выявлении проблем, касающихся обеспечения национальной безопасности, которые требует незамедлительного решения.

Конституционный суд в своих решениях в большинстве случаев отталкивается от аспектов национальной безопасности. В свою очередь, Конституционный суд не узаконил понятие «национальная безопасность», даже несмотря на то, что оно играет немаловажную роль в осуществлении суверенитета РФ, который выступает в качестве основного элемента конститу-

ционного строя [25,1].

Указом от 12.05.2009 г. № 537 Президента РФ была утверждена «Стратегия национальной безопасности Российской Федерации до 2020 года», которая является базовым правовым документом, направленным на планирование совершенствования системы национальной безопасности. Данная стратегия отражает ряд мер, которые направлены на организацию национальной безопасности. Стратегия позволяет конструктивно взаимодействовать государственным органам власти с организациями и общественными объединениями в сфере защиты национальных интересов.

«Стратегия национальной безопасности Российской Федерации до 2020 года» излагает узаконенное понятие «национальная безопасность», которое, во-первых, состоит в оказании защиты граждан, общественности и государства от угроз, как внешних, так и внутренних, во-вторых, состоит в обеспечении конституционных прав, свобод и достойного уровня жизни.

Обладание информацией – это фактор в современном мире, обеспечивающий контроль в решении любых задач. Обладание информацией позволяет значительно повысить эффективность, как многочисленных государственных сфер деятельности, так и предприятий, что по результату позволит достичь значительных успехов в экономике, финансах и т.д. К субъектам, обладающим ценной и полезной информацией, выдвигается больший показатель ответственности в ее защите и сохранности, в случае возникновения негативных факторов.

Информация может спровоцировать возникновение аварий, происшествий, военных конфликтов, а также дезорганизацию управления государства.

Доктрина в сфере информационной безопасности РФ, которая была утверждена Президентом РФ 09.09.2000 г. № Пр-1895, «На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности». С помощью

информации и информационных технологий определяются основополагающие пути развития общественности и государства, что в конечном счете оказывает влияние на формирование личности человека, а также определение его места в обществе. [19,11] Можно сделать вывод о том, что информационная безопасность – это основополагающее звено, обеспечивающее существенные интересы РФ, т.к. угрозы и опасности национальной безопасности осуществляются на информационные системы.

В настоящий момент общество в информационной сфере является достаточно защищенным в тех ситуациях, когда социальные субъекты обеспечены актуальной и достоверной информацией, позволяющей гражданам ориентироваться в определенной ситуации, а также принимать те или иные решения на основе полученной информации. Значение данного компонента национальной безопасности усиливается с помощью расширения содержания информационной безопасности и необходимость построения информационного общества в России, сменой угроз «холодной войны» и вызовами «информационной войны». [22, 198].

1.3 Нормативно-правовое регулирование информационной безопасности в системе права в Российской Федерации

Обеспечение в сфере права следует рассматривать с точки зрения информационного права. Законодательство в сфере информации представляет собой достаточно молодую отрасль. Появление Интернета и развития общественных отношений потребовало правового регулирования, а также организации политики в сфере информации и обеспечения ее безопасности.

22.07.2000 года на встрече под названием «Большая восьмерка» была узаконена Окинавская хартия обширного информационного общества. Содержание Хартии составляло положение, согласно которому информационные и телекоммуникационные технологии выступают в качестве основополагающего фактора, который оказывает немаловажное влияние на развитие

общества XXI века. После принятия Хартии страны, входящие в «Большую восьмерку» ввели у себя положения, позволяющие организовать систему информационного общества.

Благодаря проникновению информации в большинство различных сфер деятельности государства, она приобретает следующие виды стоимостных выражений, а именно политическое, материальное или стоимостное. Правовое управление в информационной сфере, благодаря возрастанию роли информации, выступает в качестве основного законопроекта, которое основано на обеспечении информационной безопасности страны.

Состав информационной сферы до 1995 года включали лишь разрозненные нормы правового регулирования. Но на сегодняшний момент в состав информационной базы входят значительное количество указов и норм, например, законодательные акты РФ, указы Президента РФ, постановления Правительства РФ, нормативно-правовые акты федеральных органов исполнительной власти, а также нормы субъектов РФ. [23]

Конституция РФ, которая была принята в 1993 году, является основным источником права, который основан на оказании информационной безопасности.

В Конституции РФ отражены следующие пункты, качающиеся информации:

– Статья 23 - «Гражданин имеет полное право на неприкосновенность собственной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений»;
– Статья 24 - «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются»;
– Статья 29 - «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, перечень сведений, составляющих государ-

ственную тайну, определяется федеральным законом»;

- Статья 42 - «Каждый имеет право на достоверную информацию о состоянии окружающей среды». [1,4398]

Федеральный закон РФ «Об информации, информатизации и защите информации», принятый в 1995 года, выступающий в качестве основного законодательного акта, действующего с конца XX – по начало XXI веков, целью которого является регулирование отношений в информационных сферах и отношений, которые касаются обеспечения безопасности и защиты информационных систем. Данный закон излагает основные задачи, связанны с персонализацией данных, сертификацией информации, лицензирования информационный систем и обеспечения информационных ресурсов.

В Федеральном законе, который был принят в 1995 году, произошли изменения по причине принятия нового Федерального закона в 2006 году № 149 ФЗ «Об информации, информационных технологиях и о защите информации», в котором указано, что данный закон может регулировать следующие отношения, которые могут возникнуть при следующих обстоятельствах:

- в случае осуществления права на поиск, передачу, хранение информации;
- в случае применения информационных технологий;
- в случае обеспечения безопасности информации.

К определению «информационная безопасность» в РФ выдвигаются два вида подходов, а именно нормативно-правовой и государственный.

Информационная безопасность характеризуется состоянием защищенности базы информации, а также является основной составляющей как в государственной, так и национальной безопасности.

Федеральный закон РФ от 03.04.1995 г. № 40-ФЗ «О Федеральной службе безопасности», узаконенный в 1995 году, отражает следующую информацию: «Федеральная служба безопасности является единой централизованной системой органов федеральной службы безопасности, цель кото-

рой состоит в осуществлении решений, направленный на обеспечении информационной защиты РФ, исключительно в пределах допустимых полномочий».

Основной задачей органов федеральной службы является осуществление информационной безопасности, которая должна выполняться в соответствии со следующими полномочиями:

- Формирование и использование научно-технической политики и политики государства, касающейся области обеспечения информационной безопасности, при этом используя различные криптографические и технические средства;
- Обеспечение криптографическими и техническими методами защиты информационных систем, а также связей специального назначения, обеспечивающие передачу достоверной зашифрованной информации.

9 сентября 2000 г. Президент РФ утвердил Доктрину информационной безопасности РФ, представляющую собой взаимосвязь взглядов, целей и задач, направленных на обеспечение защиты информационной базы.

Доктрина информационной безопасности состоит из четырех разделов, которые подразделяются на следующие пункты:

- «Национальные интересы Российской Федерации в информационной сфере и их обеспечение»;
- «Виды угроз информационной безопасности Российской Федерации»;
- «Источники угроз информационной безопасности Российской Федерации»;
- «Состояние информационной безопасности Российской Федерации и основные задачи по её обеспечению»;
- «Общие методы обеспечения информационной безопасности Российской Федерации»;
- «Особенности обеспечения информационной безопасности Рос-

сийской Федерации в различных сферах общественной жизни»;

- «Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности»;
- «Основные положения государственной политики обеспечения информационной безопасности Российской Федерации»;
- «Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации»;
- «Основные функции системы обеспечения информационной безопасности Российской Федерации»;
- «Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации».

Доктрина информационной безопасности РФ играет немаловажное значение в следующих направлениях, а именно:

- Организация политики государства, которая затрагивает область обеспечения защиты;
- Подготовка и реализация предложений, направленных на совершенствование правовой, методической и научно-технической базы информационной безопасности;
- Внедрение основных программ, которые направлены на осуществление защиты в сфере безопасности.

На сегодняшний момент был поднят вопрос, касающийся принятия нового проекта Доктрины информационной безопасности, по причине актуализации подходов, направленных на защиту национальных интересов страны. Данный вопрос был поднят 7.04.2015 года на заседании Межведомственной комиссии по информационной безопасности Совета Безопасности РФ.

Стоит отметить, что на первый план в области развития отрасли информационных и коммуникационных технологий выходят задачи повышения конкурентоспособности российской продукции, формирования условий

для ее широкого использования при создании отечественных информационных систем и сетей связи, технических средств обеспечения информационной безопасности объектов национальной информационной инфраструктуры.

На заседании Межведомственной комиссии 7 апреля 2015 года была рассмотрено, что новая редакция Доктрины информационной безопасности должна быть неразрывно связана с ключевыми документами стратегического планирования, разработка которых предусмотрена положениями Федерального закона Российской Федерации «О стратегическом планировании в Российской Федерации». [47]

В 2008 г. Президентом Российской Федерации (07.02.2008 г. № Пр-212) была утверждена «Стратегия развития информационного общества в Российской Федерации». Данная стратегия содержит цели, задачи, принципы и основополагающие направления государственной политики в области использования и развития информационных и телекоммуникационных технологий, науки, образования и культуры, необходимого для продвижения страны по пути формирования и развития информационного общества».

Стратегия развития информационного общества в Российской Федерации затрагивает следующие области деятельности:

- Формирование современной информационной и телекоммуникационной инфраструктуры, а также презентация её основе качественных услуг в сфере информационных и телекоммуникационных технологий и обеспечение высокого уровня доступности для населения информации и технологий;
- Повышение качества сферы образования, медицинского обслуживания, социальной защиты населения, благодаря развитию и использованию телекоммуникационных и информационных технологий;
- Преобразование системы государственных гарантий конституционных прав и свобод человека в информационной сфере;

- Развитие экономики РФ, с помощью информационных и телекоммуникационных технологий;
- Повышение эффективности государственного управления и местного самоуправления, взаимодействия гражданского общества и бизнеса с органами государственной власти, качества и оперативности предоставления государственных услуг;
- Развитие науки, технологий, техники и подготовки квалифицированных кадров в сфере информационных и телекоммуникационных технологий;
- Сохранение культуры многонационального народа Российской Федерации, укрепление нравственных и патриотических принципов в общественном сознании, развитие системы культурного и гуманитарного просвещения;
- Противодействие использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам России.

12 мая 2009 года указом Президента РФ была утверждена до 2020 года «Стратегия национальной безопасности Российской Федерации», которая выступает в качестве базового правового документа, направленного на планирование развития системы обеспечения национальной безопасности РФ, в котором отражается порядок действий и меры по обеспечению национальной безопасности.

С помощью вышеуказанной стратегии происходит конструктивное взаимодействие органов государственной власти, организаций и общественных объединений, направленное на обеспечение защиты национальных интересов РФ и обеспечение безопасности личности, общества и государства.

Вводная часть Стратегии составляет ряд важных положений, согласно которым в условиях глобализации процессов мирового развития, международных политических и экономических отношений, формирующих новые угрозы и риски для развития личности, общества и государства, Российская

Федерация в качестве гаранта благополучного национального развития успешно переходит к новой государственной политике в области национальной безопасности. [31,46]

15 апреля 2014 года №313 постановление Правительства РФ утвердило государственную программу РФ «Информационное общество (2011-2020 годы)», которая состоит из следующих подпрограмм:

- «Информационно-телекоммуникационная инфраструктура информационного общества и услуги, оказываемые на её основе»;
- «Информационная среда»;
- «Безопасность в информационном обществе»;
- «Информационное государство»;
- федеральная целевая программа «Развитие телерадиовещания в Российской Федерации на 2009-2015 годы».

Все вышеперечисленные подпрограммы, кроме последней, состоят из двух периодов:

- Первый период с 2011-2014 гг.;
- Второй период с 2015-2020 гг.

Благодаря Приложению, прикрепленного к программе, можно высчитать динамику развития общественности, исходя их, его показателей и данных. Россия на международном уровне, исходя из индекса развития информационных технологий: с 2010-2012 гг. - 48 место, в 2013 г. - в числе 40 ведущих стран, в 2015 г. - в числе 20 ведущих стран, с 2016-2020 гг. - в числе 10 ведущих стран.

Помимо всех вышесказанных нормативно-правовых и подзаконных актов существуют и другие указы, например:

- указ Президента РФ от 17.03.2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- распоряжение Правительства Российской Федерации от

01.11.2013 г. № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года»;

– распоряжение Правительства Российской Федерации от 29.12.2014 г. № 2769-р «Об утверждении Концепции региональной информатизации» и прочее.

Итак, сделаем выводы по первой главе:

– проанализировав вышесказанную информацию, можно сказать о том, что начало 90-х годов характеризуется начальным уровнем в формировании законодательства в сфере информационного и телекоммуникационного развития;

– на сегодняшний день, когда законодательство в сфере информационных технологий представляет собой достаточно большой массив данных, пора отказаться от количественного роста и перейти к качественному преобразованию. Отказ от количественного преобразования очень важен, т.к. за период существования и применения законодательства, затрагивающую информационную сферу и телекоммуникационные технологии, отчетливо выявились недочеты, которые были допущены в процессе разработки соответствующих законодательных актов;

– несмотря на активное совершенствование законодательства, затрагивающую информационную сферу, телекоммуникационные технологии, большое количество проблем так и осталась нерешенными, а многие вопросы, как показала практика, требуют существенной корректировки уже утвержденных актов нормативно-правового регулирования. [23,2]

2. Система правового обеспечения и управления информационной безопасности РФ и особенности ее совершенствования

2.1 Ключевые нюансы информационной безопасности в РФ

Информационная область выступает в качестве системообразующего аспекта в жизни социума. Безусловно, она имеет серьезное воздействие на состояние безопасности в стране. Речь идет о защищенности с точки зрения политики, экономики, обороны, науки, техники, духовности и т. д. Каждый из этих пунктов характеризуется особенностями обеспечения информационной безопасности, которые связаны со спецификой объектов, уровнем их уязвимости по отношению к угрозам извне.

На сегодняшний день информация и технологии, которые с ней связаны, прямо и непосредственно относятся к сфере политики. В качестве базовых условий для того, чтобы структуры политической направленности могли существовать беспрепятственно, а воздействия были эффективными, выступают такие процедуры, как сбор, накопление, обработка, распространение данных.

Если опираться в этом вопросе на мировой опыт, то можно отметить, что он показал информацию как основную причину угрозы. В связи с этим в обязательном порядке требуется информационно-правовое регулирование потоков данных. В СМИ и на просторах Интернета предоставлено много сведений в политической сфере, поэтому данные ресурсы играют важную роль. [49][54]

Все большее количество государственных структур, политических партий и объединений общественного характера стремится к открытию собственных сайтов. По этой причине граждане обретают большее количество возможностей, связанных с принятием участия в политической жизни социума и государства за счет прогрессивных устройств техники. Они

могут активно обсуждать законопроекты, проявлять инициативы, жаловаться и обращаться по определенным адресам.

Что касается непосредственно самой информационной безопасности в области политических отношений, в рамках всего процесса она может рассматриваться как целый комплекс элементов. Ключевые направления информационной безопасности в политической сфере выглядят следующим образом:

- в области политических интересов;
- отношений;
- избирательной процедуре;
- в партийно-политическом аспекте;
- во внешнеполитической области.

Отношения в сфере политики в сложившихся условиях демократии подразумевают задействование определенных форм коммуникации, пребывающих в зависимости от интересов и потребностей определенных сил, осуществляющих борьбу за власть. Информационные технологии начинают соотноситься с политическими отношениями и оказывать на них серьезное влияние.

Если властные структуры начнут чрезмерно контролировать информацию, это чревато вероятностью ее сокрытия и ограничением доступа. Также может возникнуть феномен нежелательного и даже незаконного распространения данных. Ситуация усугубляется еще и тем, что в последнее время этот контроль становится все более выраженным с политической точки зрения. [32,67]

Если сделать вывод о том, что было сказано выше, то в связи с внушительной информатизацией отношений в области политики актуальной является проблема безопасности информации в области политики. Для определения специфики воздействия информационных угроз на экономическую защищенность она должна рассматриваться с трех сторон в

соответствии с масштабами реализации. Речь идет о государственном, корпоративном, личностном направлении. [54]

1. Государственный уровень. В условиях развития информационной экономики наблюдается многократное возрастание необходимости защиты информации и технологий, а также аналогичных систем. Таким образом, Пентагон в целях разработки соответствующих средств каждый год расходует порядка 5 млрд. долларов. Если же вести речь о государственной службе, осуществляющей перехват сообщений, этот параметр равен 5 млрд. долларов. [54]

В государственных масштабах все это приводит к тому, что максимальное количество средств вкладывается не в сам экономический процесс, а в формирование идеальных информационно-компьютерных инструментов, способствующих защите данных, средств разведки электронного характера в целях обеспечения преимуществ. В итоге стоит вести речь об отставании значения ВВП. [53]

Стоит отметить, что валовой внутренний продукт выступает в качестве важнейшего параметра, характеризующего экономическую безопасность страны. Если он недополучен по причине информационных угроз, происходит сокращение уровня экономической безопасности государства.

В качестве еще одной серьезной угрозы экономической безопасности в условиях информационной экономики выступает киберпреступность. О ней пойдет речь в этой работе далее.

Глобальные негативные последствия может вызвать «цифровой разрыв», разделяющий социум на 2 части: тех, кто вправе пользоваться IT, и тех, кто не может этого делать по разным соображениям. Информационное превосходство выступает в качестве значимой социальной силы, которая способна привести к перераспределению ресурсной базы. Если же в данном направлении имеется неравенство, оно только усиливает дифференциацию в социуме.

2. Корпоративный уровень. В условиях экономики информационного типа информация стала выступать в качестве средства конкуренции. Она стала иметь стоимость, которая зависит от суммы прибыли. Информация, которая была извлечена из фирмы, может стать не очень удачным средством против нее самой. Поэтому руководство любого предприятия должно предотвращать утечку данных.

На сегодняшний день интернет представляет собой рабочий инструмент, без которого компании не могут обходиться. Он выступает в качестве глобального справочника и открывает доступ к технологиям. С его помощью можно передавать данные и просто-напросто общаться. Если произойдет атака на веб-сервер компании, это может привести к потере значительной части клиентов.

Информация в организации ворується не только снаружи, но и изнутри, т. е. «похитителями» могут быть сотрудники. Наряду с этим крупные убытки фирма рискует понести по причине неграмотности и халатности персонала.

Наряду с этим существует несколько других примеров угроз экономической безопасности. Например:

- отсутствие контроля доступа к сети Интернет сокращает значение производительности труда в коллективе;

- возможность применения рекламы в личных целях;

- снижение параметров пропускной способности сети Интернет ввиду нагрузки на сети.

В любом случае все это приводит к снижению степени экономической безопасности корпораций.

3. Личностный уровень. В настоящее время деловая и частная жизнь многих миллионов людей отслеживается. Так, фиксируются совершенные по телефону звонки, платежные операции, декларации, приобретения в магазинах. Поэтому в современном мире важную роль играет защита персональных данных. Одна из распространенных групп угроз экономиче-

ской безопасности обусловлена использованием большим количеством людей дебетовых и кредитных карт.

Еще одна серьезная угроза – кибермошенничество. Оно получило широкое распространение в отношении следующих объектов:

- электронные кошельки и обещание получения крупного дохода на них;
- предложения реального заработка в социальных сетях;
- навязчивая реализация пакетов с готовым бизнесом;
- ложные объявления о попадании в сложные жизненные ситуации;
- сайты-двойники.

На сегодняшний день наибольшую опасность и угрозу представляют спам сообщения и мошеннические действия по СМС. Оператор «Мегафон» после подведения итогов прошлого года отметил, что суммарное количество таких отправлений, которые были заблокированы, в 2014 году превзошло отметку в 1,5 млрд., в то время как годом ранее этот показатель был в 1,5 раза меньше. [41]

Еще одна существенная угроза экономической безопасности личности в экономических условиях, имеющая особую значимость, как считают эксперты, заключается в атаке на системы, которые массово применяются в современном мире. Основная цель, с которой они организуются, заключается во взаимодействии с устройствами, которые контролируют процесс существования, передвижения и функционирования многочисленных сервисов. Взлом этих систем осуществляется по причине желания бесплатно пользоваться разными сервисами. [40,33]

Специфика, характеризующая влияние информационных угроз на безопасность экономического характера, представлена в Приложении А. Если принимать во внимание важность информатизации для создания и развития экономических, политических отношений, можно отметить, что есть острая потребность в улучшении качества защиты интересов. Важную роль играет защита интересов социума и государства в процессе

распространения технологий компьютерного характера, которые связаны с попытками передачи способностей. [39,20]

2.2 Ключевые направления информационно-технических угроз в РФ

В последнее время появилось большое количество видов преступных посягательств. Связано это, в первую очередь, с активным развитием и улучшением компьютерных технологий. В качестве основных объектов этих злодеяний выступают данные и прочие информационные ресурсы, а также электронные деньги. По этим соображениям на сегодняшний день исследователи выделяют одновременно несколько групп опасностей.

Первая категория включает в себя образование и развитие информационного оружия, обладающего способностью эффективно влиять на психический фон и сознание. Активное изучение этих процессов подтверждает тот факт, что психология может изменяться с течением времени согласно направлениям деятельности в сети. Особенно это касается представителей молодого поколения. Данный феномен приводит к формированию зависимости.

Интернет-зависимость имеет тесную и непосредственную взаимосвязь с проникновением в подсознание. Она подразумевает электронную несвободу. Именно на этом пути развития находится современное человеческое общество. На практике существует немало проявлений «виртуализма». Речь идет о том, что личность нацелена на уход от реальных проблем в цифровое пространство. Так что использование современных средств и инструментов, а также методов информационного влияния делает общество управляемым. [40,32]

В качестве противодействия этой угрозе выступает безопасность информационно-психологического характера, которая может быть определена как базовый элемент всей этой системы. В итоге формируется

состояние защищенности человеческой психики, а также группового сознания. Причем в данном случае требуется не защита информации, а защита от разрушающего действия сведений. В качестве объекта влияния в данном случае выступает сам человек, а точнее – его психический фон. То есть в рамках категории информационно-психологической безопасности слово «психологическая» подразумевает конкретный объект, а слово «информационная» - тип угроз. [35,36]

Вторая группа традиционно включает контроль жизни индивидуума и социума с применением электронных технических ресурсов без получения уведомления от граждан. В связи с этим нередко без предупреждения человека подслушиваются его телефонные разговоры, ведется контроль переписки.

Что касается третьей группы опасностей, к ним относится возможность применения современных IT в целях политического характера. Борьба за осуществление контроля новых СМИ и информационной структуры, а также их применение в целях учета и обработки общественного мнения. Все это представляет собой масштабную проблему внутриполитического характера, особенно в рамках избирательных кампаний.

Четвертая группа включает в себя образование нового класса преступлений социального характера. В их базе традиционно лежит применение прогрессивных технологий. Многие эксперты в данной сфере убеждены в том, что компьютер выступает в качестве часто используемого орудия преступлений.

В УК РФ к злодеяниям в области компьютерной информации относят несколько явлений одновременно. По ст. 272 это неправомерный доступ к данным, 273 – формирование, применение и распространение софтов вредоносного содержания, 274 – несоблюдение норм эксплуатирования инструментов хранения, обработки и передачи сведений.

В ФЗ№420 от 7 декабря 2011 года дано детальное понятие компьютерной информации, которая выступает в качестве предмета

преступления и включает в себя сведения, представленные электрическими сигналами. На сегодняшний день подобные преступления встречаются относительно редко, но постепенно их количество увеличивается. Подробная информация о преступлениях в области компьютерной информации дана в Приложениях Б, В.

Наряду с этим существует еще несколько значимых терминов. Например, «киберпреступность» - это слово нередко употребляется в качестве синонима к первому понятию. Есть несколько точек зрения, связанных с соотношением между этими понятиями. Исследователи утверждают, что рассматривать их стоит вместе, чтобы получить объективную картину.

Одна из позиций гласит о том, что рассматриваемый феномен в англоязычном варианте является более широким в сравнении, например, с компьютерной преступностью. Он способствует детальному и глубинному отражению природы данного явления в рамках информационного пространства. Так, в английском языке часть слова «cyber-» выступает в качестве значимого компонента и в переводе означает что-то, что связано с компьютерами, IT-сферой, интернетом. Так, под термином «cybercrime» принято понимать собственно сам факт преступности с использованием глобальных сетей.

Кузьмин Алексей Сергеевич, являющийся заместителем начальника Центра защиты информации, в рамках 16 Национального форума сообщил о том, что информационное оружие становится все более опасным. Наряду с этим в области этой борьбы наблюдается множество опасных тенденций, связанных с воздействием на информационные объекты. В последнее время также популярными стали услуги, связанные с атаками, причем стоят они недешево. А поскольку данный рынок активно формируется, это свидетельствует о наличии спроса. В течение последних нескольких лет удалось выявить порядка 25 млн. образцов ПО. Что касается оборота денег в этом сегменте, он почти сравнялся с оборотом наркотических веществ. [43]

Как отмечается в Управлении «К», а именно – в Бюро особых мероприятий технического характера, МВД РФ, в качестве базового мотива, на основании которого действуют киберпреступники, выступает стремление к получению материальной выгоды. И если какое-то время назад компьютерные преступления совершались исключительно из хулиганских побуждений или стремления демонстрации собственных навыков, в последнее время ситуация изменилась. На сегодняшний день даже хищение личных данных нацелено на воровство денег.

В 2013 году фискальные органы, осуществляющие управление в рамках МВД РФ, а также их региональные подразделение направили свыше 6,5 тыс. уголовных дел. Наряду с этим произошло пресечение деятельности многих крупных преступных группировок. Это, в свою очередь, привело к установлению лиц, причастных к формированию и применению этих программ. Практика показала, что злоумышленники получили личные данные целых десятков тысяч клиентов.

Наряду с этим работники управления «К» сумели предотвратить факт хищения порядка 1 млрд. рублей со счетов банков граждан. Также им удалось предотвратить действие известной бот сети, которая была сформирована на базе т. н. «банковских троянов». На тот момент, когда фигуранты этого злодеяния задерживались, число зараженных компьютеров приравнивалось к отметке в 6 млн., а сумма причиненного ущерба составила более 150 млн. р. [45]

На основании сведений, полученных от Федеральной службы безопасности РФ, только на объекты, относящиеся к информационной инфраструктуре Президента, Правительства, Госдумы, Совета, каждый день совершается несколько десятков атак. Это, в свою очередь, может привести к дестабилизации процессов экономики, подрыванию суверенитета и нарушению функционирования основных механизмов жизнеобеспечения. Разумеется, возникает прямая угроза национальной безопасности.

В рамках интервью, представленного «Российской газете», секретарь Совета Безопасности РФ по имени Н. П. Патрушев отметил, что эти угрозы являются однозначными и требуют срочной реализации мер по противодействию. В качестве основного шага для решения данного вопроса выступает создание документов, связанных со стратегическим планированием. Речь идет, в первую очередь, о базовых направленностях политики государства в сфере безопасности и создания автоматизированных систем управления процессами. [47]

Технологии информационного и телекоммуникационного характера создают множество новых возможностей для классических форм криминальной деятельности, а это, как правило, приводит к увеличению количества мошеннических действий, которые базируются на доверии. В данном случае применение информационных технологий происходит в качестве удобного инструмента для поиска жертв, перевода денежных средств, а также сокрытия следов собственной деятельности. Если верить оценкам экспертов, каждую секунду жертвами подобных деяний становится 12 человек во всем мире, и каждый год этот показатель увеличивается.

Особое внимание стоит уделить речи Мошкова А. Н., который в рамках 17 Национального форума сообщил следующее. По данным ведомства 2014 года на территории РФ произошла регистрация 11 000 преступных деяний, которые связаны с мошенничеством во всемирной паутине. Как и ранее, в качестве основного мотива подобных поступков выступает извлечение выгоды материального характера. Именно по этой причине порядка 41% преступлений, которые были зарегистрированы, представляют собой кражи. [44] Таким образом, за годовой отрезок времени, а именно – с 2013 по 2014 год – число преступных деяний в информационной сфере значительно возросло. Темп роста составил 4,5 тыс., или 59%.

Эксперты, осуществляющие деятельность на территории крупнейшего изготовителя программного обеспечения в РФ под названием «Лаборатория Касперского», считают, что на протяжении 10 лет развитие

киберпреступности будет осуществляться в шпионажном направлении. Специалисты также считают, что оно будет специализироваться на атаках.

Шпионские действия в коммерческом секторе, кражи баз данных, покушения информационного характера для решения задач подрыва репутации – все это будет востребованным в условиях информационной экономики. В лаборатории есть версия, что вскоре придет серьезная война хакеров и профессионалов компьютерного дела, которые им противостоят.

Таким образом, можно без труда вести речь о создании нового направления теневого экономического сектора. Речь ведется непосредственно о «черном» кибер рынке, который оказывает отрицательное влияние на экономическую безопасность всей страны.

Стоит также отметить, что масштабное развитие кибершпионажа в экономических масштабах подразумевает далеко не самые лучшие последствия. Дело в том, что наиболее прибыльные корпорации, которые могут закупать дорогостоящие системы информационных технологий, обретут возможность добычи некоторых данных, которые являются недоступными для конкурентов. При этом наблюдается нарушение естественной информационной структуры, формирование условий для спекуляции на известных рынках и биржах. Наряду с этим прогрессивные технологии применяются в целях формирования ложного имиджа организация, завышения рейтингов и даже шантажа. [40,28]

В рамках 2001 года государства на территории Европы в городе Будапешт пришли к выводу о необходимости подписания конвенции о киберпреступности. Она стала действовать, начиная с 1 июля 2004 года. Годом позднее в силу вступило распоряжение Президента РФ о ее подписании. Тем не менее, в 2008 году его юридическая сила была утрачена.

Произошло это по причине появления второго пункта ст. 32 Конвенции. В ней сказано, что сторона, не получив согласия другой стороны, через компьютерную сеть может получить доступ к хранящимся данным. Также она может сделать это на базе добровольного согласия лица,

обладающего законными полномочиями к раскрытию этих сведений. Именно в связи с такими обстоятельствами Конвенция не была ратифицирована в РФ.

Глава МВД РФ по имени Колокольцев В. А. 4 ноября 2014 года стал активным участником министерской встречи, 83-й сессии ассамблеи Интерпола. Произошла она на территории государства Монако. Он отметил, что нынешняя конвенция, имеются тесное и непосредственное отношение к Совету Европы, связанная с киберпреступностью, с 2001 года стала устаревшей, и для нее характерны кое-какие недостатки. В сложившихся обстоятельствах она, к сожалению, не может обеспечить необходимый уровень координации сообщества международного типа в области противодействия надвигающимся угрозам. Так что в качестве альтернативного решения стоит рассматривать разработку новой конвенции под эгидой ООН. [42]

Таким образом, процесс регулирования противодействия виртуальной преступности с точки зрения права практически отсутствует. До настоящего момента времени законодательство почти нигде не закрепило и не раскрыло таких понятий как «киберпреступность», «киберпространство», «кибершпионаж», «кибертерроризм» и т. п. Наряду с этим не имеется четких критериев разграничения этих направлений преступности.

Осуществлять контроль данного направления и вести с ним борьбу в рамках отдельной державы сложно, можно даже сказать, что это невозможно. В связи с этим в целях осуществления борьбы с угрозой, которая с течением времени будет только нарастать, потребуется налаживание сотруднических связей на международном уровне. Наряду с этим появятся возможности для устранения противоправных деяний. [33,54]

2.3 Направления развития правовых норм для обеспечения информационной безопасности в РФ

На сегодняшний день безопасность с информационной точки зрения выступает в качестве одного из главных направлений обеспечения защищенности на национальном уровне. Стабильное функционирование источников информации, а также управленческих систем обеспечивает полную обороноспособность государства и способствует его активному развитию в экономическом и социальном разрезе. Наряду с этим происходит комплексная защита суверенитета.

Подвергнув детальному изучению состояние, в котором пребывает правовое обеспечение информационной безопасности РФ, а также проведя анализ нынешнего российского законодательства в рассматриваемой сфере, можно сделать определенные выводы.

В процессе выявления места информационной безопасности в рамках этой системы в работе была изучена так называемая «Стратегия национальной безопасности РФ до 2020 г.». В ней довелось обнаружить определенные недостатки.

В текстовой части этой Стратегии было закреплено понятие национальной безопасности, а также его определение. Стоит отметить, что все эти аспекты содержат логическую ошибку, связанную с тавтологией. Дело в том, что безопасность национального характера поясняется как состояние, в котором личность имеет определенную защищенность, то же самое касается общества, государства. Это значит, что угрозы внутреннего и внешнего характера им не страшны, а также происходит обеспечение прав и свобод, оптимального уровня жизни, суверенитета, целостности в социальном плане и устойчивого развития. Если говорить простыми словами, предмет, который определяется в рамках данного текста, делает это через самого себя.

В пояснении термина, который предложен в данном законодательном акте, наблюдается нарушение иерархической структуры ценностей, нуждающихся в обеспечении защиты. На первом месте находятся конституционные права со свободами, затем следует высокий уровень жизни и только после этого – целостность территориального характера, суверенитет.

Именно два последних аспекта являются наиболее ценными для государства. Связано это с тем, что данные свойства выступают в качестве базовых признаков и, конечно же, условий его существования. Если они не будут обеспечены, не возникнет и конституционных прав, свобод, достойного качества жизни граждан. Наряду с этим следует отметить, что и суверенитет, и территориальная целостность могут быть обеспечены в том случае, если у граждан отсутствуют правовые полномочия и свободы, закрепленные на конституционном уровне. [48]

На основании анализа всего, что было сказано ранее, стоит сделать вывод об однозначном нарушении структуры ценностей, которые нужно защищать, и существенном тавтологии. Причем все это присутствует не только в рамках определения национальной безопасности, но и в описании целей стратегического характера.

В п. 35 документа, который подвержен анализу, сказано, что в качестве стратегических целей, стоящих перед процессом обеспечения национальной безопасности, выступают такие моменты как защита норм конституционного строя РФ, правовых полномочий, свобод, интересов людей/граждан, а также социума в целом. Важную роль при этом играет охрана суверенитета, независимости и целостности в территориальном плане. Наряду с этим активно обеспечивается сохранение гражданского мира, стабильности в плане политики и социума.

По сути, национальная безопасность относится, как правило, к безопасности государства и социума. Она может находиться на любом уровне национальной безопасности. В связи с этим говорить о ней в плане

государства и общества нецелесообразно, иначе возникнет тавтология. Наряду с этим к основам конституционного строя на территории РФ можно отнести суверенитет, территориальную целостность. Так что рассматривать охрану независимости, целостности и суверенитета как стратегическую цель – значит повторять то, что уже было сказано.

Пониманию термина национальной безопасности как феномена обеспечения защищенности индивидуума, социума и государства от угроз внутреннего и внешнего характера соответствуют некоторые трактовки. Их полный перечень представлен в вышеописанном документе – «Стратегиии…». Особое внимание стоит уделить самим национальным интересам. Дело в том, что на территории Российской Федерации они зачастую представляют собой не что иное как комплекс потребностей страны в обеспечении устойчивого развития. Это означает лишь то, что национальные интересы державы – это по факту просто ее потребности в плане национальной безопасности.

Что касается термина «угрозы национальной безопасности», он традиционно представляют собой возможность нанесения ущерба правам, описанным в конституции, а также свободам во всех направлениях, достойному уровню жизни, целостности, суверенитету, развитию[2]. Конечно же, особое внимание уделяется обороне государства и его безопасности. Данное определение снова содержит тавтологию, ведь термины повторяются, особенно те, которые связаны с нарушением иерархии и ценностей общественного типа.

Автор придерживается позиции, которая была выражена во мнении проверенных экспертов. К ним, в первую очередь, относится доктор юридических наук и профессор МГУ по имени В. А. Томсинов. В своих многочисленных исследованиях он не раз отмечал, что истинный смысл понятие «национальная безопасность» получает в том случае, если под ним подразумеваются условия, которые обеспечивают защиту от угроз, важных для развития страны и интересов ее граждан. В рассматриваемой ситуации в

«Стратегии…» потребуется предоставление списка национальных интересов и базовых ценностей, которые и составляют базу цивилизации. [49]

Нормативные правовые акты, которые обеспечивают регулирование отношений в сфере права, формирующиеся в информационной области, пребывают в хаотичном состоянии и имеют тесное и непосредственное отношение к различным правовым отраслям. В многочисленных исследованиях показано, что зачастую нормы права просто-напросто дублируются, а иногда между ними и вовсе наблюдаются противоречия. Такие недостатки создают определенные препятствия для рационального толкования норм права и их применения. По этой причине нормы законодательства, связанные, в первую очередь, с информационной сферой, должны быть усовершенствованы и развиваться прогрессивно.

Многие исследователи отмечают, что решить данную проблему можно путем систематизации и кодификации законодательства. Объясняется данный феномен тем, что эти решения приведут к исключению субъективного рассмотрения законов. Наряду с этим с помощью кодификации можно решить несколько других важных задач:

- обеспечить единообразное регулирование информационной области, которое будет системным и на 100% обоснованным;
- приблизить его к международной практике, подстроив некоторые аспекты под мировой опыт;
- унифицировать нормы и требования, связанные с регулированием взаимоотношений в информационной сфере;
- исключить противоречия в законодательных нормах в целях регулирования сведений, выступающих в качестве объектов права;
- появление результативной правовой базы для формирования и практического применения информационных систем;
- возникновение правовых азов в целях реализации задач, поставленных перед государством, имеющих тесную и непосредствен-

ную взаимосвязь с построением и развитием на территории РФ информационного общества. [21,48]

Наряду с этим важную роль играет обеспечение входа государства в мировое пространство информационного характера. Стоит также отметить, что в течение нескольких последних лет в качестве главного направления развития политики РФ выступало обеспечение безопасности с информационной точки зрения. Наша страна на сегодняшний день пребывает в активном взаимодействии с партнерами в сфере обеспечения безопасности, включая такие сообщества как ООН, БРИКС, Шанхайская организация, нацеленная на сотрудничество.

Особого внимания в развитии законодательной базы в сфере информации заслуживает факт принятия в 2000 году Доктрины информационной безопасности РФ. Тем не менее, по факту это произошло 20 лет тому назад, и на сегодняшний день существует потребность в ее корректировке. Ведь данный документ не подразумевает учета нынешних угроз в виде войн, похищения личных данных, виртуального мошенничества. В связи с этим на сегодняшний день активно обсуждается возможность принятия новой редакции, в рамках которой будут учтены основные факторы, оказывающие влияние на безопасность.

Тем не менее, невзирая на то, что на сегодняшний день российское законодательство активно развивается, в сфере информации до сих пор наблюдается огромное количество пробелов. Формирование информационной безопасности станет доступным только в том случае, если принять во внимание основы международного сотрудничества аналогично системе комплексной безопасности, имеющей декларативный характер. в Российской Федерации не наблюдается ратификация международной конвенции о киберпреступности, которая была принята в 2001 году в городе Будапешт. В нынешнем законодательстве данная область не регулируется.

Ежегодно можно наблюдать усугубление ситуации с электронной преступностью. Но ввиду отсутствия адекватной нормативно-правовой базы,

а также практической составляющей противодействия невозможно решить данную проблему быстро и результативно. Поэтому сократить число киберпреступлений проблематично. Исследовав состояние данного аспекта на территории Российской Федерации и зарубежных стран, можно сделать вывод о том, что бороться с этим феноменом невозможно, по крайней мере, в самостоятельном порядке. Ведь он выходит за пределы проблемы национального характера и становится международным. По этой причине требуется разработка единого документа, который функционировал бы на международном уровне. В нем обязательным является закрепление понятийного аппарата, связанного с киберпространством, а также раскрытие сути и сущности некоторых понятий.

Итак, сделаем выводы по второй главе:

- важную роль также играет выявление аспектов, относящихся к информации и киберпреступности. Конечно же, внимания заслуживает закрепление норм ответственности и штрафных санкций за преступления, а также вероятность сотрудничества между странами по данному вопросу.
- выше были перечислены лишь базовые положения, которые требуют обязательного отражения в международной документации. Тем не менее, для их разработки, а также принятия верных решений требуется проведение научных исследований в отношении решения вопросов и проведения анализа всех законодательных норм.
- таким образом, киберпреступность в современном мире является серьезной проблемой, требующей незамедлительного и взвешенного решения.

3. Критическая информационная инфраструктура в РФ

3.1 Нюансы законодательной базы в сфере защиты критической информационной инфраструктуры РФ

Начало мероприятий, связанных с обеспечением защиты информационной инфраструктуры в государственных масштабах, произошло в момент подписания Указа, изданного Президентом РФ от 15 января 2013 г. под номером 31с. Документ посвящен формированию системы выявления, предотвращения и уничтожения последствий компьютерных атак на государственном уровне.

Впоследствии в июне месяце 2017 года произошло подписание ФЗ от 26 числа под номером 178-ФЗ. Акт посвящен организации безопасности критической информационной инфраструктуры (далее по тексту КИИ). Он стал действовать на законном уровне с 1 января 2018 года.

Следует отметить, что КИИ – это комплекс информационных систем, телекоммуникационных сетей, электросвязей, применяемых в рамках организации их взаимодействия. В качестве субъектов КИИ выступают фирмы, осуществляющие деятельность в отраслях, представляющих для государства стратегическую важность. Например, в медицине, науке, финансах, транспорте. А также в космическом освоении, добыче природных ресурсов, металлургии, энергетике и пр. Сюда же можно отнести организации, которые ответственны за взаимодействие всех систем и сетей КИИ.

Определение компьютерной атаки, в свою очередь, происходит в качестве целенаправленного и обязательно вредоносного влияния на конкретные объекты. Традиционно она нацелена на нарушение или вовсе прекращение их работы. Что касается компьютерного инцидента, он является фактом злодеяний и угрожает безопасности информации, подлежащей обработке со стороны объекта.

Наряду с этим внимания заслуживает тот факт, что для компаний, относящихся к сфере ТЭК, разработаны собственные нормы, прописанные в ФЗ№256 от 21 июля 2011 г. «О безопасности объектов топливно-энергетического комплекса». Все, что описано в этих законодательных актах, свидетельствует о необходимости гарантии безопасности информационных систем посредством создания защитных механизмов от неправомерного доступа, ликвидации, модификации, блокировки и прочих аналогичных деяний. Важную роль, конечно же, играет обеспечение функционирования подобных механизмов.

Организация ФСТЭК РФ, в свою очередь, была назначена силами федерального органа, относящегося к исполнительной власти, который имеет полномочия в сфере обеспечения безопасности инфраструктуры. На ФСБ Российской Федерации возлагались опции структуры, которая имела полномочия по обеспечению определенной работы. Например, по обнаружению, предотвращению и уничтожению последствий атак на ресурсы информации РФ (далее по тексту – ГосСОПКА).

Наряду с этим в рамках приказа ФСБ РФ, изданного в 2018 году, произошло создание Национального координационного центра компьютерных инцидентов (сокращенно аббревиатура выглядет как НКЦКИ). В компетенции данной организации – координация деятельности отдельных субъектов КИ, а также работа с силами, предназначенными для выявления и предотвращения, а также ликвидации последствий, связанных с компьютерными атаками. Эксперты, работающие в данной структуре, должны уметь реагировать на определенные инциденты и использовать техническую инфраструктуру в целях поддержания функционирования механизма ГосСОПКА.

Если давать пояснения на простом языке, структура НКЦКИ выступает в качестве государственной инстанции. Что касается системы ГосСОПКА, она представляет собой «SIEM» в рамках масштаба Российской Федерации. Работает все это по следующей схеме. Данные по индиденту, который

произошел в объеме в соответствии с положениями Приказа ФСБ №367, подлежат передаче со стороны субъекта КИИ в адрес субъекта ГосСОПКА. Происходит это в рамках периода времени до 24 часов с момента, когда он был обнаружен. При этом наблюдается выраженная тенденция перехода к отправке данных в автоматизированном режиме.

Впоследствии на законодательном уровне произошло подписание Постановления Правительства РФ от 8 февраля 2018 года под номером 127. Данный документ был посвящен утверждению Правил категорирования объектов КИИ, а также оформлению списка критериев, характеризующих значимость объектов. Речь идет о количественных параметрах в целях рационального выбора категории значимости. Она, в свою очередь, может быть низкой, средней или высокой, а также пребывает в зависимости от количественных значений важности объекта в рамках политики, экономики, социальной сферы.

Если рассматривать практический пример, стоит уделить внимание такой картине. Если компьютерный инцидент может спровоцировать причинение ущерба здоровью и жизни 500 граждан, объект получает первую категорию. Если есть риск отсутствия доступа транспортных услуг вследствие того, что произошло, для 2 тыс. – 1 млн. граждан, категория является третьей.

Таким образом, объекты КИИ нуждаются в категорировании. Делается это силами постоянно действующей внутренней комиссии, которая наряду с этим занимается документальным оформлением действий:

- определение конкретных объектов КИИ, обеспечивающих решение управленческих, производственных, технологических, финансовых вопросов;
- выявление критических явлений, если их нарушение или вовсе прекращение может стать причиной негативных последствий в рамках политики, экономики, социальной области;

- установление объектов КИИ, осуществляющих обработку данных в целях обеспечения протекания процессов, описанных выше, а также контроль этих действий;
- формирование модели, в которой фигурируют угрозы и нарушители, при этом комиссии стоит обратить внимание на худшие сценарии атак;
- анализ вероятных последствий с принятием во внимание взаимосвязей между объектами;
- присваивание каждому из них конкретной категории важности, вынесение мотивировочного решения о ее неприсвоении, подразумевающее составление соответствующего акта.

Итоги, связанные с категорированием, подлежат направлению в ФСТЭК РФ. В этой организации осуществляется проверка их правильности и корректности. Если какие-либо замечания отсутствуют, происходит внесение данных в соответствующий реестр. Стоит отметить, что на законодательном уровне предусмотрен регулярный и плановый пересмотр категорий.

3.2 ГосСОПКА

Если принимать во внимание документ, который был разработан ФСБ РФ от 24.12.2016 г. под номером 149/2/7-200, а именно – рекомендации методического характера, связанные с работой центров госсистемы выявления, предотвращения и уничтожения последствий компьютерных атак, можно отметить, что ключевые функции ГосСОПКА состоят в следующих аспектах:

- инвентаризация ресурсов, предоставляющих информацию;
- определение уязвимых мест информационных ресурсов;
- оценка угроз безопасности информационного характера;
- повышение квалификационного уровня персонала, занятого в рассматриваемой сфере, а также пользователей;
- выявление факта атак;

- анализ информации, посвященной событиям, связанным с безопасностью;
- регистрация различных инцидентов;
- своевременное реагирование на них;
- определение причин;
- оценка итогов устранения их последствий.

На сегодняшний день центры, относящиеся к системе ГосСОПКА, могут быть ведомственными и корпоративными. Первые структуры занимаются ведением лицензируемой деятельности, нацеленной на защиту информационных ресурсов в интересах госорганов. Корпоративные структуры, в свою очередь, занимаются ведением лицензируемой деятельности, связанной с их защитой. Наряду с этим в их компетенции находится предоставление услуг, связанных с предотвращением, обнаружением и ликвидацией последствий атак компьютерного характера.

Если сама система может утрированно получать название «SIEM» в рамках масштабов всего государства, то центры ГосСОПКА, в свою очередь, корректно ставить в сравнение со структурами мониторинга информационной безопасности.

Таким образом, говоря простыми словами, субъекты КИИ, имеющие отношение к структурам государственной власти, согласно текущим нормам и требованиям законодательства, должны подключаться к соответствующим ведомственным Центрам, в частности – ГосСОПКА. У субъектов, которые не выступают в качестве государственных структур, имеется возможность осуществления самостоятельного подключения к системе, а также создания собственного центра корпорации или подключения к существующему центру, оказывающему подобные услуги.

В рамках самостоятельной активации данного центра от субъекта требуется решение следующих задач:

- формирование собственного центра, осуществляющего мониторинг безопасности с принятием во внимание требований нормативной документации, созданной ФСБ РФ;
- внедрение прогрессивных технических решений, пребывающих в соответствии с методическими рекомендациями, нацеленными на создание центров госсистемы для выявления, предотвращения и уничтожения последствий, связанных с компьютерными атаками на ресурсы информации РФ;
- практическое внедрение и поддержка технических средств, а также решений, которые пребывают в соответствии с требованиями к лицензиату ФСТЭК РФ для ведения деятельности, связанной с мониторингом информационной безопасности;
- получение лицензионного разрешения на осуществление работы, связанной с обеспечением технической защиты конфиденциальной информации в рамках перечня осуществляемых работ и услуг;
- обретение лицензии со стороны ФСБ РФ на работу по разработке, производству и последующему распространению криптографических инструментов;
- взаимодействие с ГосСОПКА, в процессе осуществления обмена в сфере выявления, предотвращения и уничтожения последствий атак;
- вовлечение в этот процесс сотрудников и их последующее удержание, речь идет о специалистах, работающих в Центре мониторинга ИБ;
- разработка сценариев атак и мониторинга, проведение его актуализации на постоянной основе;
- анализ произошедших событий и инцидентов, формирование отчетной документации.

Если принимать во внимание практические нюансы, активация внешнего центра ГосСОПКА, оказывающего соответствующие услуги, способствует передаче львиной доли задач, описанных ранее, специализированной структуре. Все, что нужно будет сделать заказчику – только активировать источники событий, соединив их с коммерческим центром, а также согласовать формат этого взаимодействия и оговорить детали регламента. Наряду с этим он обязуется предоставлять своевременное уведомление об изменениях, которые произошли в инфраструктуре.

Наряду с этим использование услуг внешнего центра подразумевает несение исполнителем рисков, вызванных несоответствием российскому законодательству. В частности, в сфере ведения незаконного бизнеса, согласно ст. 171 УК РФ.

3.3 АСУТП

Особого внимания заслуживают принципы, связанные с защитой автоматизированных управленческих систем на производстве. В рамках приказа ФСТЭК РФ от 14.03.2014 г. под номером 31 описан порядок утверждения требований, предъявляемых к защите данных в рамках автоматизированных систем управления производственными процессами на объектах критической важности. Считается, что они таят в себе потенциальную опасность для жизни и здоровья человека и природы. Документ представлен в редакции Приказа ФСТЭК РФ от 09.08.2018 г. №138. В нем, в свою очередь, установлен набор требований в плане обеспечения безопасности рассматриваемых систем.

Несмотря на то, что эти направления защиты будто бы дублируются, на сегодняшний день государственные регуляторы считают, что если объект является значимым, т. е. имеет конкретную присвоенную категорию, то принято использовать Приказ ФСТЭК РФ от 25.12.2017 г. №239. Если же

какая-либо степень значимости отсутствует, на базе решения субъекта можно использовать приказ №31 или №239.

Согласно документу под номером 31 в качестве объектов защиты АСУТП выступают информационные сведения, характеризующие параметры объекта, находящегося под управлением, и его состояние. Важную роль играют сопутствующие средства техники. В данном документе отмечается тот факт, что все принимаемые меры, нацеленные на защиту АСУТП, должны обеспечивать доступность сведений и их целостность. На втором же месте находится обеспечение конфиденциальности информации. Наряду с этим во внимание принимается тот факт, что меры нужно гармонизировать с мерами, связанными с обеспечением прочих видов безопасности, например, промышленного, экологического, пожарного характера. Наряду с этим они не должны оказывать отрицательного воздействия на штатный режим работу АСУТП. Особые требования предъявляются по отношению к СЗИ.

В документации содержится детальная информация об организационных шагах, связанных с защитой данных. Речь идет о таких элементах как формирование набора требований, разработка системы защиты и ее внедрение, обеспечение ЗИ в процессе эксплуатирования систем. Именно на стадии, на которой происходит формирование требований, организуется важнейшая работа, связанная с классификацией АСУТП. Дело в том, что в итоге система получает один из трех классов защищенности, и каждый из них определяется в соответствии с уровнем значимости информации, которая обрабатывается, т. е. со степенью вероятного ущерба, причиненного вследствие нарушения свойств доступности, безопасности, целостности, конфиденциальности. Что касается степени ущерба, она может принимать высокое, среднее или низкое значение.

Наряду с классификацией АСУТП на стадии формирования базового набора требований происходит определение угрозы безопасности посредством формирования конкретной модели. На данном этапе происходит:

– выявление источников угроз,
– оценка возможностей, которые есть у нарушителей,
– анализ степени уязвимости применяемых механизмов,
– выявление вариантов реализации угроз и последствий.

Во внимание в обязательном порядке принимаются нормы БДУ ФСТЭК. Важную роль также играет набор мер защиты, которые должны способствовать нейтрализации действий нарушителей, имеющих высокий потенциал (для АСУТП 1). Что касается АСУТП 2, речь идет о нарушителях с потенциалом «ниже среднего», АСУТП 3 – с низким потенциалом.

Наряду с этим рассматриваемый приказ №31 предлагает алгоритм, в соответствии с которым осуществляется выбор и дальнейшая реализация мер, нацеленных на обеспечение безопасности. Эта норма соприкасается с приказом №21 от ФСТЭК и №17 (ГИС).

На начальном этапе выбирается стандартный набор мер на базе списка, а после этого происходит адаптация, которая подразумевает отсутствие принятия во внимание нерелевантных мер в соответствии с особенностями ИС и технологий. После этого происходит уточнение этого перечня, чтобы появилась возможность нейтрализации актуальных угроз. Впоследствии происходит их дополнение. Стоит отметить, что в Приказе №31 отмечается высокая степень важности процессе непрерывности технологии. Это способствует использованию компенсирующих мер защиты.

Также стоит отметить, что Приказ №31 содержит комплекс групп мер, нацеленных на обеспечение должного уровня безопасности. Именно их нужно применять в обязательном порядке в соответствии с необходимым классом защищенности:

– идентификация;
– аутентификация;
– управление доступом и соответствующие системы;
– ограничения в рамках программной среды;

– обеспечение защиты носителей информации (машинного характера);
– аудит в плане безопасности;
– защищенность против вирусов;
– профилактика несанкционированных вторжений;
– гарантия целостного функционирования системы;
– профилактика поломок средств техники;
– сохранность системы информации;
– реакция на компьютерные инциденты;
– конфигурация и управление ею;
– регулирование обновлений программного обеспечения;
– планирование мер, связанных с обеспечением высокого уровня безопасности;
– проведение мероприятий в ситуациях внештатного характера;
– комплексное обучение персонала и предоставление ему нужной информации.

Наряду с этим в документе отображается тот факт, что в случае внедрения технических средств защиты данных во внимание стоит принимать, в первую очередь, штатные функции систем, применяемых в рамках АСУТП. Только после этого можно обратить внимание на СЗИ, к которым предъявляется конкретный набор требований (подробно они описаны в п. 24 Приказа №31).

3.4 Обеспечение безопасности важной КИ

Теперь стоит рассмотреть один из наиболее значимых подзаконных актов, посвященных обеспечению защиты объектов КИ. Речь идет о Приказе №239 от 25.12.2017 г., изданном ФСТЭК России. В нем изложен набор норм, которые стоит применять по отношению к системам информации,

автоматизации, управления, телекоммуникации. Критерии, на основании которых объект может считаться значимым, рассматриваются в рамках Постановления №127, о нем речь велась ранее. Следование нормам приказа подразумевает, что отнесение объектов к конкретным категориям уже происходило по ПП-127. Наряду со значимыми объектами нормы данной документации могут использоваться по отношению к незначимым элементам. То же самое касается пунктов Приказа №31. В документе №239 отдельно указывается тот факт, что все объекты, связанные с обработкой ПДн, попадают под соответствующие нормы защиты.

В Приказе №239 сказано, что разработка этих мероприятий в обязательном порядке должна подразумевать анализ и оценку угроз безопасности, а также разработку оптимальных моделей. Что касается мер защиты, которые внедряются на практике, они не должны плохо воздействовать на рабочие процессы. Как и в соответствии с нормами Приказа №31 анализ угроз должен подразумевать определение их источников и оценивание возможностей, стоящих перед нарушителями. Важную роль играет анализ степени уязвимости применяемых систем и выявление вариантов реализации различных угроз.

В приказе №239 речь ведется о том, что при разработке нового программного обеспечения в качестве элемента подсистемы безопасности стоит учитывать нормы безопасной разработки. В рамках применения СЗИ во внимание традиционно принимается штатный функционал. А в случае реагирования на инциденты важную роль играет предоставление информации о них по адресу ГосСОПКА.

Перечень мероприятий организационного и технического характера, которые предусмотрены в рамках положений рассматриваемого приказа, имеются пункты по аналогии с Приказом №31. Речь идет о следующих аспектах:

- идентификация, аутентификация;
- управление доступностью;

- наложение ограничений на программную среду;
- обеспечение защиты машинных носителей данных;
- аудит в плане безопасности;
- защита против вирусов и вторжений;
- предоставление целостной информации;
- сохранность средств техники;
- информационной системы и ее отдельных компонентов;
- составление плана мероприятий, нацеленных на обеспечение безопасности;
- управление конфигурациями, обновлениями программного обеспечения;
- реагирование на ситуации, связанные с информационной безопасностью;
- предусмотрение действий во внерядовых ситуациях.

Порядок, в котором осуществляется выбор, описанный в тексте Приказа №239, имеет сходство с нормами приказа №31, а также 17 и 21. Исключением является тот факт, что данный этап имеет отношение к шагу по адаптации стандартного набора. То есть сначала выбирается базовый комплекс, а после этого происходит его адаптация, включение в него прочих мер, указанных в иных документах. Наряду с этим в тексте указано, что если на объекте уже применяются какие-то меры безопасности, дополнительных мероприятий можно не проводить.

Объект КИ должен работать непрерывно, если негативное воздействие на него отсутствует. Он может использовать более подходящие меры компенсации вместо базового набора. Однако требуется использование прогрессивного подхода в ИТ-сфере. Предъявление требований также происходит к СЗИ. Можно использовать средства, которые прошли оценку на предмет соответствия нормам безопасности. Проведение испытания

происходит самостоятельно или с участием лицензиатов ФСТЭК РФ. Если говорить об использовании СЗИ с сертификатом, то требования таковы:

- на объектах, относящихся к первой категории значимости, стоит использовать СЗИ 4-го класса защиты;

- если они имеют отношение ко второй категории – от 5-го класса;

- если к 3-й – от 6-го класса.

Если вести речь о значимых объектах, вне зависимости от категорий на них применяются СВТ 5-го класса.

Стоит также отметить, что в рамках Приказа №239 содержится комплекс требований к уровням доверия СЗИ. Их определение происходит на основании Приказа №131 от 30.07.2018 г. В документе сказано, что для объектов 1-й категории используются СЗИ с 4-м или более высоким УД, второй – с 5-м, третьей – с 6-м. Важную роль играет тот факт, что пункты, связанные с уровнями доверия, были введены в 2019 году, марте месяце, т. е. уже после того как произошел выпуск изначальной версии Приказа.

В документе также подчеркивается, что на объектах, относящихся к 1-й категории значимости, в роли маршрутизаторов используются устройства, которые прошли сертификацию на предмет соответствия нормам безопасности. Если это невозможно, оценка функций безопасности происходит во время приемки или непосредственно испытательных мероприятий.

На основании всего, что было изложено выше, можно сделать следующий вывод: приказ №239 имеет сходство с другими документами ФСТЭК в плане структуры, тем не менее, он предполагает некоторые новации. Речь идет о соответствии требованиям уровня доверия, упоминании санкционных рисков, повышенном внимании вопросам безопасности и т. д. Данный документ играет ключевую роль в процессе выполнения требований, связанных с защитой объектов КИИ.

3.5 Ответственность за нарушение законодательства в сфере КИИ

Она прописана в ст. 274.1 УК РФ. Данное положение было внедрено в рамках ФЗ№194 от 26 июля 2017 года. Оно действует с 1 января 2018 г. Согласно положениям этой статьи максимально серьезному наказанию подвержены следующие деяния:

- несанкционированный доступ к информации и причинение вреда;
- игнорирование правил эксплуатирования средств, предназначенных для хранения, обработки, передачи данных;
- совершение перечисленных действий группой лиц на основании заблаговременного сговора;
- наличие тяжких последствий в виде ущерба на 1 млн. р. и более (в данном случае назначается лишение свободы до 10 лет).

Справедливости ради стоит отметить, что данная статья действует по отношению к значимым и незначимым объектам КИИ. Рассматриваемая норма также не учитывает категорию значимости. Что касается размера причиненного вреда, он выступает в качестве оценочного признака и измеряется в судебном порядке. В качестве «прародителя» этой нормы выступает ст. 274, которая сегодня подразумевает ограниченное применение.

Наряду с указанной уголовной ответственностью субъектам назначаются наказания административного характера. На сегодняшний день в КОАП РФ проходят некоторые изменения, они предполагают внедрение двух новых статей:

- 13.12.1 «Несоблюдение требований в сфере обеспечения безопасности КИИ…»;
- 19.7.15 «Отсутствие предоставления сведений, предусмотренных законом, в плане обеспечения безопасности КИИ…».

3.6 Перечень документов, регламентирующих работу КИИ

Наряду с нормативными актами, которые были рассмотрены ранее, на сегодняшний день достаточно широко используются следующие документы.

1) Указ Президента РФ от 15 января 2013 г. N 31с "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации". Именно данный нормативно-правовой акт стал отправной точкой для создания ГосСОПКА и НКЦКИ.

2) Указ Президента РФ от 22 декабря 2017 г. №620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Данный документ определил перечень задач, решаемых организацией ГосСОПКА, и наделил структуру ФСБ РФ новыми правами в плане обеспечения защиты КИИ.

3) Концепция госсистемы обнаружения, а также предотвращения и уничтожения последствий компьютерных атак. Утверждение – в рамках Приказа Президента РФ от 12 декабря 2014 г. №1274.

4) Положение, посвященное лицензированию деятельности, связанной с технической защитой конфиденциальной информации. Оно утверждено в рамках Постановления Правительства РФ №79 от 3 февраля 2012 г.

5) Постановление Правительства РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Посредством данного документа регламентируется контроль субъектов со стороны ФСТЭК РФ за счет проведения проверок, согласно ФЗ№187 и подзаконных нормативно-правовых актов.

Наряду с этим действует еще несколько документов, которые регламентируют алгоритм организации проверок со стороны Роскомнадзора.

- Приказ ФСТЭК РФ от 06.12.2017 № 227 "Об утверждении порядка ведения реестра значимых объектов критической информационной инфраструктуры российской федерации"
- Приказ №235 от 21 декабря 2017 г. Здесь составлен их перечень в плане безопасности значимых объектов.
- Приказ №236 от 22 декабря 2017 г., в котором говорится о порядке утверждения формы направления данных об итогах присвоения объекты конкретной категории.
- Приказ №229 от 11 декабря 2017 г., где описывается схема утверждения формы акта проверки, формируемого по результатам госконтроля.
- Приказ, изданный ФСБ РФ, под номером 366 от 27 июля 2018 г., в документе ведется речь о национальном центре координации по инцидентам с компьютерами.
- Приказ ФСБ РФ №367 от 24 июля 2018 г., в котором ведется речь об утверждении списка данных, представляемых в госсистему выявления, предотвращения и уничтожения последствий атак. Также здесь описывается порядок представления данных. В документе сообщается о том, что информация, связанная с произошедшим инцидентом, должна обязательно передаваться со стороны субъекта КИИ в адрес системы ГосСОПКА. Происходить это должно на протяжении 24 часов с момента обнаружения инцидента.
- Приказ №368 от 24.07.2018 г. «Об утверждении порядка, в котором происходит обмен информацией между различными субъектами, находящимися в России и за рубежом…». В данном документе содержится регламент порядка, в котором осуществляется обмен информацией, причем в большей степени он осуществляется посредством НКЦКИ.
- Приказ ФСБ РФ от 6 мая 2019 г. под номером 196 «Об утверждении требований к средствам для выявления, предотвращения и ликвидации…». В данном документе подробно описан набор требований к опциям этих средств и особенностям поиска атак на объектах.

– Приказ ФСБ РФ №281 от 19.06.2019 г. «Об утверждении порядка, связанного с техническими условиями установки и эксплуатирования средств…». В данном случае исключением являются средства, применяемые в целях поиска признаков атак в рамках сетей электросвязи. В документе речь ведется о порядке взаимодействия между субъектами в плане установки «сенсоров» ГосСОПКА на определенных объектах.
– Приказ ФСБ РФ №282 от 19 июня 2019 г. «Об утверждении порядка, в котором происходит информирование контролирующих структур об инцидентах…». В данном законе содержится указание на обязательство субъектов КИИ, связанное с информированием ФСБ РФ через НКЦКИ о возникающих ситуациях, которые находятся в зоне ответственности конкретного субъекта. Наряду с этим, если он находится в подчинении норм ЦБ РФ, данные направляются в ФинЦЕРТ Банка РФ.

При всем этом стоит отметить ограниченные временные рамки: данные передаются на протяжении трех часов с момента обнаружения. Если объект является незначимым, это должно произойти на протяжении суток. Наряду с этим итоги мероприятий, связанных с реагированием на различные инциденты, должны быть переданы в течение двух суток с момента их завершения. В этом документе относительно недавно появились новшества: таким образом, в п. 10 речь ведется о том, что хотя бы раз в год требуется проведение тренировок, связанных с отработкой мероприятий по реагированию на компьютерные инциденты.

Наряду с документами, указанными выше, Федеральная служба безопасности Российской Федерации также осуществила выпуск комплекса прочих актов, посвященных вопросам защиты КИИ. Тем не менее, в настоящее время они являются недоступными для ознакомления в свободном порядке. Речь идет о следующих актах:

– методические рекомендации, разработанные ФСБ РФ для создания центров госсистемы выявления, предотвращения и уничтожения последствий компьютерных атак;
– для обнаружения атак и дальнейших действий, связанных с нейтрализацией последствий;

- для установления причин, а также устранения негативных явлений, которые повлекли за собой компьютерные инциденты;
- для проведения мероприятий, посвященных оценке степени защищенности от атак;
- базовые требования, предъявляемые к отдельным подразделениям, а также должностным лицам субъектов ГосСОПКА;
- регламентирующие положения по взаимодействиям между подразделениями ФСБ РФ и субъектами ГосСОПКА в процессе реализации обмена информацией в рассматриваемой сфере.

3.7 Категорирование объекта КИИ на примере здравоохранения

В целях категорирования объекта критической информационной инфраструктуры организации необходимо издать приказ о создании комиссии по категорированию объектов КИИ (Приложение Г), разработать положение о данной комиссии (приложение Д), после чего комиссии формирует ЗАКЛЮЧЕНИЕ о формировании перечня объектов критической информационной инфраструктуры, подлежащих категорированию, данное заключении согласовывается с вышестоящим органом здравоохранения региона, после чего данные отправляются во ФСТЭК Российской Федерации (приложение Е). С этого времени отсчитывается срок 9 месяцев в течении которого необходимо отправить во ФСТЭК данные о присвоении категории (приложение Ж)

Итак, сделаем выводы по третьей главе:

- закон о КИИ РФ первый крупный шаг в обеспечении информационной безопасности критически важных объектов.
- ответственность за инцинденты в КИИ очень высока, как для нарушителей безопасности, так и для самого владельца КИИ.

Заключение

По причине возрастания роли информации в 21 веке, это столетие является информационным. В рамках глобальной информатизации социума основной задачей считается правовое регулирование безопасности.

Ключевая цель этой работы состояла в проведении анализа правовой системы безопасности на территории РФ, а также в моделировании рациональных форм развития. Согласно этой цели было выделено несколько базовых задач, которые автор работы смог решить.

Анализ термина «информационная безопасность», который закреплен в действующих нормах российского законодательства, а также его трактовок, применяемых в процессе проведения научных исследований, способствует формированию общего вывода. Он, в первую очередь, связан с тем, что информационная безопасность выступает в качестве одного из основополагающих элементов нацбезопасности государства, поскольку рассматривается как состояние защищенности национальных интересов от угроз внутреннего и внешнего типа.

Информационную безопасность не составит труда определить перечнем интересов, которые имеет личность, а также социум и государство. Она выступает в качестве совокупности всей информационной инфраструктуры, субъектов, которые осуществляют сбор, создание и последующее распространение информации, а также системы, обеспечивающей регулирование социальных отношений.

На первый взгляд может показаться, что реальное протекание процессов, связанных с информацизацией, подразумевает необходимость постоянного совершенствования законодательной базы. Это неудивительно, ведь она является важнейшей общего правового механизма, нацеленного на поддержание законности в стране и ее правопорядка. Такой подход поспособствует созданию единой концепции безопасности на территории РФ.

На сегодняшний день в качестве базы правового регулирования данной сферы выступает определенный комплекс нормативно-правовых актов. К ним можно отнести следующие документы:

– Доктрина безопасности в информационном плане;
– Стратегия по развитию информационного общества;
– ФЗ№149;
– ФЗ №187.

В этой работе был определен ряд неточностей, которые были допущены законодателем в ходе принятия актов, обеспечивающих регулирование национальной безопасности. В связи с этим в данной работе проведен анализ понятия национальной безопасности, а также установлен тот факт, что в «Стратегии» несколько раз наблюдается тавтология, что создает препятствия для рационального толкования термина.

В работе предлагается внесение изменений в п. 6 «Стратегии», которая была разработана до 2020 года. Наряду с этим предлагается изложить понятие «национальная безопасность» так: «это комплекс условий, который обеспечивают защиту от угроз внутреннего и внешнего типа, имеющих значение в существовании и развитии государства и его интересов».

В целях обеспечения информационной безопасности с точки зрения права на территории Российской Федерации принимались соответствующие меры. Особенно те, которые были утверждены в 2000 году. К ним относятся Доктрины, которые являлись основным шагом на пути к законодательному регулированию сферы информации. По причине непрерывности и необратимости научно-технического прогресса этот акт стал устаревшим, поскольку с момента его официального принятия успело пройти более 20 лет. По этой причине появились новые угрозы в информационном плане. Например, войны, хищение личных данных, киберпреступность и пр. В связи с этим возникает необходимость внесения корректировок в некоторые законодательные акты.

Информатизация успела коснуться абсолютно всех сфер жизнедеятельности общества и государства. В первую очередь, это касается политики, экономики, социальной среды. Принимается во внимание важность информатизации в процессе создания и развития взаимоотношений между сторонами. А также вхождение в информационно-электронное пространство. На основании этого можно сделать вывод о необходимости совершенствования защитного механизма.

Наряду с этим обеспечение безопасности происходит за счет постоянного поддержания баланса между техническими средствами и рациональным механизмом правового обеспечения. В связи с этим данная проблема становится актуальной и комплексной. Она традиционно включает в себя ресурсы всей экономики, науки, идеологии и пр.

На сегодняшний день не составит труда выделить несколько категорий опасностей информационно-технического типа.

- Возникновение и последующее развитие информационного оружия, обладающего способностью эффективного влияния на психоэмоциональное состояние людей. Все это, в свою очередь, приводит к зависимости от сети Интернет и так называемым «информационным болезням». На практике нередко встречается виртуализм, а именно – нацеленность конкретной личности на уход от реальных жизненных событий в мир компьютерных технологий, который формируется за счет информационных средств. Важную роль в данном случае играет «авитализм», а именно – потеря глубинных установок личности. По этой причине применение прогрессивных методик информационного влияния приводит к управляемости общества для достижения определенных целей;
- Контроль жизни индивидуума и социума с применением электронных технических приспособлений. Причем происходит это, как правило, без уведомления граждан;
- Возможность применения современными технологиями для решения определенных политических задач;

– Возникновение нового класса преступлений социального характера, в основе которых – пользование современными технологиями.

Совершенствование информационной сферы приводит к появлению прогрессивных правонарушений. Чаще всего они являются сложными и базируются на использовании высоких технологий. В первую очередь, к ним можно отнести киберпреступность. Она вторгается в технологическую сферу безопасности, что выступает в качестве главной составной части данного раздела.

В обеспечении информационной безопасности существует немалое количество проблем, особенно на территории Российской Федерации. То же самое касается обеспечения неприкосновенности личной жизни и сохранности прав на получение доступа к информации, ресурсам и сетям. Перед властями стоит основная задача, связанная с борьбой с преступностью (кибермошенничеством). Наряду с этим существует множество других проблем, которые требуют моментального решения и комплексного анализа. Все мероприятия проводятся субъектами РФ в соответствии с нормами действующего законодательства и никак не противоречат им.

Список используемой литературы и источников

Нормативные правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от № 11-ФКЗ) // Собрание законодательства Российской Федерации. - 04.08.2014. - № 31. - Ст. 4398.
2. Гражданский кодекс Российской Федерации (часть вторая): федеральный закон от 26.01.1996 № 14-ФЗ: офиц. текст по состоянию на 06.04.2015, с изм. от 07.04.2015 // Собрание законодательства Российской Федерации. - 29.01.1996. - № 5. - Ст. 410.
3. Уголовный кодекс Российской Федерации: федеральный закон от 13.06.1996 № 63-ФЗ: офиц. текст по состоянию на 30.03.2015, с изм. от // Собрание законодательства Российской Федерации. - 17.06.1996. - № 25. - Ст. 2954.
4. О Федеральной службе безопасности: федеральный закон от 03.04.1995 № 40-ФЗ: офиц. текст по состоянию на 22.12.2014 // Российская газета. - № 72. - 12.04.1995.
5. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ: офиц. текст по состоянию на 21.07.2014 // Российская газета. - № 165. - 29.07.2006.
6. О безопасности: федеральный закон от 28.12.2010 № 390-ФЗ // Российская газета. - № 295. - 29.12.2010.
7. Доктрина информационной безопасности Российской Федерации: утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895 // Российская газета. - № 187. - 28.09.2000.
8. Стратегия развития информационного общества в Российской Федерации: утверждена Президентом Российской Федерации 07.02.2008 № Пр-212 // Российская газета. - № 34. - 16.02.2008.
9. О мерах по обеспечению информационной безопасности Российской Феде-

рации при использовании информационно-телекоммуникационных сетей международного информационного обмена: указ Президента Российской Федерации от 17.03.2008 № 351: офиц. текст по состоянию на 25.07.2014 // Собрание законодательства Российской Федерации. - 24.03.2008. - № 12. - Ст. 1110.

10. О Стратегии национальной безопасности Российской Федерации до 2020 года: указ Президента Российской Федерации от 12.05.2009 № 537: офиц. текст по состоянию на 01.07.2014 // Российская газета. - № 88. - 19.05.2009.

11. Об утверждении государственной программы Российской Федерации «Информационное общество (2011 - 2020 годы)»: постановление Правительства Российской Федерации от 15.04.2014 № 313: офиц. текст по состоянию на 21.02.2015 // Собрание законодательства Российской Федерации. - 05.05.2014. - № 18 (часть II). - Ст. 2159.

- Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года: распоряжение Правительства Российской Федерации от 01.11.2013 № 2036-р // Собрание законодательства Российской Федерации. - 18.11.2013. № 46. - Ст. 5954.

12. Об утверждении Концепции региональной информатизации: распоряжение Правительства Российской Федерации от 29.12.2014 № 2769-р // Собрание законодательства Российской Федерации. - 12.01.2015. - № 2. - Ст. 544. Международные акты

13. Всеобщая декларация прав человека: принята Генеральной Ассамблеей ООН 10.12.1948 // Российская газета. - № 67. - 05.04.1995.

14. Окинавская хартия глобального информационного общества: принята на о. Окинава 22.07.2000 // Дипломатический вестник. - № 8. - 2000.

15. Указ Президента РФ от 15 января 2013 г. N 31с "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации"

16. Указ Президента РФ от 22 декабря 2017 г. №620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

17. *Демъянец М. В.* Предпринимательская деятельность в сети Интернет: Монография / М. В. Демьянец, В. М. Елин, А. К. Жарова. - М. : ЮРКОМПАНИ. - 2014. - 440 с.

18. *Жеребин В. М.* Социальные аспекты информатизации: Монография / В. М. Жеребин. - М. : Экономическое образование. - 2013. - 212 с.

19. *Жигулин Г. П.* Организационное и правовое обеспечение информационной безопасности / Г. П. Жигулин. - СПб. : СПбНИУИТМО. - 2014. - 173 с.

20. *Куняев Н. Н.* Правовое обеспечение национальных интересов Российской Федерации в информационной сфере / Н. Н. Куняев. - М. : Логос.
2010. - 348 с.

21. *Санжаревский И. И.* Политическая наука: словарь-справочник. Изд. 6-е, испр. и доп. / И. И. Санжаревский. - Тамбов. - 2014. - 750 с.

22. *Снетков В. Н.* Власть в обществе и информационная политика /
В. Н. Снетков, А. В. Пономаренко. - СПб. : Изд-во СПбГПУ. - 2001. - 247 с.

23. *Терещенко Л. К.* Модернизация информационных отношений и информационного законодательства: Монография / Л. К. Терещенко. - М. : ИНФРА-М. - 2013. - 227 с.

24. *Ушаков Д. Н.* Толковый словарь современного русского языка / Д. Н. Ушаков. - М. : Аделант. - 2013. - 800 с.

25. *Вербицкая Т.* Суды о национальной безопасности / Т. Вербицкая // ЭЖ-Юрист. - 2014. - № 13. - С. 1-6.

26. *Емелькина И. В.* Основные характеристики российского менталитета в условиях информационного общества / И. В. Емелькина // Информационное право. - 2011. - № 1. - С. 27-29.

27. *Кардашова И. Б.* О проблемах исследования обеспечения национальной безопасности / И. Б. Кардашова // Административное право и процесс. - 2014. - № 5. - С. 29-32.

28. *Карягина А. В.* История информационной правовой политики и безопасности в Российской Федерации: доктринальный и стратегический подходы / А. В. Карягина // История государства и права. - 2012. - № 8. - С. 39-41.

29. *Козориз Н. Л.* Информационная безопасность в системе противодействия опасности / Н. Л. Козориз // Информационное право. - 2013. - № 1. - С. 28-31.

30. *Куракин А. В.* Информационная безопасность в системе государственной службы / А. В. Куракин, Г. Н. Кулешов, П. В. Несмелов // Административное и муниципальное право. - 2013. - № 2. - С. 172-176.

31. *Мигачев Ю. И.* Правовые основы национальной безопасности (административные и информационные аспекты) / Ю. И. Мигачев, Н. А. Молчанов // Административное право и процесс. - 2014. - № 1. - С. 46-49.

32. *Михайлёнок О. М.* Политические аспекты информационной безопасности личности / О. М. Михайлёнок // Власть. - 2010. - № 12. - С. 64-70.

33. *Номоконов В. А.* Киберпреступность как новая криминальная угроза / В. А. Номоконов, Т. Л. Тропина // Криминология: вчера, сегодня, завтра. - 2012. - № 24. - С. 45-55.

34. *Попов В. В.* Информация как фактор воздействия на политическую жизнь общества (социокультурный аспект) / В. В. Попов // Вопросы безопасности. - 2014. - № 6. - С. 68-97.

35. *Смирнов А. А.* К вопросу о понятии, объекте и содержании информационно-психологической безопасности / А. А. Смирнов // Административное право и процесс. - 2013. - № 1. - С. 34-39.

36. *Снетков В. Н.* Обеспечение информационной безопасности в условиях гражданского общества / В. Н. Снетков // Проблемы права в современной России : сборник статей международной межвузовской научнопрактической конференции. - СПб. : Изд-во Политехн. ун-та. - 2012. - С. 198-202.

37. *Соколова С. Н.* Информационное право и государственное регулирование информационной безопасности / С. Н. Соколова, Ю. М. Сенив // Информационное право. - 2013. - № 2. - С. 3-7.

38. *Холопова Е. Н.* Информационная безопасность пограничных органов на современном этапе: понятие, структура / Е. Н. Холопова, А. С. Бойцов // Информационное право. - 2014 - № 5. - С. 4-9.

39. *Цибуля А. Н.* К вопросу о состоянии информационной безопасности государ-

ства в условиях современных вызовов и угроз / А. Н. Цибуля, В. А. Гордин // Военно-юридический журнал. - 2014. - № 3. - С. 20-24.

40. *Ческидов М. А.* Влияние развития информационной экономики на экономическую безопасность государства / М. А. Ческидов // Вестник Саратовского государственного социально-экономического университета. - 2013. - № 3 (47). - С. 28-

41. Информационно-аналитическое агентство Content-Review.com // URL: http://www.content-review.com/articles/30093/ (дата обращения 30.03.2019).

42. *Колокольцев В. А.* 100-летие совместной борьбы с транснациональной преступностью / В. А. Колокольцев // 83-я сессия Генеральной Ассамблеи Интерпола. - URL: https://mvd.ru/speech/item/ 2782703/ (дата обращения 06.04.2019).

43. *Кузьмин А. С.* Безопасность информационного пространства в условиях нарастающих киберугроз / А. С. Кузьмин // XVI Национальный форум информационной безопасности «Инфофорум-2014». - URL: http://2014.infoforum.ru (дата обращения 02.04.2019).

44. *Мошков А. Н.* Устойчивость и безопасность российского сегмента сети Интернет / А. Н. Мошков // XVII Национальный форум информационной безопасности «Инфофорум-2015». - URL: http://2015.infoforum.ru (дата обращения 05.04.2019).

45. Официальный сайт Министерства внутренних дел Российской Федерации: Управление «К» МВД России // URL: https://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Publikacii_i_vistuplenija/item/1951798/ (дата обращения 02.04.2019).

46. Официальный сайт Министерства внутренних дел Российской Федерации // URL: https://mvd.ru (дата обращения 30.03.2019).

47. Официальный сайт Совета Безопасности Российской Федерации // URL: http://www.scrf.gov.ru/news/19/874.html (дата обращения 05.04.2019).

48. *Томсинов В. А.* Критические заметки о «Стратегии национальной безопасности Российской Федерации до 2020 года» / В. А. Томсинов // URL: http://tomsinov.com/russia_contemp/strategia_nacionalnoi_bezopasnosti.pdf (дата обращения 06.04.2019).

49. Nye JS, Owens W.Jr. America's Information Edge: the Nature of Power // Electronic Journals of the US Information Agency. - 1996. - Vol. 1, №12. - Usinfo.state.gov/joumals/itigic/0996/ijge/gjcom6.htm/ - (дата обращения 16.02.2019)

50. RAND / MR-1033-OSD "The Emergency of Noopolitik: Toward an American Informational Strategy". - 1999. (дата обращения 16.02.2019)

51. The First amendment // Legal Information Institute. URL: http://www.law.cornell.edu/anncon/html/amdt1afrag1_user.html#amdt1a_hd4 (дата обращения: 09.02.2019).

52. President's commission on critical infrastructure protection overview briefing (issued 07.1997) // U.S. Government Printing Office. URL: http://purl.access.gpo.gov/GPO/
LPS19904 (дата обращения: 15.06.2019).

53. The National Strategy to Secure Cyberspace [puplished 02.2003] // US Department of Homeland Security. URL: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (дата обращения: 16.02.2019).

54. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (issued on 29.05.2009) // The White House. URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (дата обращения: 16.02.2019)

Приложение А

Влияние информационных угроз на экономическую безопасность

Таблица А.1 - Влияние информационных угроз на экономическую безопасность

Уровень	Информационные угрозы	Экономические последствия	Влияние на экономическую безопасность
Государственный	Кибершпионаж и манипулирование уникальной разведывательной информацией	Разорение государства, обрушение валюты, нарушение устойчивости развития экономики, нереализация намеченных программ, подрыв инвестиционных проектов	Понижение уровня экономической безопасности государства
	Ведение информационных войн	Отставание ВВП, вызванное ростом непроизводительных расходов, формирование нового сегмента теневой экономики - «черного» киберрынка, нарушение рыночных механизмов и принципов конкуренции, монополизация экономики	
	Информационное доминирование развитых стран	Извлечение технологической ренты развитыми странами, усиление экономической зависимости от развитых стран, вытеснение с мирового информационного рынка	
	Информационное неравенство	Усиление экономической дифференциации общества	
Корпоративный	Повреждения информационных систем и инфраструктуры (преднамеренные и непреднамеренные)	Прямой финансовый ущерб; затраты на восстановление поврежденного оборудования	Понижение уровня экономической безопасности фирмы
	Внешний и внутренний кибершпионаж, фишинг. Неграмотность и халатность персонала	Утрата конкурентных преимуществ, снижение доверия к фирме, потеря доли рынка и доходов	
	Бесконтрольный доступ сотрудников у сети Интернет	Снижение производительности труда, потеря рабочего времени; потеря от снижения пропускной способности сети	
Личностный	Кража персональных данных, утрата приватности	Утрата профессиональной репутации; шантаж с целью изъятия денежных средств	Понижение уровня экономической безопасности личности
	Кибершпионаж с использованием банковских карт	Утрата денежных средств держателями кредитных и дебетовых банковских карт	

Приложение Б

Сведения о преступлениях в сфере компьютерной информации

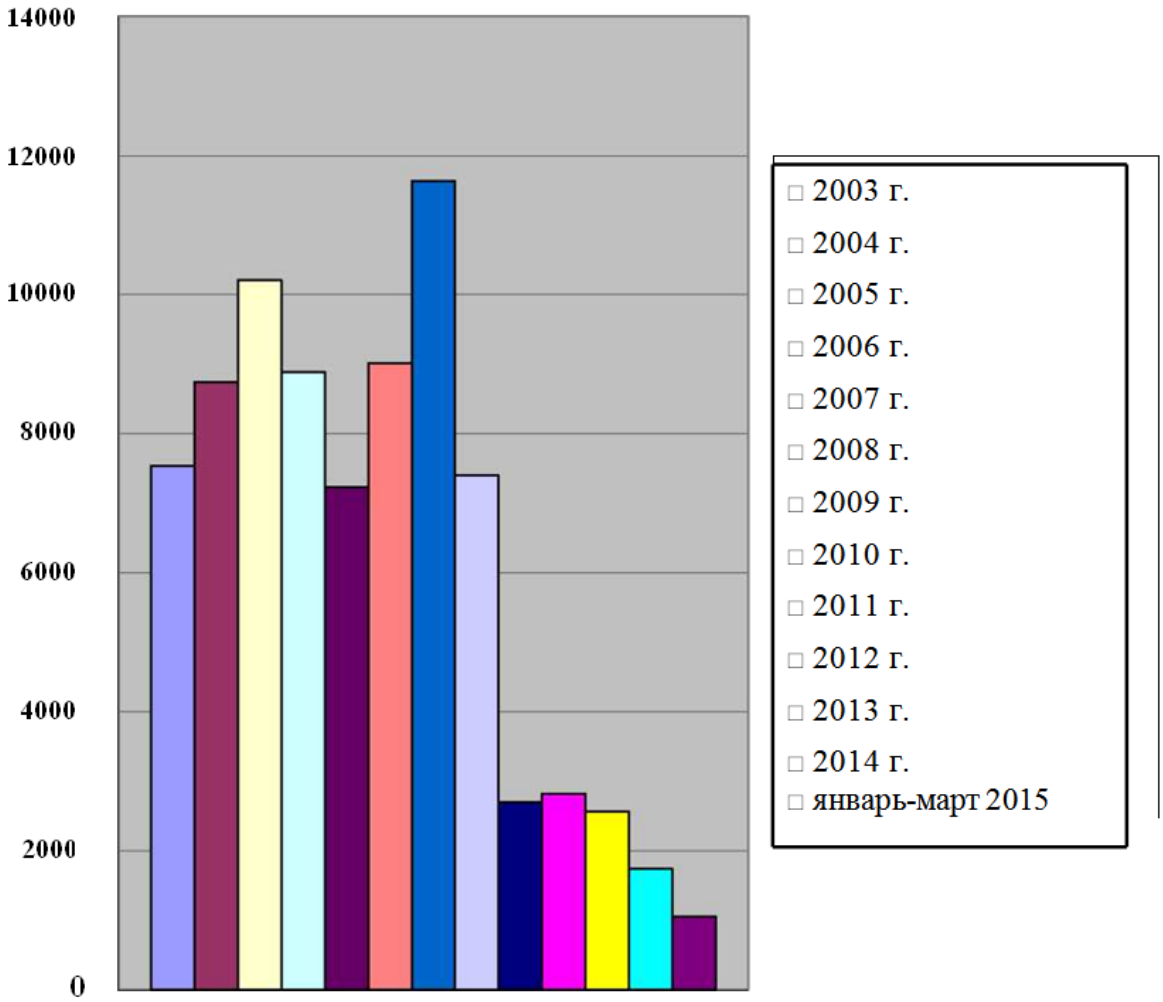
Таблица Б.1 – сведения о преступлениях в сфере компьютерной безопасности

Отчетный период	Зарегистрировано		В том числе			Из числа преступлений, дела и материалы о которых находились в производстве:	
	Всего	+, - в %	Выявлено сотрудниками ОВД			Раскрыто	
			Всего	+,- в %	Уд. вес %	Всего	+,- в %
2003 г.	7540	86,2				7186	91,5
2004 г.	8739	15,9				8406	17,0
2005 г.	10214	16,9				9759	16,1
2006 г.	8889	-13,0				8654	-11,3
2007 г.	7236	-18,6				6614	-23,6
2008 г.	9010	24,5				8419	27,3
2009 г.	11636	29,1	11599	-	99,7	11296	34,2
2010 г.	7398	-36,4	7365	-36,5	99,6	6804	-39,8
2011 г.	2698	-63,5	2671	-63,7	99,0	2687	-60,5
2012 г.	2820	4,5	2746	2,8	97,4	2425	-9,8
2013 г.	2563	-9,1	2424	-11,7	94,6	2301	-5,1

Приложение В

Количество зарегистрированных преступлений в сфере компьютерной информации

Рисунок В.1 - Количество зарегистрированных преступлений в сфере компьютерной информации



Приложение Г

О создании комиссии по категорированию объектов КИИ

В целях исполнения требований Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в соответствии с Постановлением Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации» (в частности п.11 о составе комиссии по категорированию), а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»,

ПРИКАЗЫВАЮ:

1. Создать постоянно действующую комиссию по категорированию объектов критической информационной инфраструктуры в составе:

Председателя комиссии:	Заместитель главного врача по медицинской части Иванов И.И.
Членов комиссии:	Специалист по ГО и ЧС Юрисконсульт Специалист по защите информации

2. В своей работе комиссия строго руководствуется требованиями нормативных документов в сфере обеспечения безопасности критической информационной инфраструктуры.
3. Комиссии в срок до «31» декабря 2019 года провести категорирование объектов критической информационной инфраструктуры согласно требованиям Постановления Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
4. В случае выявления объектов критической информационной инфраструктуры, комиссии направить результаты проведенного категорирования во ФСТЭК России согласно требованиям Приказа ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий». (изм. Приказом ФСТЭК от 21.03.2019 № 59)
5. Контроль за выполнением настоящего приказа оставляю за собой

Главный врач

Приложение Д

Положение о комиссии по КИИ информационной инфраструктуры

1 Общие положения

1.1. Настоящее Положение о комиссии по категорированию объектов критической информационной инфраструктуры (далее – Положение) определяет функции, порядок и обеспечение деятельности комиссии по категорированию объектов критической информационной инфраструктуры (далее – Комиссия).

1.2. Комиссия создается для проведения категорирования объектов критической информационной инфраструктуры ГУЗ «Поликлиника» (далее – Учреждение). постоянно действующим консультативно-совещательным органом Учреждения.

1.3. Комиссия руководствуется в своей деятельности Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной Федерации», постановлением Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 22.12.2017 № 236 «Об утверждении формы результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо отсутствии необходимости присвоения ему одной из таких категорий», приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 21.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (в ред. приказа ФСТЭК России от 26 марта 2019 г. № 60)».

2. Функции комиссии

2.1. Функциями Комиссии являются:

− определение управленческих, технических, производственных, финансово-экономических и (или) иных процессов, в рамках выполнения функций (полномочий) или осуществления видов деятельности Учреждения;

− выявление наличия критических процессов в Учреждении;

− выявление объектов критической информационной инфраструктуры (далее – КИИ), которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, подготовка предложений для включения в перечень объектов;

− рассмотрение возможных действий нарушителей в отношении объектов КИИ, а также иных источников угроз безопасности информации;

− анализ угроз безопасности информации и уязвимостей, которые могут привести к возникновению инцидентов на объектах КИИ;

− оценка в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения инцидентов на − установлению каждому из объектов КИИ одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им категории значимости.

3 Порядок и обеспечение деятельности комиссии

3.1. Заседания Комиссии проводятся по мере необходимости.

3.2. Заседание Комиссии считается правомочным при присутствии на нем не менее половины от общего числа членов Комиссии.

3.3. Решения принимаются простым большинством голосов членов Комиссии присутствующих на заседании. Каждый член Комиссии имеет один голос. При равенстве

голосов принятым считается решение, за которое проголосовал председательствующий на заседании Комиссии.

3.4. Комиссия при категорировании изучает:

− сведения об объекте КИИ (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами критической информационной инфраструктуры, наличие и характеристики доступа к сетям связи);

− процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности КИИ;

− состав информации, обрабатываемой объектами управлению, контролю или мониторингу, предоставляемые объектами критической информационной инфраструктуры;

− сведения о взаимодействии объекта КИИ с другими объектами КИИ и (или) о зависимости функционирования объекта КИИ от других таких объектов;

− угрозы безопасности информации в отношении объекта КИИ, а также имеющиеся данные, в том числе статистические, инцидентах, произошедших ранее на объектах КИИ соответствующего типа. Комиссия, изучив указанные сведения, утверждает перечень объектов КИИ.

3.5. Максимальный срок категорирования не должен превышать одного года со дня утверждения субъектом критической информационной инфраструктуры перечня объектов.

3.6. Решение Комиссии оформляется актом, который должен содержать сведения об объекте КИИ, результаты анализа угроз безопасности информации объекта КИИ, реализованные меры по обеспечению безопасности объекта КИИ, сведения о присвоенной объекту КИИ категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, а также сведения о необходимых мерах по обеспечению безопасности требованиями по обеспечению безопасности значимых объектов КИИ.

3.7. Акт подписывается председателем и другими членами Комиссии и утверждается главным врачом Учреждения.

3.8. В течение 10 дней со дня утверждения акта, указанного в пункте 3.1 настоящего Положения, председатель Комиссия направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Указанные сведения включают:

− сведения об объекте КИИ;

− сведения о субъекте КИИ, которому на праве собственности, аренды или ином законном основании принадлежит объект КИИ;

− сведения о взаимодействии объекта критической инфраструктуры и сетей электросвязи;

− сведения о лице, эксплуатирующем объект критической информационной инфраструктуры;

− сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры, в том числе средствах, используемых для обеспечения безопасности объекта критической информационной инфраструктуры и их сертификатах требованиям по безопасности информации (при наличии);

− сведения об угрозах безопасности информации и о категориях нарушителей в отношении объекта критической информационной инфраструктуры либо об отсутствии таких угроз;

− возможные последствия в случае возникновения компьютерных инцидентов на объекте критической информационной инфраструктуры либо сведения об отсутствии таких последствий;

− категорию значимости, которая присвоена информационной инфраструктуры, или сведения необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости;
− организационные и технические меры, применяемые для обеспечения безопасности объекта критической информационной инфраструктуры, либо сведения об отсутствии необходимости применения указанных мер.
3.9. Сведения, указанные в пункте 3.8 настоящего Положения, и их содержание направляются по форме, утверждаемой федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ.
3.10. Категория значимости может быть изменена в случаях, предусмотренных частью 12 статьи 7 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».
3.11. Не реже чем один раз в 5 лет Комиссия осуществляет пересмотр установленной категории значимости в соответствии с настоящим Положением. В случае изменения категории значимости сведения о результатах пересмотра категории значимости направляются в федеральный орган, области обеспечения безопасности КИИ.

Приложение Е

Заключение о формировании перечня объектов КИИ, подлежащих категорированию

1. Настоящее заключение составлено комиссией по категорированию объектов критической информационной инфраструктуры (далее - Комиссия) в целях принятия решения ГУЗ «Поликлиника» (далее - Учреждение) об отнесении информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, принадлежащих на праве собственности, аренды или на ином законном основании (далее – объекты) к объектам критической информационной инфраструктуры и включению объектов в перечень объектов критической информационной инфраструктуры подлежащих категорированию (далее – Перечень объектов), либо решений об отсутствии оснований для включения их в Перечень объектов.

2. Комиссия определила процессы, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ, выявила наличие критических процессов у субъекта КИИ, выявила объекты КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов и / или осуществляют управление, контроль или мониторинг критических процессов, а также готовит предложения для включения в перечень объектов.

3. По результатам работы комиссии была сформирована сводная таблица о наличии процессов и объектов критической информационной инфраструктуры

Продолжение Приложения Е

Таблица Е.1. – Список информационных систем

Вид деятельности	Процессы в рамках осуществления вида деятельности	Информационные системы, автоматизированные системы управления; сети, обеспечивающие функционирования процессов	Тип процесса	Негативные последствия в сфере	Примечание
1	2	3	4		5
Оказание медицинской помощи	**Амбулаторно-поликлиническая помощь**				
	Регистрация пациента, ведение электронной истории болезни	Региональная информационная система в сфере здравоохранения	Производственный	Социальная	
	Лекарственное обеспечение, лекарственная терапия	1С Аптека	Управленческий	нет	
Организация медицинского документооборота	Внутренний и внешний медицинский документооборот, хранение.	Региональная информационная система в сфере здравоохранения	Управленческий	нет	
	Отправка и прием электронной почты	Почтовый клиент	Управленческий	нет	

4. Комиссией были определены объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения Критических процессов, и (или) осуществляют управление, контроль или мониторинг Критических процессов. Приведенные в приложении объекты подлежат включению в Перечень объектов критической информационной инфраструктуры, подлежащих категорированию.

Продолжение Приложения Е

Таблица Е.2 – Перечень объектов подлежащих категорированию

№ п/п	Наименование объекта	Тип объекта	Сфера (область) деятельности, в которой функционирует объект	Планируемый срок категорирования объекта
1	2	3	4	5
	Региональная информационная система в сфере здравоохранения	информационная система	здравоохранение	До 31.12.2019

Председатель комиссии

Член комиссии

Член комиссии

Член комиссии

Приложение Ж

Сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

Таблица Ж.1 - Сведения об объекте критической информационной инфраструктуры

1.1.	Наименование объекта (наименование информационной системы, автоматизированной системы управления или информационно-телекоммуникационной сети)	Информационная система «Региональная информационная система в сфере здравоохранения»
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	Здравоохранение
1.4.	Назначение объекта	Автоматизация и создание структурированного информационного поля медицинского учреждения
1.5.	Критические процессы (управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, функции управления и контроля), которые обеспечиваются объектом	Регистрация пациента Направление на госпитализацию Диагностические исследования Диспансерное наблюдение Ведение медицинского документооборота
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	Сеть передачи данных, толстый и тонкий клиент

Продолжение Приложения Ж

Таблица Ж.2. - Сведения о субъекте критической информационной инфраструктуры

2.1.	Наименование субъекта	
2.2.	Адрес местонахождения субъекта	
2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	Главный врач А.А. Иванов
2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта.	Специалист по защите информации А.П. Иванов
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	Нет
2.6.	ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	3443055555

Таблица Ж.3 - Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи

3.1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	Сеть связи общего пользования
3.2.	Наименование оператора связи и (или) провайдера хостинга	ПАО «Ростелеком»
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	Передача (прием) информации
3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия	Волоконно-оптическая линии связи. 100BASE-SX.

Таблица Ж.4 - Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

4.1.	Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	ГУЗ «Поликлиника»
4.2.	Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	

Продолжение таблицы Ж.4

4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	Серверное, телекоммуникационное оборудование, автоматизированные рабочие места медперсонала и административно-технических сотрудников
4.4.	ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	3443055555

Таблица Ж.5 - Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры

5.1.	Наименования программно-аппаратных средств	АРМ врача – 200 шт, коммутатор-8 шт, маршрутизатор – 1 шт, сервер – 1шт,
5.2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	Windows 7, Windows 10, Windows Server 2012
5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	Программный комплекс Медицинская информационная система
5.4.	Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки) или сведения об отсутствии средств защиты информации	Применение программного изделия АПКШ «Континент 3.7». Сертификат соответствия ФСБ России СФ/124-3454 от 16 июля 2018, действителен до 15.05.20121 Сертификат ФСТЭК России № 3008 от 01.11.2013 действителен до 01.11.2019 Secret Net Studio 8 Сертификат ФСТЭК России № 3745 от 16.05.2017 действителен до 16.05.2020

Продолжение Приложения Ж

Таблица Ж.6 - Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры

6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	Нарушители с базовым (минимальным) потенциалом Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности, опубликованных в общедоступных источниках, и (или) самостоятельно осуществляют создание методов и средств реализации атак на информационную систему. Категории нарушителей 1. Внешние субъекты. Имеют мотивацию как причинение ущерба мошенническим или преступным путем. Или любопытство и самоутверждение. Выявление уязвимостей с целью их дальнейшей продажи. 2. Бывшие работники. Имеют мотивацию как причинение ущерба мошенническим или преступным путем. Месть за ранее совершенные действия. 3. Лица, осуществляющие технические работы на объекте (монтажники, заправщики, гарантийный ремонт). Причинение ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия. 4. Лица, обеспечивающие функционирование инфраструктуры (администрация, программисты, техники). Причинение ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия. 5. Пользователи информационной системы. Имеют мотивацию как причинение ущерба мошенническим или преступным путем. Причинение ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.
6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	УБИ.006 Угроза внедрения кода или данных Перечисляем перечень угроз по БДУ ФСТЭК РФ

Таблица Ж.7 - Возможные последствия в случае возникновения компьютерных инцидентов

7.1.	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	Отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств

Таблица Ж.8 - Категория значимости, которая присвоена объекту критической информационной инфраструктуры

8.1.	Категория значимости, которая присвоена объекту либо информация о неприсвоении объекту ни одной из таких категорий	**Категория 3**
8.2.	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	I. Социальная значимость 1) Причинение ущерба жизни и здоровью людей. Данный показатель критерия значимости применим к объекту, **присвоена категория по критерию причинения вреда здоровья одному человеку**
8.3.	Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	Например, социальная значимость – причинение вреда здоровью человеку, связанная с потенциальной возможностью неправильной постановки диагноза и методов лечения. Перечисляем перечень значимости данного объекта

Продолжение Приложения Ж

Таблица Ж.9 - Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры

9.1.	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	Установление контролируемой зоны; разграничение доступа к информации; утверждение политик, приказов, инструкций, актов, обеспечивающих защищенное нормальное функционирование объекта КИИ
9.2.	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	Применение программного изделия АПКШ «Континент 3.7». Сертификат соответствия ФСБ России СФ/124-3454 от 16 июля 2018, действителен до 15.05.20121 Сертификат ФСТЭК России № 3008 от 01.11.2013 действителен до 01.11.2019 Kaspersky Endpoint Security 11.x для Windows (для рабочих станций и файловых серверов) Сертификат ФСБ России СФ/019-3471 от 07.08.2018 действителен до 31.07.2013 Сертификат ФСТЭК России № 4068 от 22.01.2019 действителен до 22.01.2024 Secret Net Studio 8 Сертификат ФСТЭК России № 3745 от 16.05.2017 действителен до 16.05.2020

Главный врач

"__" _____ 20__ г.