Министерство науки и высшего образования Российской Федерации Федеральное государственное автономное образовательное
учреждение высшего образования
«Южно-Уральский государственный университет»
(национальный исследовательский университет)
ЮРИДИЧЕСКИЙ ИНСТИТУТ
Кафедра «Теория государства и права, конституционное и административное право»

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФГАОУ ВО «ЮУрГУ»
ЮУрГУ - 40.03.01. 2020. 019. ВКР

Руководитель работы,
канд. юрид. наук, доцент,
доцент кафедры
_____Максим Юрьевич Буртовой
_____ 2020 г.
Автор работы,
Студент группы Ю-519
_____Ляйсан Гирфановна Айдашева
_____ 2020 г.
Нормоконтролер,
_____Наталья Александровна Миронова
_____ 2020 г.

Челябинск
2020

АННОТАЦИЯ

Айдашева Л.Г. Выпускная квалификационная работа «Государственное регулирование информационной безопасности»: ФГАОУ ВО «ЮУрГУ (НИУ)», Ю-519, 83 с., библиогр. список – 91 наим., прил. 1.

Объектом дипломной работы является общественные отношения, которые возникают в процессе государственного регулирования информационной безопасности в Российской Федерации.

Предметом дипломной работы являются рассмотрение политики, правового регулирования, принципов и методологии обеспечения государственного регулирования информационной безопасности в Российской Федерации.

Целью дипломной работы является изучение теоретических основ, которые определяют место и роль государственного регулирования информационной безопасности Российской Федерации, определение проблем в ходе осуществления государственного регулирования в этой сфере, определения пути решения выявленных проблем.

В процессе работы над дипломной работой мною было изучено значительное количество нормативного материала, общетеоретической и специальной литературы, а также некоторые примеры из практики. В рамках проведенной работы было проанализировано современное понятие «информационной безопасности», определена политика информационной безопасности Российской Федерации, выявлены проблемные аспекты; раскрыты основы правового регулирования информационной безопасности в Российской Федерации, а зарубежных странах и на международно-правовом уровне, выявлены проблемные аспекты и выделены ведущие страны, которые осуществляют правовое регулирование на достойном уровне, определены основные направления международно-правового регулирования информационной безопасности; проанализировано содержание государственно правового регулирования информационной безопасности Российской Федерации,

определены органы, осуществляющие государственное регулирование информационной безопасности, раскрыты принципы и методы государственное регулирование информационной безопасности.

Результаты исследования имеют практическую значимость, содержат выводы и предложения обозначенных в выпускной квалификационной работе проблем, связанных с государственным регулированием информационной безопасности.

Результаты исследования могут быть полезны при разработке программ обучения юристов, а также при изучении предмета «Информационное право», «Информационная безопасность».

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Развитие личности, общества и государства в различные исторические периоды всегда проходило и проходит через стадию кризиса, проявляющегося в их разнообразных кризиса. В условиях развития компьютерных и информационно-телекоммуникационных технологий нахождение границы частного и публичного интересов становится с каждым разом все более затруднительным, особенно в свете недавно принятых законодательных мер противодействия терроризму и обеспечения общественной безопасности. Между тем кризис выступает не только орудием расшатывания сложившейся системы ценностей, в которой пребывает общество и человек, но переломным моментом в осмыслении того огромного значения, которое несет в себе неприкосновенность частной жизни для развития правосознания человека.

Обеспечение информационной безопасности является одним из центральных звеньев во внешней политике любого государства, всё это, безусловно, связано с глобальной информационной революцией. Одновременное развитие двух сфер, с одной стороны постоянный рост объема информации и его роли в жизни каждого, с другой стороны, постоянный процесс развития и совершенствования технологий накопления и распространений информации. Поэтому надёжная работа информационных ресурсов, систем управления и связи имеет исключительное значение для обороноспособности страны, для устойчивого развития экономики и социальной сферы, для того чтобы обеспечить суверенитет государства.

Современный мир не стоит на месте, и он подвергается постоянным изменениям, преобразованиям, которые связаны, в первую очередь с информационными и цифровыми технологиями. Формирование информационного пространство окончательно не закончилось, оно постоянного находится в развитие, создавая при этом новые возможности, перспективы для развития государства в экономических, политических, культурных и других сферах. Но за каждым явлением могут быть как

положительные стороны, так и отрицательные. Так, несомненно, развитие информационной сферы дало огромные плюсы в развитие государства, но и при этом есть и плохие стороны данного фактора. Рост зависимости государств от информационных систем, их проникновение во все человеческие жизни поспособствовало появлению и развитию компьютерных преступлений, а также дало толчок в возникновении новых международных конфликтов, вплоть до того что появились международные хакерские атаки. Международные войны теперь происходят не только в тех привычных нам средах: водных, воздушных и наземных, но и на информационном пространстве.

Ведение так называемых «информационных войн», имеющее своей целью воздействие на сознание человека, не запрещено на международном уровне, что дает возможность технически развитым странам использовать информационные технологии против других государств.[1] Учитывая данные факты, думаю не вызывает никаких сомнений то, что тема государственного регулирования в информационной безопасности на сегодняшний день и с течением времени достаточно актуальна и находится в центре внимания общества и государства.

«Для системы государственного управления актуальной является проблема качественных изменений в деятельности органов власти, то есть переформатирование системы управления с учетом механизма согласования интересов управляемых и управляющих субъектов, который должен получить основание в законодательстве, в общественно сознании и политической культуре государственных служащих и граждан».[2]

Безусловно, ни одна сфера жизни на современном этапе развития общества не может функционировать без развитой информационной структуры. Именно, поэтому национальный информационный ресурс стал на

[1] Артюшова Е.А. Проблемы международно-правового регулирования информационной безопасности // Lex russica (Русский закон). 2009. № 5. С. 1166.
[2] Филатов В.В. Зарубежный опыт правового регулирования информационной безопасности // WSCHODNIOEUROPEJSKIE CZASOPISMO NAUKOWE. 2018. № 3-6 (31). С. 70.

сегодняшний момент одним из ключевых факторов, влияющих на все сферы, а основным из них является экономика, так как рост любого государства, зависит от экономической составляющей, государство заинтересовано в тщательном регулирование данной сферы.

Необходимо отметить, что государство в ходе осуществления государственного регулирования информационной безопасности исходит из необходимости, в первую очередь, защитить собственные интересы в информационной сфере, а, в свою очередь, общество исходит из своих интересов. И в итоге получается, что происходит конфликт интересов, каждая сторона, хочет получить свою выгоду, что приводит к абсолютному игнорированию информационной безопасности, в погоне получения выгоды для себя.

Государству в свою очередь необходимо пристально уделить внимание и направить все свои усилия в сторону предотвращения действий, которые направлены на возникновение и введение информационных войн против государства, которые дестабилизируют систему национальной безопасности. Для того, чтобы общество продолжало развиваться и стремительно прогрессировало, государству необходимо обеспечить кибербезопасность.

Проблемами государственного регулирования информационной безопасности в Российской Федерации занимались различные ученые, такие как: О.А. Городов, В.Н. Лопатин, О.А. Степанов, Д.Б Фролов, Ю.М. Батурин, В.А. Копылов, А.А. Фатьянов, В.Д. Элькин, И.Б. Григорьев. Также вызывают большой интерес, научно-исследовательские труды, следующих авторов: Т.П. Кукса, А.С. Минзов, Д.Н. Садчикова, К.С. Садов, Н.А. Антоненко, И.О. Мельникова, А.Э. Мысев, Н.В. Морозов, Н.М. Курбатов, Е.А. Проценко, Н.В. Михайленко, Х.А. Андриашин, А.А. Карцхия, В.В. Филатов, Р.М. Асланов, Д.Н. Щедрин, В.М. Кулешов, А.В. Тарасенко, О.В. Столетов, М.В. Ареева, В.М. Елин, Е.А. Артюшова, В.Н. Тихонов, Р. Мардашина, Н.И. Костенко, В.В. Середа, А.Ю. Карась, Г.О. Крылов, В.М. Лазарев, А.Е. Любимов, А.А. Ефремов, Е.С. Зиновьева, А.П. Фисун, Ю.А. Белявская, И.В. Плюгина, А.А.

Мурашкин, Н.А. Трынченков, Д. Устинов, И.П. Михнев, С.В. Михнева, Ю.В. Косов, Ю.В. Вовенда, В.А. Мазуров, С.А. Дементьев.

Объектом дипломной работы является общественные отношения, которые возникают в процессе государственного регулирования информационной безопасности в Российской Федерации.

Предметом дипломной работы являются рассмотрение политики, правового регулирования, принципов и методологии обеспечения государственного регулирования информационной безопасности в Российской Федерации.

Целью дипломной работы является изучение теоретических основ, которые определяют место и роль государственного регулирования информационной безопасности Российской Федерации, определение проблем в ходе осуществления государственного регулирования в этой сфере, определения пути решения выявленных проблем.

Для достижения указанной цели в дипломной работе решались следующие задачи:

1) рассмотрение понятия информационной безопасности;

2) определение государственной политики в сфере информационной безопасности;

3) изучение правового регулирования информационной безопасности в Российской Федерации;

4) изучение правового регулирования информационной безопасности в зарубежных странах;

5) изучение международно-правового регулирования информационной безопасности;

6) рассмотрение органов государственной исполнительной власти в сфере информационной безопасности;

7) рассмотрение принципов государственного регулирования информационной безопасности;

8) определение и рассмотрение методов государственного регулирования информационной безопасности;

В процессе работы над дипломной работой мною было изучено значительное количество нормативного материала, общетеоретической и специальной литературы, а также некоторые примеры из практики.

Во время работы общую методологическую основу дипломной работы составил диалектический метод познания, системный, исторический для изучения проблемы. А также использовались специальные юридические методы познания: исторически-правовой, системно-структурный, сравнительно-правовой, формально-логический, аналогии, моделирования и обобщения.

Структура работы соответствует поставленным целям и задачам. В первой главе рассматриваются доктринальные основы информационной безопасности в современных условиях, дается понятие информационной безопасности и определяется государственная политика информационной безопасности. Вторая глава посвящена правовым основам информационной безопасности, а Российской Федерации, зарубежных странах и в рамках международно-правового регулирования информационной безопасности. В заключительной третей главе изложено органы, обеспечивающие государственное регулирование информационной безопасности, рассмотрены органы государственной власти, принципы и методы государственного регулирования в этой сфере.

1. ДОКТРИНАЛЬНЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ.

1.1 Понятие информационной безопасности.

Информационная безопасность в XXI представляет собой большую значимость, учитывая тот факт, насколько быстро развиваются технологии обработки, хранения и передачи информации, применение информационных технологий. Происходят постоянные изменения, модификации, блокирование, копирование информационных ресурсов, которое приводит к нанесению ущерба не только отдельно взятому гражданину или организации, но и государству в целом.

Для того, чтобы дать полное определение «информационной безопасности», необходимо определится, что из себя представляет «информация» и «безопасность» как отдельные категории.

В научной литературе существует большое количество мнений о том, что же представляет собой понятие «информация». Так, согласно мнению А.А. Снытникова, «информация как благо нематериальное имеет множество разнообразных оттенков. В зависимости от тех или иных обстоятельств в повседневной жизни информация может быть актуальной и устаревшей, объективной и субъективной, основательной и безосновательной, многоплановой и однобокой, укрепляющей и компрометирующей и т.д.»[1]

Достаточно интересное мнение у О.А. Городова, он считает, что «… информации только прагматика интересуется конкретными пользователями информационного продукта и той областью общественных отношений, участниками которых они выступают».[2]

---

[1] Снытников А.А. Обеспечение и защита прав на информацию // М. 2001. 22с

[2] Городов О.А. Информационного права России. Учебное пособие // СПб.: Юридический центр Пресс, 2003 с. 19

В словаре основных понятий книги, содержится следующее толкование информации:

Информация (в узком смысле) - это любые сведения об окружающем мире, которые человек получает с помощью органов чувств.

Информация (в широком смысле) - это общенаучное понятие, включающее в себя обмен сведениями между людьми, обмен сигналами между живой и неживой природой, людьми и устройствами, между устройствами без участия человека.[1]

Информация - это сведения (сообщения, данные) независимо от формы их представления.[2]

Что же в свою очередь представляет «безопасность»? Если трактовать безопасность как указано в Законе Российской Федерации «О безопасности», то под безопасностью подразумевается «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». Так, например, «Кукса Т.П. в своих работах писал, что безопасность довольно часто представляют как способность объекта сохранять при наличии деструктивных, дезорганизующих воздействий (внешних и/или внутренних) свои важнейшие, системообразующие свойства, основные характеристики и параметры, потеря которых может привести к тому, что объект утрачивает свою сущность, перестает быть самим собой».[3]

Теперь необходимо определится, что же собой представляет общее понятие «информационная безопасность». Так из Доктрины информационной безопасности Российской Федерации под ней понимается защищенность личности, общества и государства от информационных угроз извне и изнутри,

---

[1] Панфилова О.А. Информационная безопасность и защита информации: учебное пособие для направления подготовки 40.03.01 - Юриспруденция, специальности 40.05.02 - Психология служебной деятельности, очной и заочной форм обучения // Вологда, ВИПЭ ФСИН России, 2018. с.59

[2] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ // СЗ РФ. 2004. № 27. Ст. 2711.

[3] Кукса Т.П. Содержание понятия «Информационная безопасность» // В сборнике: Морская стратегия и политика России в контексте обеспечения национальной безопасности и устойчивого развития в XXI

обеспечивающее реализацию конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое социально-экономическое развитие Российской Федерации, оборону и безопасность государства. Таким образом, под информационной безопасностью понимаются 2 составляющие:

В первую очередь, состояние (качество) определенного объекта (под объектом понимается, данные, информация, информационно-коммуникационные сети, ресурсы автоматизированных систем). Во вторую очередь, это деятельность, которая направлена на организацию обеспечения состояния защищенности объекта (в данную деятельность входят мероприятия правового, организационного, технического характера, которые направлены на предотвращение угроз информационной безопасности).

Но в научной литературе не сложилось единого взгляда на содержание понятия «информационная безопасность». Понятие «информационная безопасность» тесно взаимосвязано с понятием «безопасность информации». Их достаточно часто используют в качестве синонимов, но необходимо заметить, что существование «безопасности», без определения объекта понятия «безопасность» является неопределенным и бессмысленным (лишенном внутреннего смысла).

Понятие «информационная безопасность» приобретает тот или иной смысл в зависимости от объекта безопасности. В том случае, если объектом защиты будет выступать информация, то в таком случае, понятия «информационная безопасность» и «безопасность информации» будут выступать синонимами и их значение будет идентичное. В том случае, если объектом будет выступать другой объект, например, участник информационных отношений, то в понятие «информационная безопасность» слово «информационная» указывает на направление деятельности, в таком случае трактуется как состояние защищенности данного объекта от угроз информационного характера.

Так, в утратившей силу Доктрине информационной безопасности РФ, под информационной безопасностью понималось «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства».[1] В этом случае, под безопасностью информации, понимается безопасность интересов общественных отношений в информационной сфере, от устойчивости которых зависит уровень угроз.

Если рассматривать другие официальные источники, в которых содержалось бы полное понятие информационной безопасности. Так в утратившем силу «в федеральном законе Российской Федерации «Об участии в международном информационном обмене», под информационной безопасностью понимается состояние защищенности информационной среды общества, которая также обеспечивает формирование, использование и развитие в интересах граждан, организаций и государства».[2] В данном понятии защита информации и информационная инфраструктура является одним целым и представляет одно понятие «информационная безопасность». Важную сторону в этом понятии является техническая сторона.

В последнее время, достаточно большое внимание уделяется к другому подходу, совершенно противоположному предшествующим определениям информационной безопасности. Так, под информационной безопасностью понимается, защита от информации. Так одним из сторонников данного понимания определения «информационная безопасность» является С.П. Расторгуев, который высказывался по этому поводу следующим образом: «В результате проблема защиты информации, которая ранее была как никогда актуальна, перевернулась подобно монете, что вызвало к жизни ее противоположность. Теперь уже саму информационную систему и, в первую

---

[1] Доктрина информационной безопасности Российской Федерации: утв. Президентом Рос. Федерации 9 сент. 2000 г. № ПР-1895 // Российская газета. 2000. № 28. Признан утратившим силу.

[2] Федеральный закон от 4 июля 1996 г. № 85-ФЗ «Об участии в международном информационном обмене» // СЗ РФ 2006. № 149. Признан утратившим силу.

очередь человека - необходимо защищать от поступающей «на вход» информации, потому что любая поступающая на вход самообучающейся системы информация неизбежно изменяет систему. Целенаправленное же деструктивное информационное воздействие может привести систему к необратимым изменениям и, при определенных условиях, к самоуничтожению».[1] Всё больше и больше взаимоотношения людей становится опосредованной и переходит в информационную среду. Во главу угла общественной жизни все чаще становится отношение человека к самой информации, которая стала сегодня основной ориентации людей в повседневной жизни. Поэтому контроль над информацией, циркулирующей в средствах информации и телекоммуникационных каналах, позволяет активно влиять на формирование модели мира, и, следовательно, обеспечивать желаемые типы поведения. Средства коммуникации, оперирующие, трансформирующие, дозирующие информацию, становятся главными инструментами влияния на современное общество. Для повышения эффективности осуществления властных стратегий используются самые современные информационные технологии, которые помогают превратить публику в объект манипулирования. При этом сознание массового человека оказывается насквозь структурировано немногими, но настойчиво внедряемыми в него утверждениями, которые, бесконечно транслируясь средствами информации, образуют некий невидимый каркас из управляющих мнений, установлений, ограничений, который определяет и регламентирует реакции, оценки, поведение публики.[2]

Понятие «информационная безопасность» достаточно тесно взаимосвязано с понятием «безопасность информации» или «защита информации», они достаточно синонимичны. Но «безопасность» не может существовать сама по себе, безотносительно к объекту, «без внутреннего

---

[1] Расторгуев С.П. Философия информационной войны / С.П. Расторгуев. М., 2016. С. 47

[2] Лепский В.Е. Становление стратегических субъектов в глобальном информационном обществе: постановка проблемы // Информационное общество, 2002. С.58

смысла».[1] Содержание понятия «безопасность» предопределяется выбором объекта безопасности. Если в качестве объекта защиты выступает собственно информация, то понятия «информационная безопасность» и «безопасность информации» действительно становятся синонимами. Если же в качестве объекта защиты рассматривается другой объект (субъект) - участник информационных отношений, то слово «информационная» в термине «информационная безопасность» указывает на направление деятельности, посредством которой может быть причинен вред объекту защиты и понятие «информационная безопасность» в этом случае следует трактовать как состояние защищенности данного объекта от угроз информационного характера.[2]

Таким образом, учитывая всё вышесказанное информационная безопасность - это достаточно широкое понятие, которое включает в себя все, что взаимодействует с информацией. Было приведено достаточно большое количество понятии, которые содержатся, как в научной литературе, так и в некоторых правовых актах. Но, достаточно большой интерес вызывает определение, данное А.И. Алексенцевым: «информационная безопасность - состояние информационной среды, обеспечивающее удовлетворение информационных потребностей субъектов информационных отношений, безопасность информации и защиты субъектов от негативного информационного воздействия».[3] В понятие А.И. Алексенцевым, по моему мнению, содержатся все необходимые признаки для характеристики информационной безопасности.

---

[1] Стрельцов А.А. Обеспечение информационной безопасности России // Теоретические и методические основы. М.:МЦНМО, 2002. С. 55.

[2] Кукса Т.П. Содержание понятия «Информационная безопасность» // В сборнике: Морская стратегия и политика России в контексте обеспечения национальной безопасности и устойчивого развития в XXI.

[3] Алексенцев А.И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» // Безопасность информационных технологий. 1999. № 1. С. 45

1.2 Государственная политика в сфере информационной безопасности.

В России, как и в других государствах, наблюдается возрастание роли информационной сферы, увеличение значения информации как фактора жизни, непосредственно влияющие на национальную безопасность государства. Именно поэтому возникает потребность правовой оценки и регламентации информационных отношений.

Интересное мнение выразила Антоненко Н.А. в своей научной работе: «Анализируя нормативно-правовую литературу можно увидеть определенную поэтапный процесс развития и формирования государственной политики в сфере информационной безопасности и их можно условно разделить на семь этапов.

Характеризуя 1й этап, этап условно, называемый становлением информационной безопасности и он охватывал период до 1816 года. Данный этап заключался в защите сведений о событиях, фактах, имуществе, а также местонахождении и других данных, которые имеют значение для государства и для его граждан жизненное значение.

Второй этап, начинает свой отсчет с 1816 года. Данный этап связан с началом использования искусственно создаваемых технических средств электрики и радиосвязи. Опыт данного периода информационной безопасности сводился к применению помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения.

Третий этап, он начинается с 1935 года, который связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение активности радиолокационных средств от воздействия на их приемные устройства

активными маскирующими и пассивными имитирующими радиоэлектронными помехами».[1]

Государственная политика России в сфере информационной безопасности построена на основе соблюдения интересов личности, общества и государства в информационной сфере. Государственная политика прежде всего определяет важнейшие направления деятельности федеральных органов государственной власти и органов государственной власти субъектов РФ в сфере обеспечения информационной безопасности, кроме того в нём закрепляется порядок реализации их обязанностей, которые направлены на защиту интересов РФ в информационной среде.

Развитие информационных технологий и проникновение их во все сферы общества и государства, привили к необходимости принятия Российской Федерацией ряда правовых документов для защищенности информационного пространства России.

Доктрина информационной безопасности, которая была утверждена Указом Президента РФ от 5 декабря 2016 г. № 646.[2] Данную доктрину можно расценивать, как огромный шаг в развитие безопасности нашей страны. В данной доктрине отражаются государственные интересы, взгляды, которые официально придерживается государство, цели, задачи, принципы, также основные направления в обеспечении информационной безопасности Российской Федерации.

Данная доктрина содержит информацию не только обеспечивающую информационную безопасность в нашей стране на десятки лет вперед, но также отражаются существующие недостатки мер, которые были предприняты. В доктрине стало намного больше конкретики, а все те детерминанты, влияющие на ситуацию, которая связана с информационной

---

[1] Антоненко Н.А. Этапы развития и становления государственной политики России в сфере информационной безопасности // Новая наука: Проблемы и перспективы. 2016. № 9-1. С. 132.

[2] Указ Президента «Об утверждении Доктрины информационной безопасности Российской Федерации» от 5 декабря 2016 г. № 646 // СЗ РФ. 2016. № 50. Ст. 7074

безопасностью в России, охватили все сферы деятельности общества: кредитно-финансовую сферу, государственную и общественную безопасность.

Но нельзя ограничиться, одним нормативным актом, государственная политика в области информационной безопасности в Российской Федерации регулируется целым рядом нормативных правовых актов, «особое место среди них занимает Стратегия национальной безопасности РФ, которая была подписана 31 декабря 2015 г. президентов Российской Федерации В.В. Путиным».[1] Данный документ имеет достаточно большое значение, обусловлено это тем, «что современная государственная информационная политика тесно взаимодействует с государственной политикой обеспечения национальной безопасности страны посредством системы информационной безопасности. В данном правовом акте определены национальные интересы, а также стратегические приоритеты Российской Федерации в современных условиях. Как отмечает К.А. Мамедова: в данном документе подчеркивается, что укрепление России происходит на фоне новых угроз национальной безопасности, имеющих взаимосвязанный характер».[2]

«Стратегия национальной безопасности РФ выступает в роли основополагающего, базового документа стратегического планирования, в котором закреплены не только национальные интересы и стратегические приоритеты страны, но также определяются цели, задачи и меры в сфере внутренней и внешней политики, ориентированные на укрепление национальной безопасности государства в целом и обеспечение его стабильного развития на долгосрочную перспективу».[3] При этом Стратегия своими целями преследует обеспечения безопасности во всех сферах жизни современного общества. Так, «она предусматривает в перспективе обеспечить

---

[1] Указ Президента РФ «О Стратегии национальной безопасности Российской Федерации» 5 декабря 2016 г. № 646

[2] Мамедова, К.А. Основные принципы обеспечения информационной безопасности страны/ К.А. Мамедова // Информационная безопасность регионов.2016. № 1. С. 16-20.

[3] Полякова Т.А., Базовые принципы как основные начала правового обеспечения информационной безопасности / Т.А. Полякова // Труды института государства и права Российской академии наук. 2016. № 3. С. 17-40.

развитие национальной экономики, здравоохранения, образования, культуры, науки, улучшение качества жизни граждан, укрепление политической стабильности в обществе, а также обороны страны, развитие государственной и общественной безопасности, эффективное повышение конкурентоспособности и международного престижа России».[1] Одной из основных угроз информационной безопасности в вышеуказанных документах признана киберпреступность. Да, это действительно так, масштабы, которые охватывает компьютерная преступность, прогрессирует и достаточно быстро, большая масса преступлений связана с кредитно-финансовой сферой и с нарушениями прав и свобод человека и гражданина, которые касаются персональных данных. Так, по данным лаборатории Каперского, «финансовое мошенничество стало одной из наиболее распространенных угроз информационной безопасности. Примерно 20 % российских интернет-пользователей при совершении банковских операций и онлайн-покупок как минимум два раза становились жертвами киберпреступников, теряя при этом денежные средства. Схожая проблема существует и при обработке информации новая Стратегия предполагает использование российских криптоалгоритмов и средств шифрования при взаимодействии органов власти между собой, а также с гражданами и организациями. Предполагается, что для предоставления безопасных услуг и программного обеспечения в отечественных информационно-телекоммуникационных системах будут использоваться встроенные средства защиты информации».[2]

Главной целью поставленной в Стратегии является формирование в России «общества знаний», то есть такого общества, «в котором преобладающее значение для развития гражданина, экономики и государства имеют получение, сохранение, производство и распространение достоверной

---

[1] Садчикова, Д.Н. О современной государственной политике в области информационной безопасности / Д.Н. Садчикова // Поколение будущего: Взгляд молодых ученых. 2018. С 236-239

[2] Козырева А.А., Тарасов Д.А. Современное состояние государственной политики в сфере информационной безопасности // Вестник Воронежского института МВД России. 2018. № 4. С. 244.

информации с учетом стратегических национальных приоритетов Российской Федерации».[1]

Только в таких условиях, когда современные информационные угрозы снова актуализируются основы безопасности человека. И в таком случае одним из основных направлений по обеспечению информационной безопасности, становится повышение эффективности по осуществлению защиты информационных инфраструктур и их устойчивости в функционировании, отработка механизмов обнаружения и, конечно же, «предупреждения информационных угроз, ликвидации последствий их проявления, а также повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных негативным воздействием на объекты информационной инфраструктуры».[2]

До настоящего времени основным концептуальным документом, определяющим политику Российской Федерации в информационной сфере, содержание национальных интересов и потребность государства в обеспечении их безопасности в настоящий момент является утвержденная Указом Президента от 9 мая 2019 г. № 203 новая Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы,[3] в которой были определены основные цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и телекоммуникационных технологий, направленных на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Стратегия, которая была принята, сформулированы новые направления, положения Стратегии не сильно отличаются от предыдущих правовых актов,

---

[1] Указ Президента РФ «О Стратегии национальной безопасности Российской Федерации» 5 декабря 2016 г. № 646

[2] Так же. С. 245

[3] Указ Президента РФ от 9 мая 2017 г. № 203 «О стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // СЗ. 2017. № 20. Ст. 2901.

но они заметны при детальном анализе. Об этом и отмечают некоторые специалисты, которые утверждаю о «смещение акцентов в восприятии окружающего мира с научного, образовательного и культурного на развлекательно-справочный, что сформировало новую модель восприятия – так называемое «клиповое» мышление, характерной особенностью которого является массовое поверхностное восприятие информации».[1]

Так в Стратегии развития информационного общества в РФ, определены следующие приоритетные направления развития, данные направления достаточно подробно:

1. «Развитие «общества знаний». Новая стратегия развития информационного общества принята в целях обеспечения условий для формирования в Российской Федерации общества знаний».[2]

Согласно Стратегии, общество знаний – это общество, в котором преобладающее значение для развития гражданина, экономики и государства имеет получение, сохранение, производство и распространение достоверной информации с учетом стратегических национальных приоритетов Российской Федерации.

В Стратегии подчеркивается то, что российское общество заинтересовано в получении информации, которая соответствует высокому интеллектуальному и культурному развитию граждан России.

В силу таких преобразований, перед Стратегией были поставлены среди основных целей: «развитие человеческого потенциала, обеспечение безопасности граждан и государства; повышение роли России в мировом гуманитарном и культурном пространстве».[3]

---

[1] Азаренок Н.К., Клиповое сознание и его влияние на психологию человека в современном мире // Традиционная Всероссийская юбилейная научная конференция «Психология человека в современном мире», посвящ. 120-летию со дня рожд. С.Л. Рубинштейна. Т.3. личность и группа в условиях социальных изменений. Отв. Ред. А.Л. Журавлев. М.: «Институт психологии РАН», 2016. С.110.

[2] Чубукова С.Г., Стратегии развития информационного общества и направления развития законодательства // Правовая информатика. 2017. № 2. С. 69.

[3] Чубукова С.Г. Стратегии развития информационного общества и направления развития законодательства // Правовая информатика. 2017. № 2. С. 69.

Основополагающими принципами Стратегии стали: приоритет традиционных российских духовно-нравственных ценностей и соблюдение основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий.

Так для достижения своих целей и формирования информационного пространства знания Стратегия предусмотрела целый ряд мер, в том числе: мероприятия в области духовно-нравственного воспитания граждан; просветительские проекты; популяризация информационных ресурсов, способствующих распространению традиционных российских духовно-нравственных; создание условия для научно-технического творчества; развитие различных образовательных технологий, дистанционного, электронного обучения. Что, в свою очередь, потребует развития механизма законодательного регулирования, в следующих областях:

- в области ограничения доступа к информации, распространение которой в РФ запрещено федеральным законом;

- в области средств массовой информации, а также средств обеспечения доступа к информации, которые по многим признакам могут быть отнесены к СМИ, но с точки зрения законодательства, не являются таковыми.

- по эффективному использованию современных информационных платформ для распространения достоверной и качественной информации российского производства.

2. «Цифровая экономика». Экономика является одним из основных составляющих для развития любой странны. «А информационное общество – это, прежде всего, экономика, основанная на знаниях. Вместе с тем развитие технологий сбора и анализа данных, обмена ими, когда управление производственными процессами осуществляется на основе внедрения нано- и биотехнологий, технологий искусственного интеллекта, робототехники.

Повсеместное применение таких технологий способствует развитию нового этапа экономики – «цифровой экономики»».[1]

В Стратегии впервые дано определение понятия цифровой экономики как хозяйственной деятельности, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг.[2]

Стоит уделить большое внимание, так в Стратегии была поставлена в числе основных задач создание системы, обеспечивающей возможность устойчивого, безопасного и независимого функционирования российского сегмента сети Интернет. Проблема правового регулирования интернет-отношений были актуальны в 2017 году, как и по сегодняшний день. Но, принятая Стратегии внесла большие коррективы и дала толчок для развития законодательства обеспечения безопасности в сфере развития интернет-отношений.

В Стратегии были предусмотрены, следующие основные моменты для обеспечения безопасного и независимого функционирования сегмента сети Интернет:

1. Принять меры по обеспечения устойчивого функционирования российского сегмента сети Интернет;

2. Реализовывать государственную политику в части, касающейся государственного управления инфраструктурой российского сегмента сети Интернет;

3. Выработать технические и законодательные меры по предотвращению нарушений работы сети интернет и отдельных ее ресурсов

---

[1] Чубукова С.Г., Стратегии развития информационного общества и направления развития законодательства // Правовая информатика. 2017. № 2. С. 68.
[2] Так же. С. 69

на территории Российской Федерации в результате целенаправленных действий.

Как уже отмечалось, положения данной стратегии, вызвали большой интерес и активность для проявления законотворческой инициативы. И с этого момента было предложено большое количество предложений, которые стали большим толчком в развитие интернет-отношений.[1]

Так, «в мае 2017 г. депутаты от «Единой России», КПРФ и «Справедливой России» внесли на рассмотрение Государственной думы РФ законопроект о регулировании мессенджеров в России, который был принят в первом чтении. Документ обязывает организаторов обмена сообщениями идентифицировать пользователей по номеру и оказывать в предоставлении услуг при несоблюдении этого правила. Также мессенджеры обязаны вводить отказ получать сообщения от других пользователей, обеспечить возможность рассылки и передачи сообщений инициативе органов государственной власти и ограничить передачу сообщений, содержащих информацию, распространяемую с нарушением требований законодательства РФ».[2]

С 1 октября 2017 г. Федеральный закон «Об информации, информационных технологиях и о защите информации» установил запрет на размещение в сети «Интернет» сайтов, сходнях до степени смешения с сайтами, доступ к которым ограничен по решению московского городского суда («зеркальных» сайтов), определил порядок блокировки указанных сайтов Роскомнадзором, а также установил обязанность операторов связи и операторов поисковых систем по ограничению доступа к копиям заблокированных сайтов и прекращению выдачи сведений о доменных именах и об указателях страниц копий заблокированных сайтов.[3]

---

[1] Чубукова С.Г. Стратегии развития информационного общества и направления развития законодательства // Правовая информатика. 2017. № 2. С. 72.
[2] Так же. С. 71.
[3] Федеральный закон от 01 июля 2017 г. № 156-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»» // СЗ РФ. 2017. № 27. Ст. 3953

«В июне 2017 г. парламентарии внесли на рассмотрение законопроект о запрете обхода блокировок сайтов с помощью VPN-сервисов и анонимайзеров».[1] «С ноября 2017 г. вступили в силу поправки в Закон «Об информации, информационных технологиях и о защите информации», которые установили, что Роскомнадзором определяет порядок идентификации информационных ресурсов в целях принятия мер по ограничению доступа к таким ресурсам, требования к способам (методам) ограничения доступа, а также размещаемой информации об ограничении доступа к информационным ресурсам. Данные поправки определили перечень мер, направленных на противодействие использованию в России информационно-телекоммуникационных сетей и информационных ресурсов, посредством которых обеспечивается доступ к информационно-телекоммуникационным сетям и информационным ресурсам, доступ к которым в России ограничен».[2]

Не вызывает сомнений, что обеспечение безопасности жизнедеятельности человека и гражданина должно обеспечиваться и за счет сформирования культуры личной безопасности в информационной сфере. Для совершенствования данной отрасли было даже сформировано отдельная наука, достаточно молодая «Информационное право», которая в свою очередь способствует развитию законодательства в данной сфере.

Чем же можно подтвердить, что государство достаточно активно участвует в реализации политики в области информационной безопасности на данный момент? Для того, чтобы ответить на данный вопрос, достаточно проследить ключевые новости начала текущего года, касающиеся обеспечения защиты от киберугроз в России, а именно:

---

[1] В Госдуму внесли законопроект о запрете анонимайзеров [Электронный ресурс] URL: https://meduza.io/news/2017/06/08/v-gosdumu-vnesli-zakonoproekt-o-zaprete-anonimayzerov-i-vpn

[2] М.А. Кудрявцев Стратегия развития информационного общества в России и основные направления развития информационного законодательства // Современное российское право: взаимодействие науки, нормотворчества и практики. Часть 3. XIII Международная научно-практическая конференция. «Проспект». 2018 г. С. 371.

1. Так, «В.В. Путин в своем обращении 21.02.2020 г. отметил рост угроз в сфере информационной безопасности. И призвал службу безопасности России уделить особое внимание защите критической инфраструктуры, а также предпринять меры по предупреждению кибератак и устранению последствий успешных проникновений в важные системы».[1]

2. «В.В. Путин в своем выступлении от 26.02.2020 поддержал идею нормы о кибербезопасности личности в Конституции РФ. Инициатива закрепления в Конституции специальной нормы, гарантирующей гражданам безопасность личности в цифровом пространстве, внесенная Андреем Макаровым, была одобрена».[2]

В современном мире киберпреступность достаточно острая проблема и борьба с ней выходит на одни из ключевых задач государства, но и даже приобретает мировой масштаб, так как атаки приобретают более глобальный характер. И те атаки на крупные корпорации, предприятия и государственные учреждения, данные атаки могут произойти когда и где угодно. Поэтому для предотвращения данных атак недостаточно издание нормативных актов, которые направлены на борьбу с этими угрозами, но, а также инициатива должна исходить и от тех субъектов, кто заинтересован в защите информации. Чтобы нормативные акты, которые принимаются в государстве, а также на международном уровне имели, какой-либо эффект.

Таким образом, всё вышеуказанное говорит о том, что государство активно ведёт работу, направленную на обеспечение информационной безопасности. И это положительный момент, так как развитие информационных технологий не остановится, изменения грядут во всех сферах жизни общества. Учитывая, что на сегодняшний момент активность пользователей сетью интернет с каждым днём увеличивается, вопросы конфиденциальности пользователей, защита информации на пространства

---

[1] Новости информационной безопасности. [Электронный ресурс] URL: https://www.anti-malware.ru/news/2020-02-21-111332/32041 (дата обращения 17.03.2020).

[2] Новости информационной безопасности. [Электронный ресурс] URL: https://www.anti-malware.ru/news/2020-02-26-111332/32074 (дата обращения 17.03.2020).

приобретает большое значение. Государство, которое сможет правильно выстроить государственную политику для обеспечения информационной безопасности. Такое государство, которое сможет обеспечить достойную защиту права граждан и предотвратить «информационную войну», сможет увидеть свои результаты не только в рамках обеспечения информационной безопасности, но и в рамках экономического развития государства, для формирования более развитого общества, обеспечив защищенное свободное информационное пространство. Кроме того необходимо повысить правовую грамотность населения, данные выводы можно констатировать на основание результатов тестирования (Приложение 1).

2 ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

2.1 Правовое регулирование информационной безопасности в Российской Федерации.

Правовое регулирование информационной безопасности является достаточно важным аспектом в обеспечение информационной безопасности. Для того, чтобы происходило развитие информационного общества необходимо развитие нормативно-правовой базы и использование новейших информационно-телекоммуникационных технологий.

Правовое регулирование информационной безопасности Российской Федерации прошло долгий путь перед тем, как обрести ту форму, которую обрела сейчас, легитимизация данных прав происходило достаточно долго. История информационной безопасности начинается задолго до XX века, однако в современной трактовке понятие «информация» в большинстве случаев неразрывно связано именно с применением компьютерных технологий в связи со стремительным развитием данной сферы во второй половине XX века, которое продолжается и на сегодняшний день.

Первыми из норм, которые содержали основные зачатки информационных прав и свобод имеются в Конституции СССР 1977 г. и в Конституции РСФСР 1978 г.. В данных правовых актах право на информацию не включались как самостоятельные права, а содержались как одни из элементов политических прав и свобод (такие как, свободы слова, печати, права на тайну переписки, телефонные переговоры и телефонные сообщения, и др.).

Формирование основных понятий информационных инфраструктуры в Российской Федерации шло своим путем в отличие от других зарубежных стран. Так одной из первой попыток защиты компьютерной информации, а также обеспечения безопасности компьютерных коммуникаций в Российской Федерации стало принятие Закона от 23 сентября 1992 г. № 3523-1 «О

правовой охране программ для электронных вычислительных машин и баз данных».[1] Но основополагающим законодательным актом в Российской Федерации с 1995 г. по 2006 г., который регулирует общественные отношения в информационной сфере, является Федеральный закон РФ «Об информации, информатизации и защите информации»,[2] основополагающим правовым актом, для которого явилась Конституция РФ 1993 года. Главными положениями, закрепляющиеся в Законе, включали в себя регулирование общественных отношений в вопросах формирования и использования информационных ресурсов, создание и использовании информационных технологий, защиты информации и др. (ст.1, п.1). При этом обеспечение национальной безопасности в сфере информации было как одно из основных направлений государственной политики в сфере информатизации (ст.3, п.2).[3]

Следующим этапом явилось принятие основополагающих нормативных актов, принятыми в Российской Федерации по регулированию информационной безопасности, являются федеральный закон «Об информации, информационных технологиях и о защите информации»[4], принятый в июле 2006 года и закон «О персональных данных».[5]

Любопытен, тот факт, что принятый закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149 -ФЗ, вызвал множество споров и дискуссий, которые продолжаются и по сегодняшний день. «Споры возникают, по поводу правовой природы информации - ключевого понятия в информационной сфере, так и необходимости правового закрепления целого ряда понятий и терминов,

---

[1] Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» от 23 сентября 1992 № 3523-1 // признан утратившим силу.

[2] Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ // СЗ РФ. 2006. № 31 (1 ч.). Ст.3451.

[3] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ// СЗ РФ. - 2006. - № 31 (ч.1). - Ст. 3448.

[4] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ// СЗ РФ. - 2006. - № 31 (ч.1). - Ст. 3448.

[5] Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ // СЗ РФ. 2006. № 31 (1 ч.). Ст.3451

которые широко применяются в информационной сфере, к числу таких можно отнести, такие как информационные ресурсы, информатизация и т.д. позиция законодателя не сформировалась по данным категориям и поэтому позиции ученых и правоприменителей разнятся».[1] Так, одним из примеров споров, вызванных применением норм Федерального закона «Об информации, информационных технологиях и о защите информации», явилось разграничение понятий: «конфиденциальность информации» и «конфиденциальная информация», в данном законе содержится понятие следующего содержания: «конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации».

В существующей формулировке Закона «Об информации» отсутствуют ссылки на документированность информации, на ограничения в доступе к этой информации.

Достаточно интересно мнение по этому поводу Конституционного суда Российской Федерации, так по ряду судебных актов, можно проследить переход от одной терминологии конфиденциальности информации к другой.[2]

В свою очередь понятие конфиденциальности информации включает в себя определенные признаки, а именно:

- обязательные для выполнения лицом, получившим доступ к определенной информации требования не передавать такую информацию третьим лицам;

---

[1] Чубукова С.Г. Стратегии развития информационного общества и направления развития законодательства // Правовая информатика. 2017. № 2. С. 69.

[2] Определение Конституционного Суда РФ от 18.01.2011 № 8-О-П «По жалобе открытого акционерного общества «Нефтяная компания «Роснефть» на нарушение конституционных прав и свобод положением абзаца первого пункта 1 статьи 91 Федерального закона «Об акционерных обществах»»; Постановление Конституционного Суда РФ от 29.11.2010 № 20-П «По делу о проверке конституционности положений статей 20 и 21 Федерального закона «О содержании под стражей подозреваемых и обвиняемых в совершении преступлений» в связи с жалобами граждан Д.Р. Барановского, Ю.Н. Волохонского и И.В. Плотникова» и т.д.

- согласие (несогласие) обладателя на передачу определенной информации третьим лицам.

Таким образом, в законодательстве определена обязанность одного субъекта и право другого субъекта, никак не взаимосвязанные с предметом правоотношения, что можно было бы связать с правовым режимом конфиденциальности информации.

Кроме того, необходимо отметить, что распоряжением Правительства Российской Федерации от 27 июля 2007 г. № 1003-р утвержден план подготовки проектов актов, которые необходимы для реализации Федерального закона.[1]

Достаточно, интересный факт был написан в работе Скиба А.В., который писал, что проекты нормативных правовых актов, направленных на их реализацию и внесение изменений в законодательство в связи с их принятием, проходят сложный процесс согласования и принятия. Нельзя не согласиться с тем, что в указанном Федеральном законе есть определенные преимущества перед предыдущим законом 1995 года «Об информации, информатизации и защите информации»,[2] который, конечно, за истекшее десятилетие нуждался в совершенствовании. «В ходе принятия этого закона, внесенный Правительством Российской Федерации законопроект претерпел существенные изменения(ко второму чтению было рассмотрено более 200 поправок к законопроекту). Изменено было не только название проекта, но и структура, возникли новые статьи, изменен их порядок, уточнены цели и сфера действия закона, внесены изменения в терминологический аппарат законопроекта (были уточнены определения понятий «информационные технологии», «обладатель информации», «доступ к информации» и другие), иначе, но отнюдь не бесспорно, сформулированы положения об информации

[1] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ // СЗ РФ. 2004. № 27. Ст. 2711.
[2] Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ // СЗ РФ. 1995. № 8. Ст.609. признан утратившим силу.

как объекте правового регулирования, а также скорректированы права и обязанности обладателя информации».[1]

В федеральный закон «Об информации, информационных технологиях и о защите информации» была включена норма, которая регулировала порядок функционирования государственных и муниципальных информационных систем на языках народов России. Скиба А.В. также отмечала в своей работе данный нормативный акт и указала, что «Несмотря на то, что базовый закон в информационной сфере уже вступил в силу - только его «жизнь», а иначе правоприменительная практика покажет, его положительные стороны, а также что в нем совершенно и нуждается в уточнении, и, наверное, это неизбежно в условиях такого быстрого развития информационных технологий, построения информационного общества». Я соглашусь с мнением Скиба А.В., мы не можем говорить о влияние нормативных правовых актов, которые вступили в силу в течение 2-3 лет, результаты будут проявляться по истечению нескольких лет.

Стоит отметить научную статью Андриашина Х.А. в которой он выделил блочную систему подразделения законодательства в рамках регулирования информационной безопасности, так он выделял 5 блоков:

1. Законодательство о средствах массовой информации (СМИ). Закон РФ от 27 декабря 1991 г. «О средствах массовой информации» [2] регулирует отношения, связанные с поиском, получением, производством и распространением массовой информации, под которой понимаются предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы. «Закон допускает создание и распространение средств массовой информации с использованием новых информационных технологий и устанавливает недопустимость цензуры и разглашения сведений, составляющих государственную и иную охраняемую

[1] Полякова Т.А. Базовые принципы как основные начала правового обеспечения информационной безопасности // Труды института государства и права Российской академии наук. 2016. № 3. С. 24.
[2] Закон РФ «О средствах массовой информации» от 27.12.1991 № 2124-1 // СЗ РФ. 2020.

законом тайну, регулирует организацию деятельности СМИ и их отношения с гражданами и организациями, политическими партиями и государственными органами».[1]

2. Законодательство о формировании информационных ресурсов, подготовки информационных продуктов, предоставлении информационных услуг. Важным правовым актом в этой области является ФЗ от 20 февраля 1995 г. «Об информации, информатизации и защите информации»,[2] который регулирует отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации.

3. Законодательство о поиске, получении, передаче и использовании информации основывается на конституционных нормах, закрепляющих право каждого свободно искать, получать, производить и распространять информацию любым законным способом, а также соответствующих положениях ФЗ «Об информации, информатизации и защите информации».[3]

4. Законодательство о средствах связи. «Формирование единого информационного пространства невозможно без средств связи, которые вместе со средствами вычислительной техники составляют техническую базу обеспечения процесса сбора, обработки, накопления и распространения информации. Отношения в области связи регулируются ФЗ от 16 февраля 1995 г. «О связи»[4], который определяет полномочия государственных органов, права и обязанности физических и юридических лиц в обеспечении пользователей средствами либо пользующихся услугами связи».[5]

---

[1] Трашкова С.М. Основы правового регулирования защиты информации в Российской Федерации // Вестник Восточно-сибирской открытой академии. 2014. № 16. С.1-13.

[2] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ // СЗ РФ. 2004. № 27. Ст. 2711.

[3] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ // СЗ РФ. 2004. № 27. Ст. 2711.

[4] Федеральный закон «О связи» от 7 июля 2003 г. № 126-ФЗ.

[5] Трашкова С.М. Основы правового регулирования защиты информации в Российской Федерации // Вестник Восточно-сибирской открытой академии. 2014. № 16. С.7.

5. Законодательство об информационной безопасности состоит из конституционных норм, Федеральных законов от 5 марта 1992 г. «О безопасности», от 19 февраля 1993 г. «О федеральных органах правительственной связи и информации» и других актов, «которые закрепляют правовые основы обеспечения безопасности личности, общества и государства, систему безопасности и ее функции, порядок организации и финансирования органов, занимающихся обеспечением безопасности, а так же контролем и надзором за законностью в сфере обеспечения безопасности».[1]

На мой взгляд, действительно было бы неплохо подразделить нормативно-правовые акты, которые регулируют информационную безопасность, на определенные группы, даже в рамках научного исследования, так как на законодательном уровне это сделать практически не возможно. Если будет проведена такой формы подразделение на группы, то возможно это бы помогло правоприменителям и законодательным органам, чтобы сориентироваться в каком направление лучше двигаться и где требуются изменения.

Следует отметить, что Россия достаточно прочно связана с международными правовыми актами и в период развития законодательства информационной безопасности, Российская Федерация ратифицировала большое количество международно-правовых актов, а также подписала большое количество международных договоров. Но проблемы информационной безопасности продолжаются, «одним из проявлений угроз является пропаганда терроризма и насильственный экстремизм, осуществляемый через Интернет-сайты, это одна из главных составляющих, с чем должно бороться государство в рамках осуществления информационной безопасности. Если на международном уровне приняты следующие акты:

---

[1] Трашкова С.М., Основы правового регулирования защиты информации в Российской Федерации // Вестник Восточно-сибирской открытой академии. 2014. № 16. С.1-13.

Европейская конвенция о пресечении терроризма от 27.01.1997;[1] Международная конвенция о борьбе с финансированием терроризма от 09.12.1999;[2] Международная конвенция о борьбе с бомбовым терроризмом от 15.12.1997;[3] Конвенция Совета Европы о предупреждении терроризма от 16.05.2005[4] и другие.

Скиба А.В. предложила достаточно интересную идею. В России следует реализовать некоторые правовые нормы, ограничивающие содержащие отрицательную информацию, коммуникационных и информационных услуг в интернете в соответствии с определенным набором признаков. Я соглашусь с данным мнением, на сегодняшний день имеется положительный опыт по законодательному регулирования функционирования системы жалоб на содержание информации, использование инструментов условного доступа с помощью кодов, шифров и паролей, а также функционирования системы сотрудничества саморегулируемых организаций провайдеров и пользователей с правоохранительными органами. Несомненный интерес представляют предложения о создании международного органа при ООН, координирующего управление в интернете, так называемой международной паутине, с учетом ее трансграничного характера.[5]

Таким образом, законодательство об информационной безопасности осуществляется путем отражения соответствующих положений в нормативных правовых актах, предусматривая различные виды ответственности за правонарушения в информационной сфере: за нарушение прав и свобод личности в сфере информации; недостоверность и ложность

---

[1] Международная конвенция о пресечении терроризма от 27.01.1977 (ETS N 90)// СЗ РФ. 2003. № 3. Ст. 202.

[2] Международная конвенция о борьбе с финансированием терроризма от 09.12.1999 // СЗ РФ. 2003. № 12. № 12. Ст. 1059.

[3] Международная конвенция о борьбе с бомбовым терроризмом от 15.12.1997 // СЗ РФ. 2001. № 35. № 12. Ст. 3513.

[4] Конвенция Совета Европы о предупреждении терроризма от 16.05.2005 // ратифицирована от 20.04.2006. СЗ РФ 2006. № 56.

[5] Скиба А.В. Развитие правового регулирования в области правового обеспечения информационной безопасности при построении информационного общества России // Актуальные проблемы государства, права и гуманитарных наук. 2015. С. 307.

информации, создаваемой и распространяемой СМИ; сокрытие, умышленное искажение информации об источниках угроз; незаконное использование персональных данных, незаконное получение и использование информации с ограниченным доступом; создание некачественных информационных технологий и средств обеспечения. Информационное законодательство в Российской Федерации нуждается в совершенствовании, те отношения, которые складываются в информационном пространстве, государство, на данный момент, не может организовать регулирование их.

2.2 Правовое регулирование информационной безопасности в зарубежных странах.

Новые технологии, электронные услуги стали неотъемлемой частью нашей повседневной жизни. «Учитывая то, что общество становится все более зависимым от информационных телекоммуникации и поэтому защита и доступность этих технологий становится критичным моментом и достаточно важной темой для национального интереса всего государства. Для каждой системы государственного управления актуальной является проблема качественных изменений в деятельности органов власти, то есть переформатирование системы управления с учетом механизма интересов управляемых и управляющих субъектов, который должен получить основание в законодательстве, в общественном сознании и политической культуре с государственных служащих и граждан».[1]

События последних лет, когда многие страны Западной Европы ввели свои ограничения, в виде санкций против России и тем самым Россия оказалась в санкционном режиме. Кроме того, случилось достаточно большое количество политических, военных кризисов в различных частях мира,

[1] Филатов В.В. Зарубежный опыт правового регулирования информационной безопасности // Wschodnioeuropejskie Czasopismo Naukowe (East European Scientific Journal). 2018. № 3(31). С. 69.

которые очередной раз доказали, что значение информационных систем безопасности и кибербезопасности достаточно велико.

На сегодняшний день, «необходимым условием развития информационного общества является кибербезопасность, за которой может стоять практически бесконечный список проблем безопасности и их решений, начиная от технических и заканчивая законодательными.

В современных условиях, вопросы кибербезопасности выходят из уровня защиты информации на отдельном объекте вычислительной технике на уровень создания единой системы кибербезопасности, как составной части информационной и национальной безопасности каждого государства.

Вместе с тем, на мировой арене политика информационной безопасности в том или ином государстве, обеспечивается путем принятия Стратегий кибербезопасности[1] и другими основными законами страны.[2]

Следует рассмотреть несколько ведущих страна, которые выстраивают свою политику информационной безопасности.

Итак, начнем с Германии. Германия ведет информационную политику, «которая основана на принципах транснационального обмена информацией, развития коммуникации в информационных систем, свободной конкуренции в информационной сфере, четкой правовой регламентации информационных правоотношений на разных уровнях. При этом, перспективным направлениями политики информационной безопасности Германии являются: становление информационного общества, создание информационных супермагистралей, информатизация государственного управления, либерализация государственного управления, либерализация коммуникаций, поддержка национальных производителей информационной продукции,

[1] Филатов В.В. Зарубежный опыт правового регулирования информационной безопасности // Wschodnioeuropejskie Czasopismo Naukowe (East European Scientific Journal). 2018. № 3(31). С.69.

[2] Щедрин Д.Н. Некоторые аспекты правового регулирования кибербезопасности на территории Российской Федерации и зарубежных стран // Инновационные тенденции развития российской науки. Часть II. [Электронный ресурс]: мат-лы XII междунар. науч.-практ. конф. молод. учен. (8-9апреля 2019 г.) / Краснояр. гос. аграр. ун-т. Красноярск, 2019. С. 324

развитие государственного и частного информационного бизнеса».[1] Выбранная стратегия информационной безопасности Германии, достаточно правильная, так как все концепции в этой сфере основаны на балансе интересов государства и гражданина и нашли правильное нормативно-правовое отражение. Следует отметить, что законодательство об информационной безопасности Германии состоит из ряда актов, которые регламентируются отдельные аспекты защиты информационных интересов государства и общества. Основными из них являются: Федеральный закон «О вещательной деятельности (Телемедиа)»[2], Федеральный Закон «Об охране персональных данных»,[3] Федеральный Закон «О порядке доступа к информации деятельности государственных органов и органов местного самоуправления», Федеральный Закон «О связи».[4]

Согласно германской стратегии кибербезопасности на федеральное правительство возлагается принятие мер на основе созданных структур, которые соответствуют определенным уровням угроз по стратегическим направлениям, в число которых входит международное сотрудничество, эффективная борьба с преступностью в киберпространстве. Происходит стремительное усиление возможностей правоохранительных органов, Федеральной службы безопасности в сфере ИТ и экономики в контексте преодоления ИКТ- преступности.

В рамках Национальной стратегии кибербезопасности 2016 г. указывается, что «с учетом глобальных технологий, международное сотрудничество, сконцентрированное на аспектах международной политики и безопасности носит обязательный характер».[5]

---

[1] Так же. С. 69

[2] Закон РФ «О средствах массовой информации» от 27.12.1991 № 2124-1 // СЗ РФ. 2020.

[3] Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ // СЗ РФ. 2006. № 31 (1 ч.). Ст.3451

[4] Германия. Законы. URL: http://www.wipo.int/wipolex/ru/profile.jsp? Code=DE (дата обращения: 14.02.2020).

[5] Cyber-Sicherheitsstategie fur Deutsthland 2016 URL: https://www.bmi.bund.de/cybersicherheitsstrategie-/BMI_CyberSicherheitsStrategie.pdf

Следующей, рассматриваемой страной является Великобритания. Информационная политика Великобритании основана на технологической нейтральности законов; «активизация международного сотрудничества в сфере защиты информации; поддержка и защита интересов пользователей компьютерных и телекоммуникационных систем; развитие электронной коммерции во всех сферах хозяйствования; развитие автоматизированных систем обмена научно-технической информацией. Подобная ориентация политики ориентация политики информационной безопасности позволяет согласовать общегосударственный и местный уровни защиты интересов государства в информационной сфере, поскольку возрастает функциональность механизмов информационной безопасности».[1]

Следует отметить, что в Великобритании принята национальная Стратегии кибербезопасности Великобритании 2016-2021.В данной стратегии даны ключевые понятия, в том числе понятие «Киберпреступность» - киберзависимые преступления, которые совершаются с использованием устройств ИКТ, которые являются инструментом и целью преступления, а также преступления, совершаемые с использованием кибер-средств без устройств на основе ИКТ. «Но стоит заметить, что данная Стратегия предусматривает не только понятии, цели и задачи, а включает в себя также программы по сдерживанию киберпреступности, также указан перечень лиц, кто может проводить кибератаки».[2] Достаточно интересно, то, что некоторые тезисы, которые были прописаны в данной стратегии, в последующем были подкреплены реальными примерами, произошедшими потом в реальной жизни. Так, в «Стратегии кибербезопасности Великобритании 2016-2021» указано в п.3.14 кем являются ««Скрипт-кидди» - как правило, дилетанты, пользующиеся скриптами или программами, разработанными другими, для

[1] Филатов В.В. Зарубежный опыт правового регулирования информационной безопасности // Wschodnioeuropejskie Czasopismo Naukowe (East European Scientific Journal). 2018. № 3(31). С.69.

[2] Национальная стратегия кибербезопасности 2016-2021 [Электронный ресурс].URL: https://government.ru (дата обращения:04.03.2020).

атаки компьютерных систем и сетей - не представляют серьезной угрозы для экономики или общества. Однако они имеют доступ к хакерским руководствам, ресурсам и инструментам через интернет. В силу уязвимостей систем с выходом в интернет, используемых многими организациями, действия «скрпит-кидди» могут, в некоторых случаях иметь непропорционально серьезные последствия для пострадавшей организации».[1] Ярким примером, который случился за последние пять лет, явилась атака на электронную сеть Украины. В итоге кибератаки на электрораспределительные предприятия «Прикарпатьеоблэнерго» и «Киеволэнго», произошедший 23.12.2015 г. отключение энергии, которая нарушила работу более 50 подстанций в распределительных сетях. Перерыв в регионе был нескольких часов, при этом другие жители и территории испытали менее значительные перерывы в электроснабжении, а без электричества осталось более 220 000 жителей. Некоторые пришли к выводу, что атака была произведена с использованием программы BlackEnergy3, после того как в сети были выявлены образцы данной программы. За шесть месяцев до атаки персонал энергокомпании получил фишинговое письмо от преступников, имеющие автоматические выключатели, что привело к прерыванию энергоснабжения. Вероятно, при помощи вредоносной программы, преступники получили и собрали учетные данные, с помощью которых они получили удаленный доступ к сети, которая способствовала отключению электроснабжения. Это первое происшествие, которое вывело из строя электрические сети с помощью кибератаке.

Далее рассмотрим правовое регулирование информационной безопасности в США. Одной из самых первых стран, начавших осуществление стратегического планирования в сфере кибербезопасности

[1] Щедрин Д.Н. Некоторые аспекты правового регулирования кибербезопасности на территории Российской Федерации и зарубежных стран // Инновационные тенденции развития российской науки. Часть II. [Электронный ресурс]: мат-лы XII междунар. науч.-практ. конф. молод. учен. (8-9апреля 2019 г.) / Краснояр. гос. аграр. ун-т. Красноярск, 2019. С. 324.

является Соединенные Штаты Америки. «Первая национальная доктринальная инициатива, котрая опередилила необходимоть координации различных ведомств государства в сфере национальной защиты информационного пространства, утвержденная в США в феврале 2003 г.»[1] International Strategy for cyberspace (Prosperity, Security and a Networked World)[2] (Международная стратегия по действиям в киберпространстве) которая раскрывает видение будущего киберпространства и план сотрудничества между странами и народами с целью его реализации.

International Strategy for cyberspace это документ который определяет, что в США планируется противостояние тем, кто пытается разрушить сети и системы, также содержаться нормы о сдерживание злоумышленников, при которым сохраняются важные активы необходимыми и адекватными методами.

Основная сущность стратегии США является, то что она призывает другие государства присоединится к ней, для того чтобы реализовать совместные цели, а именно реализовать идеи процветания, безопасности и открытости не только в США, но и во всем мире.

Большой интерес вызывает норма International Strategy for cyberspace обеспечивающая открытость и безопасность киберпространства и те средства, которые использует США для достижения своих целей. Согласно этой норме США может применять для обеспечения безопасности не только экономические, дипломатические и информационные средства, но и также возможно вмешательство вооруженных сил США.

---

[1] Корсаков Г.Б. Информационное оружие супердержавы: кибервойна и «управляемые кризисы» // Военно-политическое образование [Электронный ресурс] http://www.belvpo.com/ru/10497.html (дата обращения: 26.02.2020).

[2] International Strategy for cyberspace (Prosperity, Security and Openness in a Networked World [Электронный ресурс] URL: https:whitehouse.gov/sites/default/rss_viewer/international_strategy_for_cyberspace.pdf. (дата обращения: 04.03.2020).

Кроме того в законодательстве Соединенных Штатах Америки содержатся другие нормативно-правовые акты, регламентирующие правоотношения в сфере информационной безопасности.

Одним из основных законов США информационной безопасности является закон Electronic Communications Privacy Act of 1986 (Электронный Закон о конфиденциальности электронных коммуникаций 1986 года, ECPA).[1] Данный закон содержит 3 раздела. Первый раздел закона ECPA, включает в себя нормы, защищающие данные в процессе, а также устанавливает требования по производству обысков. Второй же раздел ECPA содержит в себе другой нормативный акт the Stored Communications Act of 1986 (Закон о хранении контактов), который целенаправлен на сохранение коммуникаций, базы информации, сообщений, находящиеся в компьютерах. Раздел третий ECPA включает в себя запрет на использования записей и регистрационных данных, устройства трассировки, маршрутизации, адресации и передачи сигнальной информации, без постановления суда.

Stored Communications Act of 1986[2] (Закон о хранении контактов (SCA)) о данном законе говорилось выше, SCA планирует добровольного процедуру или раскрытия хранящихся проводных и электронных сообщений и транзакционных записей, являющиеся собственностью провайдеров интернет-услуг (ISP). SCA определяет возможности Правительства США по предупреждению к раскрытию информации, а также предусматривает две категории услуг:

- Electronic communication service (услуга электронной коммуникации) и
- Remote computing service (дистанционное компьютерное обслуживание).

Также закон Stored Communications Act of 1986 регламентирует деятельность в тех случаях, когда электронные данные сохраняются за

---

[1] Electronic Communications Privacy Act of 1986 [Электронный ресурс] URL: https:law.comell.edu/uscode/text/18/2510.

[2] Stored Communications Act [Электронный ресурс] URL: www.law.cornell.edu/uscode/text/18/2701

пределами границ, оказывающиеся под юрисдикцию США, в связи с тем, что многие Интернет-провайдеры имеют распространенные по всему миру центры и сервера обработки данных.[1]

Интересен факт применения закона SCA на практике. Так, рассматривалось дело Microsoft Corporation vs United States of America, в связи с тем, что государственные органы 4 декабря 2013 года получили ордер на розыск определенной учетной записи электронной почты, регулируемой и поддерживаемой Microsoft Corporation. Представитель Microsoft указал, что требуемое данные хранятся на сервере в Ирландии, в связи с чем Microsoft подала ходатайство об аннулировании ордера, в связи с его административно-территореальным применением. Однако ходатайтельство было отклонено судом и на основании SCA, предписание было объяснено как коллизия, которая выполняется как повестка в суд. Апелляционный суд 14 июля 2016 года второго округа США было вынесено решение в пользу Microsoft, поскольку положения SCA не могут использоваться экстерриториально.[2]

Другой прецедент «Robbins vs. Lower Merion School District связан с тем, что в 2010 году средние школы Филадельфии шпионили за учащимися путем скрытной и удаленной активации веб-камер, встроенных в ноутбуки учащихся школы, которые те использовали у себя дома, тем самым нарушалось право на частную жизнь учащихся. Школы признали виновными в осуществлении более 66000 вебшотов и скриншотов, в том числе в спальнях учащихся».[3]

Таким образом, рассмотренные страны имеют свои специфические особенности правового регулирования информационной безопасности. И каждая страна, рассмотренная выше достойна внимания, в каждой концепции правового регулирования информационной безопасности имеются

---

[1] Улин В.М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом. Монография // М.:. 2016

[2] Microsoft Corp. против Соединенных Штатов. – Microsoft Corp. v. United States. [Электронный ресурс] URL: https://ru.qwe.wiki/wiki/Microsoft_Corp._v._United_States

[3] Robbins v. Lower Merion School District. [Электронный ресурс] URL: https://en.wikipedia.org/wiki/Robbins_v._Lower_Merion_School_District

положительные и отрицательные стороны. Необходимо учесть опыт развития различных стран в данной сфере для недопущения ошибок, как в государственной политики, так и правовом регулирование информационной безопасности своей страны. Государство должно разрабатывать политику, направленную на обеспечении информационной безопасности, также издавать нормативно-правовые акты для ускорения совершенствования этой сферы.

2.3 Международно-правовое регулирование информационной безопасности.

«Обеспечение информационной безопасности современных государств, в тех условиях, которые стали уже обыденностью, стало одно из приоритетных задач не только государства, но и основной задачей на международном уровне. Человечество находится в такой ситуации, когда военные действия могут вестись не только на земле, море, в воздухе или в космосе, но и на совершенно новой площадке, информационной. Так называемая «информационная война», которая подразумевает воздействие на сознание человека, так как это не запрещено на международном уровне и это в свою очередь дает возможность технически развитым странам использовать свои информационные технологии против других государств. Поэтому особое место в системе международной безопасности на сегодняшний день занимает именно информационная безопасность».[1]

«Международная информационная безопасность в полной мере зависит от информационного пространства. Информационное пространство - это сфера деятельности, которая связана с хранением информации, использованием, созданием, формированием, преобразованием, передачей

[1] Айдашева Л.Г. Информационная война, как основная проблема международно-правового регулирования информационной безопасности // Наука сегодня задачи и пути их решения. 2020. С. 142.

информации и оказывает воздействие, как на индивидуальное, так и общественное сознание».[1]

Важным компонентом национальной безопасности служит информационная составляющая. «В силу своей многогранности информационная безопасность затрагивает различные сферы общественной жизнедеятельности. Она является неотъемлемой частью военной безопасности и не замыкается в ее рамках. Информационная безопасность не ограничивается сугубо техническими и технологическими параметрами (информационно-технологическая безопасность)».[2]

Как отмечал в своей работе Костенко Н.И. «Обеспечение информационной безопасности любого взятого государства на национальном уровне, неотделимо от обеспечения её на международном уровне».[3] Да, я полностью согласна с данным мнением, ведь действительно, обеспечение международной информационной безопасности основывается на то том, как каждое отдельное государство обеспечивает свою информационную безопасность, как организована деятельность его органов, также юридических и физических лиц, в указанной сфере.

Для того, чтобы подробно разобраться о значение функционирования международного права в сфере информационной безопасности, для этого необходимо определить несколько важных моментов:

1. «Международное право является разновидностью социальной информации. В своих нормах и принципах оно аккумулирует сведения о системе международных отношений. Информация, накопленная системой международно-правового регулирования, передает от поколения к поколению достижения в области организации международных отношений, и тем самым

---

[1] Капустин А.Я. Угрозы международной информационной безопасности формирование концептуальных подходов // Журнал российского права. 2015. № 8. С. 92.
[2] Марков А. Некоторые аспекты информационной безопасности в контексте национальной безопасности // Вестник СПбУ. №12 С. 47.
[3] Костенко Н.И. Международная информационная безопасность в рамках международного права (методология, теория) // Russian journal studies. 2018. № 4 (17) С. 13.

служит одним из факторов обеспечения нормального функционирования и развития их системы.

2. Международное право является важным средством коммуникации и общения государств и других субъектов международного права.

3. Актуальность информационного подхода к исследованию международного права обусловливается местом и ролью, которую играет правовая информация в механизме международно-правового регулирования. Действенность международно-правовых норм основного элемента правового регулирования - зависит от качества и количества содержащихся в них информации».[1]

Большую роль играет развитее информационных отношений и усовершенствование данных норм.

Прогресс в развитии законодательства в информационной сфере, как в целом, так и в области обеспечения информационной безопасности, было принято и провозглашено 10 декабря 1948 г. Генеральной ассамблеей ООН Всеобщей декларации прав человека,[2] имеющий смысл аспект данного законодательного акта, является то, что было установлено в статьях 12,19,26 права каждого человека на мысли, религии, свободу убеждений, право на образование, совести и на свободное выражение этих убеждений. Также право получать, распространять и искать информацию и идеи любыми средствами, которые не ограничены законом, независимо от территорий государства.

Государственные отношения находятся в области обмена информации и всегда под влиянием принципов и норм межнационального права, регулирующиеся на международным уровне. «Данных документов, регулирующих эти отношения достаточно большое количество, но одними из основных из них являются: Конвенция о борьбе с распространением порнографических изданий 1923 г., Международная конвенция об

[1] Середа В.В., Карась А.Ю. Международный обмен информацией в рамках международно-правового регулирования // Научные стремления. 2015. № 4 (16). С. 68

[2] Права и свободы личности./ Библиотечка «Российской газеты» совместно с библиотечкой журнала «Социальная защита» М. 1995. №. 11. С. 45

использовании радиовещания в интересах мира 1936 г., Соглашение об облегчении международных обменов визуальными и звуковыми материалами образовательного, научного и культурного характера 1948 г., Соглашение о ввозе материалов просветительного, научного и культурного характера 1950 г., Конвенция о международном обмене изданиями 1958 г., Конвенция об обмене официальными изданиями и правительственными документами между государствами 1958 г., Регламент радиосвязи Международного союза электросвязи 1979 г. (последняя редакция от 2002 г.), Международная конвенция электросвязи, а также ряд международных соглашений в области авторского права».[1]

«На сегодняшний день, мировое сообщество, доверившись многим объектам инфраструктуры вычислительных систем, оказалось беззащитно перед прямыми угрозами. Цель прямых угроз - это уничтожение жизненно важных объектов без применения военной боевой силы».[2] Но, а также следует отметить, что в каждом государстве идет усиление деятельности спецслужб, которые осуществляют разведывательную деятельность в отношении государственных органов, различных научных организация, а также предприятий оборонно-промышленного комплекса и вооруженных сил государства.

Т.А. Полякова и А.В.Морозова считаю, «что деятельность государств в информационном пространстве должна гарантировать свободу технологического обмена и свободу обмена информацией с учетом уважения суверенитета государств, существующих политических, исторических и культурных особенностей».[3]

В данный момент партнерство по вопросам между государствами об межнациональной информационной безопасности, которое осуществляется в

---

[1] Лукашук И.И. Международно-правовое регулирование международных отношений (системный подход) // М., 1975. С. 10.

[2] Костенко Н.И. Международная информационная безопасность в рамках международного права (методология, теория) // Russian journal studies. 2018. № 4 (17) С. 14.

[3] Морозова А.В., Полякова, Т.А. Организационно-правовое обеспечение информационной безопасности // М.: РПА Минюста России. 2013. С. 251.

форме международных договоров. «Так, например, 08.05.2015 между Правительством Российской Федерации и Правительством Китайской Народной Республики было подписано Соглашение о сотрудничестве в области обеспечения международной информационной безопасности. В преамбуле данного Соглашения подтверждается, что государственный суверенитет и международные нормы и принципы, вытекающие из государственного суверенитет, распространяются на поведение государств в рамках их деятельности, связанной с использованием информационно-коммуникационных технологий, а также юрисдикцию государств над информационной инфраструктурой на их территории. В то же время государство имеет суверенное право определять и проводить государственную политику по вопросам, связанным с информационно-телекоммуникационной сетью Интернет, включая обеспечение безопасности».[1]

Также стоит обратить внимание на основании данного соглашения. Основная угроза в рамках обеспечения международной информационной безопасности принимается использование информационно-коммуникационных технологий для осуществления актов агрессии, направленных на нарушение суверенитета, безопасности, территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

Одной из особенностей Соглашения является то, что страны, подписавшие данный документ, обмениваются информацией о возможных рисках и угрозах, которые могут возникнуть в сфере информационной безопасности, а также должны осуществлять взаимодействие для того, чтобы совершенствовать международно-правовую базу сотрудничества в сфере информационной безопасности.

Следующий один из важных документов является Стратегия сотрудничества государств, утвержденная решением Совета правительств

[1] Костенко Н.И. Международная информационная безопасность в рамках международного права (методология, теория) // Russian journal studies. 2018. № 4 (17) С. 14.

СНГ 28.10.2016. В данном документе страны-участницы выбрали путь развития в целях построения нового информационного общества, данная Стратегия предусмотрена до 2025 года и также разработали план действий для того, чтобы реализовать данную стратегию. «Из Стратегии усматривается, что использование информационно-коммуникационных технологий является одним из приоритетов и необходимым условием повышения качества жизни граждан, развития экономической, социально-политической и культурной сфер жизни общества, а также совершенствования системы государственного управления».[1]

Примечательным моментом является то, что 11.07.2014 г. Президент РФ В.В. Путин посетил с официальным визитом Республику Куба, в рамках данной поездки был подписан двухстороннее межправительственное Соглашение о сотрудничестве в области обеспечения международной информационной безопасности. Данное Соглашение принесло достаточно весомый вклад в развитие международных отношений в сфере информационной безопасности. Когда был подписано Соглашение, это стало отправной точной для формирования общих взглядов к проблеме международной информационной безопасности. Отношения между Россией и Кубой вышли на новый уровень в области обеспечения международной информационной безопасности. Были обсуждены важные направления работы такие, «как выработка совместных мер по развитию норм международного права в области ограничения распространения и применения информационного оружия, разработка и осуществление совместных мер доверия, формирование согласованной политики в области ограничения распространения и применения информационного оружия, разработка и осуществление согласованной политики в области международной информационной безопасности, обеспечение информационной безопасности, обеспечение информационной безопасности критически важных объектов,

[1] Костенко Н.И. Международная информационная безопасность в рамках международного права (методология, теория) // Russian journal studies. 2018. № 4 (17) С. 14.

борьба с использованием информационно-коммуникационных технологий и террористических и иных преступных целях, содействие обеспечению безопасного, стабильного функционирования и интернационализации управления сетью Интернет».[1]

Таким образом, на сегодняшний день разработано и принято большое количество нормативно-правовых актов на международном уровне регулирующих информационную безопасность в целом мире. В мире не установилось, какой-то определенного способа закрепления правовых актов, которые регулируют информационную безопасность, но сложилась тенденция закреплений соглашения между несколькими стран. Это достаточно хороший способ установления контакт между странами для того чтобы совместно бороться с информационными угрозами.

[1] Костенко Н.И. Международная информационная безопасность в рамках международного права (методология, теория) // Russian journal studies. 2018. № 4 (17) С. 9-16

3 СОДЕРЖАНИЕ ГОСУДАРСТВЕННОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1 Органы государственной исполнительной власти в сфере информационной безопасности

В 2009 г. заместитель начальника Генерального штаба Вооруженных Сил Российской Федерации генерал-полковник Анатолий Ноговицын отметил, что развитые страны скоро будут иметь возможность в участвовать в масштабных информационных войнах, он отметил, что основная задача в этих войнах будет дезорганизация функционировании ключевых административных, военных, промышленных объектов и систем противника, а также психологически-информационного влияние на его политически-военного руководство, население и войска, прежде всего с использованием современных информационных технологий и средств. «Ноговицын выделяет ряд характерных черт информационной войны, которые отличают ее от других форм ведения военных действий, ставят новые проблемы перед ее участниками и заслуживают особого внимания. Основной из них являются незначительные затраты на разработку и применение информационного оружия, так как стоимость разработки высококачественных средств ведения информационной войны относительно невелика и доступна широкому кругу ее участников, повышение роли управления восприятием. Разрабатываемые средства «информационной войны» могут стать совершенно новым мощным инструментом манипуляции восприятием».[1] Да, действительно, на сегодняшний день одни из лидирующих позиций занимают государства, в которых достаточно хорошо развиты информационные технологии.

Общество не стоит на месте, он постоянно находится в развитие, но и с этим возрастает количество угроз, как уже говорилось выше,

[1] Бегишев И.Р. Информационное оружие как средство совершения преступлений // Информационное право. 2010. № 4. С. 24.

информационные грозы занимают одно из ведущих в списке потенциальных угроз. Для того, чтобы предотвратить данную угрозу, необходимо обеспечить на общегосударственном уровне информационную безопасность. Для достижения данной цели, для более успешной организации информационной безопасности необходимо организовать правильную работу органов осуществляющих и регулирующих информационную безопасность, не только на федеральном уровне, но и на уровне субъектов. Безусловно, каждый район обладает своими особенностями, для более слаженной и эффективной работы необходимо учесть данные о том регионе, в котором обеспечивается информационная безопасность.

Когда в отношении России появились международные санкционные меры со стороны других государств, это стало толчком для принятия определенных решений и проведения изменений в различных сферах: в здравоохранении, науки, транспорта, различных финансовых секторов и других областях, но ключевую роль занимает информационная безопасность.

«Основными субъектами, осуществляющими деятельность по обеспечению информационной безопасности, являются федеральные органы государственной власти, которые обладают специальными полномочиями в рамках закрепленного правового положения, и выполняемыми в соответствии с ним функциями. Важное место в системе федеральных органов государственной власти, обладающих полномочиями в области обеспечения безопасности информационной безопасности, занимают: Президент РФ, Правительство РФ, Федеральная служба безопасности России».[1] Когда был принят Федеральный закон № 187 - ФЗ от 01.01.2018 г. «О безопасности критической инфраструктуры»[2] данный акт увеличил полномочия

---

[1] Михнев И.П., Михнева С.В., Махова А.А., Лапшина А.Р. Полномочия Федеральных органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры // Юридические науки. Вестник Алтайской академии экономики и права. 2019. № 1.Ч 2. С.206.

[2] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ // Российская газета. 31 июля 2017. № 7333 (167).

федеральных органов власти. Так с произошедшими изменениями, которые были внесены вышеуказанным федеральным законом, в число полномочии ФСБ России дополнили следующими: создание и функционирование государственной системы обнаружения, предотвращения и ликвидации компьютерных атак и образование Национального координационного центра по компьютерным инцидентам, цель которого заключается в координировании мероприятий по реагированию на компьютерные инциденты и непосредственное участие в таких мероприятиях, организация и осуществление обмена информацией о компьютерных инцидентах между субъектами информационной безопасности, а также между субъектами и уполномоченными органами иностранных государств, международными организациями.

Правовое положение органов государственной власти представляет собой определенное место данных государственных субъектов в системе государственного и муниципального управления, выраженное совокупностью прав и обязанностей, а также полномочия данного органа в рамках осуществления задач государства.

Муниципальное и государственные управление России демонстрируют собой три уровня распределения органов государства и местного самоуправления. Распространение государственной власти РФ на федеральном и на субъективном уровне федерации. Следуя принципам разделения властей, различают исполнительные, судебные и законодательные (представительные) органы власти государства на федеральном и на региональном уровне. Согласно статье 12 Конституции РФ, органы местного самоуправления не входят в систему органов государственной власти. «Учитывая важность сферы безопасности критической информационной инфраструктуры, основные функции по обеспечению ее безопасности отводятся федеральной власти, прежде всего Президенту РФ, Правительству РФ, ФСБ России и ФСТЭК России. В целях оптимального распределения и определения функций, полномочий, прав и обязанностей данных органов,

исключения их дублирования законодатель закрепляет понятие критической информационной инфраструктуры».[1]

Деятельность и полномочия каждого составного элемента регулируется нормами закона. Так в данной области регулируются полномочия нормами Конституции РФ, а также дополнительно нормами положения Доктрины. Но учитывая это, на практике разграничение затрудняется ввиду наличия реальных возможностей у властей регионе проводить политику информационной безопасности в соответствии с установленными федеральным законодательством приоритетами, особенно учитывая возможный недостаток опыта подобной деятельности на уровне регионов.

Первостепенную роль нужно отметить ряд полномочий Президента РФ в обеспечении информационной безопасности. Так Президент РФ вырабатывает основу государственной политики по обеспечению информационной безопасности, а также определяет два федеральных органа исполнительной власти - орган, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры и орган, обеспечивающий функционирование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, порядок создания и задачи этой системы.[2]

Если рассматривать полномочия Правительства РФ по обеспечению информационной безопасности, то в общем виде оно осуществляет категорирование, контроль, интегрирование электросвязи. «Таким образом, можно выделить 3 основные направляющие:

---

[1] Михнев И.П., Михнева С.В. Обеспечение безопасности критической инфраструктуры информационной инфраструктуры: полномочия федеральных органов государственной власти // Актуальные проблемы менеджмента, экономики и экономической безопасности. 2019. С. 276.

[2] Михнева С.В., Михнев И.П., Чернова А.П. Правовые основы определения юридического положения должностных лиц местного самоуправления и муниципальных служащих в Российской Федерации. // В сборнике: Социально-экономические и правовые основы инновационного развития: сборник научных статей. Пенза. 2018. С. 109.

1) по категорирования -установление данных факторов и критериев значимости объектов критической информационной инфраструктуры с их значениями, а также порядок и сроки осуществления их категорирования;

2) определение порядка и процедуры осуществления госконтроля в области безопасности информационной инфраструктуры;

3) налаживание единой сети электросвязи РФ для функционирования объектов информационной инфраструктуры».[1]

Если провести анализ правовых актов, которые закрепляют и регулируют компетенции и полномочия государственных органов по обеспечению информационной безопасности, то можно их подразделить на 2 группы. Итак, по сфере деятельности выделяют 2 группы федеральных органов, осуществляющие обеспечение информационной безопасности. Первый орган - это Федеральная служба безопасности (ФСБ), он осуществляет функционирование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. Второй орган - Федеральный орган по техническому и экспертному контролю (ФСТЭК) в его полномочия входит обеспечение безопасности критической информационной инфраструктуры.

Правовое положение Федерального органа по техническому и экспертному контролю предусматривает собой, то, что данный орган несет ответственность за ведение реестра объектов КИИ, а также осуществляет проверочную деятельность за правильностью категорирования объектов критической информационной инфраструктуры. В свою очередь, правовое положение ФСБ устанавливает полномочия данного органа, связанные с порядком реагирования на компьютерные инциденты, осуществляет разработку требований к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак.

---

[1] Михнев И.П., Михнева С.В., Махова А.А., Лапшина А.Р. Полномочия Федеральных органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры // Юридические науки. Вестник Алтайской академии экономики и права. № 1.Ч 2. 2019. С.206.

Согласно Указу Президента РФ от 25.11.2017 № 569 было установлено, что федеральным органом исполнительной власти, который уполномочен осуществлять в области обеспечения безопасности критической информационной инфраструктуры - Федеральную службу технического и экспертного контроля России. «Данный орган обладает следующими полномочиями в рассматриваемой сфере: ведет реестр объектов критической информационной инфраструктуры; устанавливает требования по обеспечению их безопасности и к созданию систем безопасности их функционирования; разрабатывает меры совершенствования правового регулирования в области обеспечения безопасности критической информационной инфраструктуры и предлагает их Президенту РФ и Правительству РФ; утверждает форму соответствующих документов; осуществляет государственный контроль в области информационной безопасности».[1]

Указом Президента РФ от 15 января 2013 г. № 31 «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ», создание государственной системы предупреждающая о компьютерных атаках, контролируемая степень защищенности информационной инфраструктуры РФ.

При этом до сих пор не было однозначного понимания, кто должен конкретно подключиться к этой системе. Теперь четко закреплено законом, что должны подключиться к системе ГосСОПКА все субъекты критической информационной инфраструктуры. Таким образом, одной из ключевых идей принятия ФЗ № 187 являлось создание единого центра, которые осуществлял бы мониторинг и управление информационной безопасности в государстве. Так, ранее на ФСБ были возложены полномочия по содержанию системы

[1] Михнев И.П., Михнева С.В., Махова А.А., Лапшина А.Р. Полномочия Федеральных органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной // Юридические науки. Вестник Алтайской академии экономики и права. 2019. № 1.Ч 2. С.206.

обнаружения, предупреждения компьютерных атак на информресурсы России (информсистемы и информационно-телекоммуникационные сети), ликвидации данных атак. Теперь решено возложить на ФСБ функции по созданию ГосСОПКА.

Ещё одним Указом Президента РФ от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ» возложены на Федеральную службу безопасности функции федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы выявления компьютерных атак. «В связи с чем, полномочиями ФСБ в этой сфере является: обеспечение и контролирование данной системы, научно-техническая политика в этой сфере, разработка документации по обеспечению безопасности с использованием суперкомпьютерных и грид-технологий, проведения экспертных криптографических и специальных средств. Также в полномочия ФСБ входит: создание Национального координационного центра по компьютерным инцидентам, координация деятельности субъектов информационной инфраструктуры компьютерным атакам, оценка уровня безопасности информационной инфраструктуры».[1]

Для того, чтобы более детально рассмотреть данный вопрос, необходимо рассмотреть на примере, одного из региональных субъектов. Рассмотрим Северо-Западный федеральный округ, данный округ был выбран не случайно. Северо-Западный федеральный округ граничит с такими странами, как: Латвия, Литва, Норвегия, Эстония, Польша, страны блока НАТО, данные страны всегда будут представлять угрозу, так как обладают передовыми техническими средствами ведения разведки и управления. Угрозы, которые существуют на сегодняшний день в информационной сфере,

[1] Михнев И.П., Михнева С.В., Махова А.А., Лапшина А.Р. Полномочия Федеральных органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры // Юридические науки. Вестник Алтайской академии экономики и права. № 1.Ч 2. 2019. С.207.

в первую очередь направлены на дизбалансирование деятельности органов государственной власти.

Примечательно, то, что на территории Северо-Западного федерального округа расположены важные части стратегического командования Минобороны Российской Федерации. Большое количество защищаемых объектов расположены непосредственно в пределах данного округа и вызывают большой интерес у различных подразделений разведки.

«Наибольшую угрозу для государственных информационных систем Северо-Западного федерального округа представляет техническая компьютерная разведка, реализованная в системе электронного наблюдения PRISM, созданной Агентством национальной безопасности США для сбора информации с крупнейших интернет-сервисов, включая электронную почту, поисковые запросы, разговоры в Skype, мобильные приложения, транзакции в системах Visa и MasterCard».[1]

Государственное регулирование информационной безопасности осуществляется путем установления конкретных требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Так согласно, Федеральному закону РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» защита информации «представляет собой принятие правовых, организационных и технических мер, направленных на: обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение

[1] Кучерявый М.М., Косов Ю.В., Вовенда Ю.В. Деятельность органов государственной власти Северо-Западного федерального округа по обеспечению безопасности информации // Управленческое консультирование. 2017. № 10. С. 11.

конфиденциальности информации ограниченного доступа; реализация права на доступ к информации».[1]

В рамках обеспечения информационной безопасности в Северо-Западном федеральном округе сформирована система защиты информации, которая охватывает все ветви и уровни органов власти для своевременного реагирования на возникающие угрозы.

Так общее руководство деятельностью по осуществлению информационной безопасности возложены на полномочного представителя Президента РФ, а также на Межведомственный совет по осуществлению защиты информации. В субъектах Российской Федерации - главы высших органов исполнительной власти субъектов российской Федерации и комиссии по защите информации.

В свою очередь, управление Федеральной службы по техническому и экспертному контролю (ФСТЭК) по Северо-Западному Федеральному округу осуществляет реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1. обеспечения безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;

2. противодействия иностранным техническим разведкам на территории российской Федерации;

3. обеспечения защиты информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным

[1] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ // СЗ РФ. 2004. № 27. Ст. 2711.

доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носителей информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;

4. защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

5. осуществления экспертного контроля.[1]

После того, как была проведен контроль органов государственной власти Севера-Западного федерального округа по показателям, которые были получены, видно, то, рекомендации нормативно и методических документов ФСТЭК России выполняются не в полной мере, что в свою очередь приводит к допущению серьезных нарушений безопасности в информационной сфере.

Одними из главных нарушений, которые были выявлены, можно подразделить на следующие группы:

1. уполномоченные должностные лица субъектов РФ не должным образом осуществляют руководство системой информационной безопасности;

2. специалисты, назначаемые на должность, в большинстве случаев не имеют должного профильного высшего образования, а и не прошедших переподготовку и повышение квалификации;

3. проблемы с финансированием для приобретения лицензионного и сертифицированного информационно коммуникационного оборудования;

4. назначение на должности специалистов по защите информации без соответствующего согласования с Управлением ФСТЭК России по Северо-Западному федеральному округу.

Проведенная оценка говорит нам о том, что произошло ослабление контроля со стороны руководства регионов, организаций и учреждений.

---

[1] Сведения о полномочиях ФСТЭК России; перечень нормативных правовых актов, определяющих эти полномочия // ФСТЭК России [Электронный ресурс]. URL: http://fstec.ru/obshchaya-informatsiya/polnomochiya (дата обращения: 07.03.2020).

Не принимаются меры по устранению нарушений и недостатков, которые были выявлены в предыдущих проверках.

Как показывает статистика, наибольшее количество нарушений связано с плохой организацией работы и несоответствующим уровнем профессиональной подготовкой специалистов.

Система органов государственной власти и управления в Северо-Западном федеральном округе является центральным и связующим звеном по обеспечению информационного противоборства в регионе.

В этой связи большое значение имеет обеспечение защиты информации в государственных информационных системах.

Стоит признать, что информационные системы органов власти обрабатывают большое количество информации, которая имеет большое значение для деятельности государства и региона, а также в социальной сфере, здравоохранении и образовании, раскрытие которой может привести к нежелательным, негативным последствиям и общественному резонансу.

Проблема обеспечения информационной безопасности, достаточно актуальна на сегодняшний день и активно развивается. Но мы не можем говорить о том, что современное состояние государственного и общественного обеспечения информационной безопасности на должном уровне, как и развитие информационных технологий. Анализируя тенденции положений нормативно-правовых актов, можно выделить следующие направления государственного аппарата: так Президент РФ осуществляет разработку основ государственной политики в сфере информационной безопасности, в свою очередь законодательные органы законодательной власти определяют нормативную основу политики государства в этой сфере, законодательно закрепляют правовое положение основных субъектов критической информационной инфраструктуры, их права, обязанности и ответственность; а исполнительная власть определяет ключевые исполнительные органы, отвечающие за информационную безопасность, и обеспечивает непосредственно сам процесс защиты значимых объектов

критической информационной инфраструктуры и ликвидации компьютерных атак.

Таким образом, всем субъектам информационной инфраструктуры нужно провести массу продолжительных по времени мероприятий для того, чтобы создать эффективную системы безопасности. Создаваемые системы национальных органов в рамках осуществления информационной безопасности, организациям и должностным лицам, должны предъявляться требования: компетентности, независимости, беспристрастности.

3.2 Принципы государственного регулирования информационной безопасности

Обеспечение информационной безопасности каждого государства требует, прежде всего, реализации некоторых задач. Когда государство определяет цели, задачи, принципы обеспечения информационной безопасности страны даст возможность для формирования определенных границ для достижения цели информационной безопасности и важным элементом данной системы. Информационная безопасность должна является связующим звеном между политикой национальной безопасности и информационной безопасности, то важно проводить ее по единым принципам, общим и для национальной безопасности, и для информационной политики.

Определение базовых принципов в рамках государственного регулирования информационной безопасности является основополагающим началом, ввиду того что они способствуют развитию правовой системы государства, тем самым определяя основу правовой политики в сфере информационной безопасности. Так, В.В. Лапаева в своей работе отмечает, что «в рамках такой трактовки правовой политики право представляет

одновременно и как цель и как средство ее достижения»».[1] А в свою очередь, В.С. Нерсесянц, утверждает следующее: «правовая политика - это государственная политика в области развития права (внутреннего и международного), стратегии и тактики правового пути развития общества, государства, страны, система идей, принципов, норм, форм и процедур признания, осуществления и развития начал и требований господства права в общественной и государственной жизни.[2]

Если рассматривать принципы непосредственно связанные с обеспечением информационной безопасности, с учётом представленных в Доктрине информационной безопасности РФ, а также с учетом выделенных принципов в учебной литературе, то можно указать на следующие основополагающие принципы информационной безопасности:

1. Принцип системности - основной, требующий учёта всех возможных угроз и рисков, хотя в полной мере учесть все невозможно. Поэтому нужно абстрагирование от мелких деталей, но с учетом воздействия этих деталей на систему в целом.

2. Принцип комплексности предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все каналы реализации угроз и не содержащий слабых мест на стыках ее компонентов.

3. Принцип непрерывности. Защита – непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла автоматизированных систем. Для эффективного функционирования физических и технических средств защиты необходима постоянная организационная поддержка. Применение мер защиты

---

[1] Полякова Т.А. Базовые принципы как основные начала правового обеспечения информационной безопасности // Труды института государства и права Российской академии наук. 2016. № 3. С.27.

[2] Полякова Т.А. Базовые принципы как основные начала правового обеспечения информационной безопасности // Труды института государства и права Российской академии наук. 2016. № 3. С.23

– это, прежде всего, предполагает не разовое применение, а комплексное и непрерывное применение мер.

4. Принцип разумной достаточности. Предполагает обеспечение лишь такого уровня информационной безопасности, при котором затраты, риск и размер возможного ущерба были бы приемлемы. Абсолютной защиты нет, или она стоит бесконечно много, либо система становится нефункциональной. Очень важна правильная оценка возможного ущерба, из субъективных соображений очень часто он либо сильно преуменьшается, либо сильно преувеличивается.

5. Принцип гибкости. Система создается в условиях неопределенности. Особенно важно, если защита устанавливается на уже работающую систему. Внешние условия постоянно меняются. Поскольку нельзя предвидеть будущее, необходимо иметь возможность относительно простого внесения изменений, настроек или дополнения новыми компонентами уже существующей системы защиты. Обязательно должен иметься запас «по мощности»: оперативной памяти, производительности процессора, пропускной способности каналов, места на внешних носителях и т.п.

6. Принцип открытости механизмов и алгоритмов защиты. Защита не должна обеспечиваться исключительно за счет секретности структурной организации и алгоритмов функционирования. Знание алгоритмов и механизмов защиты не должно давать возможность ее преодоления. Но это не значит, что эта информация должна быть общедоступна.

7. Принцип простоты применения. Механизмы защиты должны быть понятны и просты в использовании. Не должно быть значительных дополнительных трудозатрат при обычной работе законных пользователей, должна быть минимизация дополнительных ручных операций. Чем проще и понятнее действия, тем меньше вероятность дополнительных действий, меньше желание уклониться от выполнения этих действий. Чем проще

выполнение процедур защиты, тем больше времени персонал сможет посвятить выполнению своих прямых обязанностей.

Также деятельность государственных органов по обеспечению информационной безопасности строится на основании принципов, указанных в Законе РФ «О безопасности», которые были сформулированы в основные принципы обеспечения безопасности. К таким принципам относятся: законность, соблюдение баланса жизненно важных интересов личности, общества и государства; взаимная ответственность личности, общества и государства по обеспечению безопасности; интеграция с международными системами безопасности.

«Законность - в широком смысле принцип точного и неукоснительного исполнения всеми органами государства, должностными лицами и гражданами требований закона. Законность - это один из элементов демократии и правового государства. Принцип законности служит базой для законотворчества в частности правового обеспечения защиты информации, информационных структур, субъектов, осуществляющих сбор, формирование, распространение и использование информации, системы регулирования возникающих при этом отношений, требует, чтобы содержание всех законов соответствовало положениям Конституции РФ, международным договорам и соглашениям России с зарубежными государствами, заключенными для координации и взаимодействия в вопросах противодействия преступным посягательствам в информационной сфере. Правоохранительные, иные государственные органы, частные организации и граждане, уполномоченные осуществлять деятельность по обеспечению информационной безопасности, обязаны точно и неукоснительно соблюдать требования действующего законодательства. Виновные в совершении правонарушений и преступлений в информационной сфере несут ответственность в соответствии с действующим административным, гражданским и уголовным законом.

Применительно к информационной безопасности, можно выделить 3 основополагающих принципа - это принцип обоснованности, своевременности и прогноза.

Принцип обоснованности. Данный принцип главным образом связан с доступом к ограниченной информации, в случае, если произойдет незаконное получение данных, которые могут причинить вред гражданину, обществу или государству. В случае, если информация будет защищаться необоснованно, то в таком случае будет усматриваться посягательство на конституционные права граждан на информацию.

Принцип своевременности. В данном случае речь идёт, о защите информации своевременно, т.е. все процедуры, которые необходимы в рамках процесса защиты доступа к информации ограничения по распространению, должны осуществляться, непосредственно после получения такой угрозы или же заблаговременно. В практике такие меры достигаются путем разработки четко регламентированных положений концепции и системы защиты объекта, на котором сконцентрированы технические средства, средства связи, информация, подлежащая защите. Система защиты включает в себя совокупность правовых, научно-технических, специальных и организационных мер.

И последний принцип – это принцип прогноза информационной безопасности, который основан на выделении конкретных внешних и внутренних угроз к охраняемой информационной сфере и базируется на объектной, реальной оценке охраняемых объектов - информации, инфраструктуры, субъектов, связанных с созданием, преобразованием и потреблением информации; моделировании возможной противоправной деятельности, посягающей на информационную безопасность.

Таким образом, под принципами, следует понимать, совокупность общих установлений, императивов, руководящих потенциалом для формирования такой модели информационных отношений, в рамках которой не будут нарушаться базовые и присущие конкретному обществу, его

социокультурной программе информационные права и свободы. Инструментально принципы призваны решить проблему информационной агрессии, которая разрушает устои информационной безопасности человека. В целом можно отметить, что в совокупности таких принципов следует отнести принцип баланса информационных интересов как важную характеристику позитивной и неагрессивной информационной среды, принцип неуклонного соблюдения информационной свободы, принцип информационной ответственности и принцип социального информационного контроля.

3.3 Методы государственного регулирования информационной безопасности.

Обеспечение информационной безопасности является одной из приоритетных задач государства. Целью защиты информационной инфраструктуры критически важных объектов сдержать кибератаку и не допустить несанкционированный доступ и т.п., при этом обеспечивается стабильная работа всей информационной инфраструктуры, что является гарантом безопасности России.

Данные цели достигаются путем выполнения определенных методов, которые направлены на повышение информационной безопасности, данные методы хорошо выделены в работе Романовой Н.А., Домрачевой Т.С., Гусева И.В.. Они выделили следующие методы:

1. «Метод препятствие. Суть данного метода в том, что использование физические средства запрета на доступ к информационной инфраструктуре (носителям и аппаратуре). Например, охранно-пропускной режим на предприятии, построение защищенного периметра, использование разных типов сигнализации, - тем самым мы исключаем, а в некоторых

случаях затрудняем проникновение и доступ злоумышленника к информационной инфраструктуре.

2. Метод управления доступом. Основу данного метода составляет использование аппаратно-программных и/или программных комплексов, предотвращающих несанкционированный доступ к информационной инфраструктуре. Данный метод осуществляется при помощи следующих функций:

- идентификация личности субъекта (каждому субъекту присаивается уникальный идентификатор, при помощи которого субъект может получить доступ к объекту информационной структуры);

- аутентификация (устанавливается принадлежность субъекта или объекта к заявленном ими идентификатору);

- проверка соответствия полномочий (устанавливается точная дата и время проведения запланированных и регламентированных работ);

-доступ для проведения регламентированных работ и создание необходимых условий для их проведения;

- введение журнала доступа к защищенным ресурсам информационной инфраструктуры;

- реагирование на попытку скомпрометировать работу сигнализации, отключения, отказ в обслуживании и т.д.

3. Маскировка. Использование криптографических методов защиты информации - на сегодняшний день эффективность использования данных методов весьма высока.

4. Регламентация. Организационно-правовой метод защиты информации заключается в том, что все взаимодействия субъекта и объекта прописываются в регламентах.

5. Принуждение. Метод заключается в то, что вынуждает пользователя при доступе к защищенной информации соблюдать установленные правила обращения с конфиденциальной информацией или уголовной ответственности.

6. Побуждение. Метод основан на работе с персоналом предприятия. Работа происходит на уровне этических и моральных норм, запрещающих использование закрытой информации в неправомерных целях, и побуждает соблюдать установленные правила».[1]

Обеспечение и создание режима, в котором будет осуществлена информационная безопасности - это комплексная проблема. И для борьбы с данной проблемой необходимо предпринять меры различных уровней. Уровни формирования режима информационной безопасности можно сформулировать, следующим образом:

Уровни формирования режима информационной безопасности

1. «Первый уровень. Законодательный (законы, нормативные акты)
2. Второй уровень. Морально-этический (всевозможные нормы поведения).
3. Третий уровень. Административный (действия общего характера, предпринимаемые руководством организации).
4. Четвёртый уровень. Физический (механические, электро- и электронно-механические препятствия на путях проникновения нарушителей).
5. Пятый уровень. Аппаратно программный (электронные устройств и специальные программы защиты информации)».[2]

Важным направлением, как основного метода государственного регулирования в сфере информационной безопасности является правовое обеспечение. Нормативно-правовые акты регулируют вопросы обеспечения информационной безопасности, вопросы защиты информации, охраны государственной тайны, обеспечения защиты конфиденциальной информации, информационных ресурсов, направленные на реализацию положений Доктрины информационной безопасности. Политика информационной

[1] Шиганова М.В., Романова Н.А., Домрачева Т.С., Гусев И.В. Методы обеспечения информационной безопасности на объектах национальной важности // Аллея Науки. 2018. № 5(21). С. 917.

[2] Зайцева Д.С. Сущность и методы защиты информационной безопасности // В сборнике: Экономическая наука в 21 веке: вопросы теории и практики сборник материалов 9-ой международной научно-практической конференции. 2015. С. 20.

безопасности, а также безопасность информации в целом, разработаны с учетом методологии.

«Информационная безопасность и её составляющие рассматриваются сквозь призму функционального подхода в качестве объекта управления. Существующие концепции по видам опасностей, в том числе в информационной сфере, получили определенное нормативно-правовое закрепление в рамках парадигмы «безопасность является защитой от угроз»». [1] «Эта парадигма нашла отражение в Стратегии национальной безопасности Российской Федерации».[2]

На сегодняшний день пути, который выбрала Россия в рамках осуществления информационной безопасности недостаточно эффективна, необходимо введение функционального подхода. Если на данный момент, когда осуществляется борьба в этой сфере, меры защиты вводит тот орган, в чьи компетенции это входит. Но следовала бы провести корректировка в составляющей и когда осуществляется информационная безопасность - борьбу с этим должны осуществлять органы совместно, сообща, ведь только в рамках совместной работы министерств, ведомств и других органов можно добиться национальной безопасности в этой сфере. Только в рамках функционального подхода можно установить взаимодействие всех министерств и ведомств, а также скоординировать их деятельность, обеспечив организационными, материально-техническими возможностями.

Нинциева Т.М. достаточно ярко выразилась по этому поводу в своей работе «Обеспечение информационной безопасности государства правовыми методами регулирования». «Она утверждает, что содержательную сущность информационной безопасности в упрощенном виде можно изложить как

---

[1] Нинциева Т.М. Обеспечение информационной безопасности государства правовыми методами регулирования // В сборнике: Основные тенденции и принципы реализации положений Конституции Российской Федерации в различных отраслях правовой Российской Федерации Материалы 2 Международной научно-практической конференции, посвященной дню Конституции Российской Федерации. 2019. С. 131.

[2] Указ Президента РФ «О Стратегии национальной безопасности Российской Федерации» 5 декабря 2016 г. № 646

комплекс превентивных действий, направленных на обеспечение права на информацию и свободы информационной деятельности, на защиту информации и права собственности на информацию, на защиту от информации и от информационных воздействий. Методология формирования системы обеспечения информационной безопасности и практическое решение этих проблем свидетельствуют о том, что эффективность любой подсистемы будет напрямую зависеть от эффективного функционирования системы, в которую эта подсистема встроена. Иными словами, основой для совершенствования системы обеспечения информационной безопасности в процессе расширения межгосударственного сотрудничества должна быть эффективно действующая общая система обеспечения информационной безопасности как важная составляющая национальной безопасности РФ».[1]

Следует также отметить, некоторых авторов, которые в своих работах предложили некоторые методы совершенствования защиты информации от различных угроз, для более лучшего достижения цели информационной безопасности, так:

Так, «Р.И. Захарченко и И.Д. Королев в своей работе «Методика оценки устойчивости функционирования объектов критической инфраструктуры, функционирующей в киберпространстве» в рамках разработки методики оценки устойчивости объектов КИИ предложили расширить свойство устойчивости за счет внедрения нового свойства- киберустойчивости. Внедрение данного свойства аргументируется новой средой функционирования ГИС Российской Федерации и применения кибероружия, что, как следствие, является причиной возникновения новых угроз и уязвимостей для объектов критической инфраструктуры. Суть предлагаемой методики заключается в декомпозиции критической инфраструктуры на

[1] Нинциева Т.М. Обеспечение информационной безопасности государства правовыми методами регулирования // В сборнике: Основные тенденции и принципы реализации положений Конституции Российской Федерации в различных отраслях правовой Российской Федерации Материалы 2 Международной научно-практической конференции, посвященной дню Конституции Российской Федерации. 2019. С. 131.

отдельные объекты, что в теории позволит однозначно дать оценку состоянию защищенности критической информационной инфраструктуры от компьютерных атак».[1]

В.Е. Новичков и И.Г. Пыхтин в работе «Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» «проводят исследование о необходимости введения уголовной ответственности за преступления в сфере информационной безопасности. Обосновывает необходимость таких мер, тем, что по данным статистики количество компьютерных преступлений в последние годы значительно возросло. Учитывая это, а также действующее законодательство Российской Федерации, автор делает выводы об актуальности и необходимости введения уголовной ответственности за данные правонарушения»».[2]

А.О. Калашников, Е.А. Сакрутина в своей работе «Модель оценки безопасности критической информационной инфраструктуры на основе метода вейвлет-анализа» рассматривают модель оценки безопасности критической информационной инфраструктуры на основе прогнозирования рисков объектов, находящихся под воздействием компьютерных атак. Они предлагают модель оценки безопасности, построенную на основе вейвлет-разложения. Дальнейшее исследование динамики коэффициентов вейвлет-разложения позволит точнее выявлять опасные события, способные нарушить безопасность критической информационной инфраструктуры в будущем.

Г.А. Остапенко, Д.Г. Плотников, А.С. Рогозина в работе «Жизнестойкость элементов критической информационной инфраструктуры: аналитическая оценка с учетом возможных ущербов» рассматривают

---

[1] Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. № 2. С. 53.

[2] Новичков В.Е., Пыхтин И.Г. Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Психопедагогика в правоохранительных органах. 2018. № 2 (73). С. 27.

параметры функции риска для элементов критической информационной инфраструктуры на основе параметров рисков и их компонентов. Авторами предлагаются способы расчета риска для сложных многокомпонентных систем, учитывающих как синхронные, так и асинхронные атаки. Предложенные формулы дают возможность оценки риска совместного и несовместного воздействия дестабилизирующих факторов, а также жизнестойкости системы, что, как следствие, позволяет адекватно классифицировать степень защищенности инфраструктуры и точнее прогнозировать ущерб от потери работоспособности данных объектов».[1]

Подводя итог, можно сказать следующее, для государства одним из важных методов воздействия на информационную безопасность является нормативно-правовое регулирование российской Федерации в этой сфере. В текущих нормативных правовых актах существует некоторые проблемы, начиная от понимания определенных категорий до регулирования функционирования тех или иных органов. Учитывая это, государству следует усилить и продолжить совершенствовать правовое регулирование в области информационной безопасности, так как это его исключительная прерогатива государства.

[1] Остапенко Г.А., Плотников Д.Г., Рогозина А.С. Жизнестойкость элементов критической информационной инфраструктуры: аналитическая оценка с учетом возможных ущербов» // Информационная безопасность. Воронежский гос. техн. ун-т. 2013. № 3. С. 361.

ЗАКЛЮЧЕНИЕ

Важной особенностью современного общества является его информатизация, широкое применение информационных технологий, как в повседневной жизни, так и в профессиональной деятельности. Те объемы информации, информационные технологии и процессы глобализации формируют условия, в рамках которых мировое информационное пространство становится средством достижения различных целей: созидательных, способствующих развитию и улучшению жизнедеятельности социума, с одной стороны, и объектом противоправных посягательств в отношении государства, общества, отдельного человека и угроз их информационной безопасности – с другой. Именно поэтому на первый план в современном обществе, наряду с развитием коммуникационных систем, выходит проблема информационной безопасности.

В ходе проведенной работы, было установлено, что представляется собой информационная безопасность. Было дано большое количество определений информационной безопасности, но достаточно, большой интерес вызывает определение, данное А.И. Алексенцевым: «информационная безопасность - состояние информационной среды, обеспечивающее удовлетворение информационных потребностей субъектов информационных отношений, безопасность информации и защиты субъектов от негативного информационного воздействия».[1] Понятие информационной безопасности, достаточно широкое и включает в себя большое количество системообразующих признаков и из которого последующим и складывается понятие информационной безопасности.

Современная российская государственная политика в области информационной безопасности отличается сложностью и присущим ей, разносторонним характером. Её правовое регулирование основывается на

[1] Алексенцев А.И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» // Безопасность информационных технологий. 1999. № 1. С. 45

целом ряде нормативных правовых актов, каждый из которых уделяет значительной внимание вопросам информационной безопасности Российской Федерации. Государство активно ведёт работу, направленную на обеспечение информационной безопасности. И это положительный момент, так как развитие информационных технологий не остановится, изменения грядут во всех сферах жизни общества. Учитывая, что на сегодняшний момент активность пользователей сетью интернет с каждым днём увеличивается, вопросы конфиденциальности пользователей, защита информации на пространства приобретает большое значение. Российская Федерация, на мой взгляд, уделяет большое внимание информационной безопасности, это подтверждается тем, что каждое мероприятие на государственном уровне, где участниками являются представители государственной власти, которые в свою очередь в большинстве своих выступлений, стараются отметить важность обеспечения информационной безопасности. В нашей стране ведется государственная политика, но результаты и влияние тех путей развития, определенная государством на сегодняшний день не ясна, потому как взвесить все положительные и отрицательные стороны мы сможем, спустя определенное время.

Законодательство информационной безопасности Российской Федерации осуществляется путем отражения соответствующих положений в нормативных правовых актах различные виды ответственности за правонарушения в информационной сфере: за нарушение прав и свобод личности в сфере информации; недостоверность и ложность информации, создаваемой и распространяемой СМИ; сокрытие, умышленное искажение информации об источниках угроз; незаконное использование персональных данных, незаконное получение и использование информации с ограниченным доступом; создание некачественных информационных технологий и средств обеспечения. Информационное законодательство в Российской Федерации нуждается в совершенствовании, те отношения, которые складываются в информационном пространстве, государство, на данный момент, не может

организовать регулирование их. Поэтому необходимо обратить внимание на зарубежный опыт применения тех или иных мер по осуществления информационной безопасности.

В моей работе были рассмотрены несколько лидирующих стран, которые ведут положительную политику информационной безопасности. На данном этапе развития, можно добиться государственного регулировании информационной безопасности в бизнесе, промышленном производстве, IT-индустрии и в других сферах, только путем активного участия государства в регулировании этой сферы.

Тенденция развития института международной информационной безопасности, как элемента реализации государственного суверенитета, основывается на следующих основных моментах: формирование подходов к регулированию международной информационной безопасности на универсальном уровне идет в рамках рекомендаций группы правительственных экспертов ООН; развитие российской модели международной информационной безопасности осуществляется в рамках двухсторонних соглашений; различные международные организации, направлены на формирование и обеспечение единого международно-правового режима информационной безопасности.

В Российской Федерации информационная сфера находится под постоянным влиянием введения новых технологий, программ и для того, чтобы обеспечить осуществление государственными органами своих функций на должном уровне. На данный момент мы не можем говорить о том, что современное состояние государственного и общественного обеспечения информационной безопасности на должном уровне, как и развитие информационных технологий. Анализ тенденций нормативных положений позволяет выделить основные направления деятельности государственного аппарата: Президент РФ разрабатывает основу государственной политики в этой сфере, органы законодательной власти определяют концептуальную нормативную основу ключевых направлений государственной политики в

сфере информационной безопасности, закрепляют правовое положение основных субъектов критической информационной инфраструктуры, их права, обязанности и ответственность; а исполнительная власть определяет ключевые исполнительные органы, отвечающие за информационную безопасность, и обеспечивает непосредственно сам процесс защиты значимых объектов критической информационной инфраструктуры и ликвидации компьютерных атак. Поэтому субъектам информационной инфраструктуры нужно провести массу продолжительных по времени мероприятий для того, чтобы создать эффективную систему безопасности. Создаваемые системы национальных органов в рамках осуществления информационной безопасности, организациям и должностным лицам, должны предъявляться требования: компетентности, независимости, беспристрастности.

Для того, чтобы достойно и правильно осуществить свои функции, государственные органы должны соблюдать установленные на международном и национальном уровне принципы, а именно принцип баланса информационных интересов как важную характеристику позитивной и неагрессивной информационной среды, принцип неуклонного соблюдения информационной свободы, принцип информационной ответственности и принцип социального информационного контроля. Инструментально принципы призваны решить проблему информационной агрессии, которая разрушает устои информационной безопасности человека.

Подводя итог, можно сказать следующее, для государства одним из важных методов воздействия на информационную безопасность является нормативно-правовое регулирование российской Федерации в этой сфере. В текущих нормативных правовых актах существует некоторые проблемы, начиная от понимания определенных категорий до регулирования функционирования тех или иных органов. Учитывая это, государству следует усилить и продолжить совершенствовать правовое регулирование в области информационной безопасности, так как это и есть исключительная прерогатива государства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

РАЗДЕЛ I НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ И ИНЫЕ ОФИЦИАЛЬНЫЕ АКТЫ

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ // СЗ РФ. 2004. № 27. Ст. 2711.

2. Доктрина информационной безопасности Российской Федерации: утв. Президентом Рос. Федерации 9 сент. 2000 г. № ПР-1895 // Российская газета. 2000. № 28. признан утратившим силу.

3. Указ Президента «Об утверждении Доктрины информационной безопасности Российской Федерации» от 5 декабря 2016 г. № 646 // СЗ РФ. 2016. № 50. Ст. 7074.

4. Указ Президента РФ «О Стратегии национальной безопасности Российской Федерации» 5 декабря 2016 г. № 646.

5. Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» от 23 сентября 1992 № 3523-1 // признан утратившим силу.

6. Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ // СЗ РФ. 2006. № 31 (1 ч.). Ст.3451.

7. Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ // СЗ РФ. 1995. №8. Ст.609. признан утратившим силу.

8. Закон РФ «О средствах массовой информации» от 27.12.1991 № 2124-1 // СЗ РФ. 2020.

9. Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» от 9 февраля 2009 г. № 8-ФЗ // СЗ РФ. 2009.

10. Федеральный закон «О связи» от 7 июля 2003 г. № 126-ФЗ // СЗ РФ. 2003.

11. Национальная стратегия кибербезопасности 2016-2021. URL: https://government.ru (дата обращения:04.03.2020).

12. Cyber-Sicherheitsstategie fur Deutsthland 2016. URL:https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.

13. International Strategy for cyberspace (Prosperity, Security and Openness in a Networked World. URL: https:whitehouse.gov/sites/default/rss_viewer/international_strategy_for_cyberspace.pd. (дата обращения: 04.03.2020)

14. Electronic Communications Privacy Act of 1986 URL: https:law.comell.edu/uscode/text/18/2510.

15. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ // Российская газета. 31 июля 2017. № 7333 (167).

16. Указ Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05 декабря 2016 г. № 646 // СЗ РФ. 2016. № 50. Ст. 7074

17. Международная конвенция о пресечении терроризма от 27.01.1977 (ETS N 90)// СЗ РФ. - 2003. - № 3. - Ст. 202.

18. Международная конвенция о борьбе с финансированием терроризма от 09.12.1999 // СЗ РФ. - 2003. - № 12. - № 12. - Ст. 1059.

19. Международная конвенция о борьбе с бомбовым терроризмом от 15.12.1997 // СЗ РФ. - 2001. - № 35. - № 12. - Ст. 3513.

20. Конвенция Совета Европы о предупреждении терроризма от 16.05.2005 // ратифицирована от 20.04.2006. Федеральный закон от 20.04.2006 № 56-ФЗ.

РАЗДЕЛ II ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Азаренок, Н.К. Клиповое сознание и его влияние на психологию человека в современном мире // Традиционная Всероссийская юбилейная научная конференция «Психология человека в современном мире», посвящ. 120-летию со дня рожд. С.Л. Рубинштейна. Т.3. личность и группа в условиях социальных изменений / Н.К. Азаренок // Отв. Ред. А.Л. Журавлев. М.: «Институт психологии РАН», 2016. С.110-112.

2. Айдашева, Л.Г. Информационная война, как основная проблема международно-правового регулирования информационной безопасности / Л.Г. Айдашева // Наука сегодня задачи и пути их решения. 2020. С. 142-144.

3. Алексенцев, А.И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» / А.И. Алексенцев // Безопасность информационных технологий. 1999. № 1. С. 45.

4. Андриашин, Х.А. Правовые основы регулирования безопасности и защиты информации в современной России / Х.А. Андриашин // Вестник Московского университета МВД России. № 8. 2012. С.154-159.

5. Антоненко, Н.А., Этапы развития и становления государственной политики России в сфере информационной безопасности / Н.А. Антоненко // Новая наука: Проблемы и перспективы. 2016. № 9-1. С. 132-133.

6. Артюшова, Е.А. Проблемы международно-правового регулирования информационной безопасности / Е.А. Артюшова // Lex russica (Русский закон). 2009. № 5. С. 1165-1168.

7. Бегишев, И.Р. Информационное оружие как средство совершения преступлений / И.Р. Бегишев // Информационное право. 2010. № 4. С. 23-25.

8. Городов, О.А. Информационного права России. Учебное пособие / О.А. Городов // СПб.: Юридический центр Пресс, 2003 с. 19

9. Ефремов, А.А. Защита государственного суверенитета РФ в информационном пространстве / А.А. Ефремов // М.: Норма, 2017. С. 109-111.

10. Зайцева, Д.С. Сущность и методы защиты информационной безопасности / Д.С. Зайцева // В сборнике: Экономическая наука в 21 веке: вопросы теории и практики сборник материалов 9-ой международной научно-практической конференции. 2015. С. 18-22.

11. Захарченко, Р.И. Королев, И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры функционирующей в киберпространстве / Р.И. Захаренко, И.Д. Королев // Наукоемкие технологии в космических исследованиях Земли. 2018. № 2. С. 51-60.

12. Зиновьева, Е.С. Международная информационная безопасность / Е.С. Зиновьева // М.: МГИМО-Университет. 2013. С. 118-123.

13. Иванский, В.П. Мельничук, Г.В. Государственный контроль (надзор) - инструмент противодействия угрозам национальной безопасности в информационной сфере и средство защиты неприкосновенности частной жизни: соотношение частного и публичного интересов./ В.П. Ивановский, Г.В. Мельничук // Вестник РУДН. 2017. № 1. 136-152.

14. Иванова, Ю.О. Крылов, А.Н. Функции субъектов по защите критической информационной инфраструктуры в РФ / Ю.О. Иванова, А.Н. Крылов // Муниципальная служба: правовые вопросы. 2018. № 4. С. 33-35.

15. Калашников, А.О. Сакрутина, Е.А. Модель оценки безопасности критической информационной инфраструктуры на основе метода вейвлет-анализа / А.О. Калашников, Е.А. Сакрутина // Информационная безопасность. Воронежский гос. техн. ун-т. 2017. № 4. С. 478-491.

16. Капустин, А.Я. Угрозы международной информационной безопасности формирование концептуальных подходов / А.Я. Капустин // Журнал российского права. 2015. № 8. С. 89-100.

17. Кленина, В.И. Информационные технологии в профессиональной деятельности юриста / В.И. Кленина // Ученые записки. 2010. № 7. С. 99-102.

18. Козырева, А.А. Тарасов, Д.А. Современное состояние государственной политики в сфере информационной безопасности / А.А.

Козырева, Д.А. Тарасов // Юридические науки Вестник Воронежского института МВД России. 2018. №4. С 1-5.

19. Корсаков, Г.Б. Информационное оружие супердержавы: кибервойна и «управляемые кризисы» / Г.Б. Корсаков // Военно-политическое образование URL: http://www.belvpo.com/ru/10497.html (дата обращения: 26.02.2020).

20. Костенко, Н.И. Международная информационная безопасность в рамках международного права (методология, теория) / Н.И. Марков // Russian journal studies. 2018. № 4 (17) С. 9-16.

21. Кудрявцев, М.А. Стратегия развития информационного общества в России и основные направления развития информационного законодательства / М.А. Кудрявцев // Современное российское право: взаимодействие науки, нормотворчества и практики. Часть 3. XIII Международная научно-практическая конференция. «Проспект». 2018 г. С. 364-373.

22. Кукса, Т.П. Содержание понятия «Информационная безопасность» / Т.П. Кукса // В сборнике: Морская стратегия и политика России в контексте обеспечения национальной безопасности и устойчивого развития в XXI. 2018. С. 213-218.

23. Кучерявый, М.М. Косов, Ю.В. Вовенда, Ю.В. Деятельность органов власти Северо-Западного федерального округа по обеспечению безопасности информации / М.М. Кучерявый, Косов Ю.В., Вовенда Ю.В. // Управленческое консультирование. 2017. №10. С 8-14.

24. Кучерявый М.М. Роль информационной составляющей в системе политики обеспечения национальной безопасности Российской Федерации / М.М. Кучерявый // Известия Российского государственного педагогического университета им. А.И. Герцена. 2016. № 164. С. 155-163.

25. Лапаева, В.В. Философско-правовое основы российской государственной политики / В.В. Лапаева // Сб. материалов Всероссийской конференции «Правовая политика в условиях модернизации». М. 2011. С. 21.

26. Лепский, В.Е. Становление стратегических субъектов в глобальном информационном обществе: постановка проблемы / В.Е. Лепский. // Информационное общество, 2002. С.58.

27. Лукашук, И.И. Международно-правовое регулирование международных отношений (системный подход). / И.И. Лукашук // М., 1975. С. 10.

28. Мазуров, В.А., Невинский, В.В. Понятие и принципы информационной безопасности / В.А. Мазуров, В.В. Невинский. М.: 2017. № 3. С. 78-84.

29. Мамедова, К.А. Основные принципы обеспечения информационной безопасности страны/ К.А. Мамедова // Информационная безопасность регионов.2016. № 1. С. 16-20.

30. Марков, А. Некоторые аспекты информационной безопасности в контексте национальной безопасности / А. Марков // Вестник СПбУ. №12 С. 43-48.

31. Михнев, И.П. Информационная безопасность на просторах мобильного интернета / И.П. Михнев // Образовательные ресурсы и технологии. 2015. № 4 (12). С. 66-70.

32. Михнев, И.П. Михнева, С.В. Махова, А.А. Лапшина, А.Р. Полномочия Федеральных органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры / И.П. Михнев, С.В. Михнева, А.А. Махова, А.Р. Лапшина // Юридические науки. Вестник Алтайской академии экономики и права. № 1.Ч 2. 2019. С.202-208.

33. Михнев, И.П. Михнева, С.В. Природные радионуклиды как источник фонового обучения населения Нижневолжского региона. / И.П. Михнев, С.В. Михнева // В сборнике: Образование и наука: современные тренды: коллективная монография. Чебоксары. 2018. С. 151-166.

34. Михнева, С.В. Михнев, И.П. Чернова, А.П. Правовые основы определения юридического положения должностных лиц местного

самоуправления и муниципальных служащих в Российской Федерации. / С.В. Михнева, И.П. Михнев, А.П. Чернова // В сборнике: Социально-экономические и правовые основы инновационного развития: сборник научных статей. Пенза. 2018. С. 104-111.

35. Морозова, А.В., Полякова, Т.А. Организационно-правовое обеспечение информационной безопасности / А.В. Морозова, Т.А.Полякова. М.: РПА Минюста России. 2013. С. 251.

36. Нерсесянц, В.С. Правовая политика и совершенствование законодательства: теоретически-методологические проблемы / В.С. Нерсесянц // Актуальные проблемы совершенствования российского законодательства на современном этапе. Материалы Всероссийской научно-практической конференции. М. 2003. С. 3.

37. Нинциева, Т.М. Обеспечение информационной безопасности государства правовыми методами регулирования / Т.М. Нинциева // В сборнике: Основные тенденции и принципы реализации положений Конституции Российской Федерации в различных отраслях правовой Российской Федерации Материалы 2 Международной научно-практической конференции, посвященной дню Конституции Российской Федерации. 2019. С. 129-134.

38. Новичков, В.Е. Пыхтин, И.Г. Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации / В.Е. Новичков, И.Г. Пыхтин // Психопедагогика в правоохранительных органах. 2018. № 2 (73). С. 25-29.

39. Новости информационной безопасности. URL: https://www.anti-malware.ru/news/2020-02-21-111332/32041 (дата обращения 17.03.2020).

40. Новости информационной безопасности. URL: https://www.anti-malware.ru/news/2020-02-26-111332/32074 (дата обращения 17.03.2020).

41. Остапенко, Г.А. Плотников, Д.Г. Рогозина А.С. Жизнестойкость элементов критической информационной инфраструктуры: аналитическая

оценка с учетом возможных ущербов» / Г.А. Остапенко, Д.Г. Плотников, А.С. Рогозина // Информационная безопасность. Воронежский гос. техн. ун-т. 2013. № 3. С. 353-364.

42. Панфилова, О.А. Информационная безопасность и защита информации: учебное пособие для направления подготовки 40.03.01 - Юриспруденция, специальности 40.05.02 - Психология служебной деятельности, очной и заочной форм обучения / О.А. Панфилова // и др., Вологда, ВИПЭ ФСИН России, 2018. С. 59

43. Подболотова, Н.Б. Связи с общественностью в государственных органах власти и управления: автореф. дис. канд. полит. наук: 23.00.01. / Н.Б. Подболотова // М., 2001. С. 20

44. Полякова, Т.А. Базовые принципы как основные начала правового обеспечения информационной безопасности / Т.А. Полякова // Труды института государства и права Российской академии наук. 2016. № 3. С. 17-40.

45. Права и свободы личности./ Библиотечка «Российской газеты» совместно с библиотечкой журнала «Социальная защита» М. 1995. №. 11.

46. Расторгуев, С.П. Философия информационной войны / С.П. Расторгуев // М. 2016. С. 47

47. Садчикова, Д.Н. О современной государственной политике в области информационной безопасности / Д.Н. Садчикова // Поколение будущего: Взгляд молодых ученых. 2018. С 236-239.

48. Сведения о полномочиях ФСТЭК России; перечень нормативных правовых актов, определяющих эти полномочия // ФСТЭК России. URL: http://fstec.ru/obshchaya-informatsiya/polnomochiya (дата обращения: 07.03.2020).

49. Стрельцов, А.А. Обеспечение информационной безопасности России / А.А. Стрельцов // Теоретические и методические основы. М.:МЦНМО, 2002. С. 52-57.

50. Середа, В.В. Карась, А.Ю. Международный обмен информацией в рамках международно-правового регулирования / В.В. Середа, А.Ю. Карась // Научные стремления. 2015. № 4 (16).

51. Скиба, А.В. Развитие правового регулирования в области правового обеспечения информационной безопасности при построении информационного общества России / А.В. Скиба // Актуальные проблемы государства, права и гуманитарных наук. 2015. С 305-311.

52. Снытников, А.А. Обеспечение и защита прав на информацию / А.А. Снытников М. 2001. С. 22.

53. Тарасов, А.М. Киберугрозы, прогнозы, предложения / А. М. Тарасов. Информационное право. 2014. №3. С. 12.

54. Трашкова, С.М. Основы правового регулирования защиты информации в Российской Федерации / С.М. Трашкова // Вестник Восточно-сибирской открытой академии. 2014. № 16. С.1-13.

55. Улин, В.М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом. Монография / В.М. Улин // М.:. 2016

56. Устинов, Д. Основные направления участия органов государственной власти субъектов РФ в реализации политики информационной безопасности / Д. Устинов // Экономика и бизнес: теория и практика. 2018. № 5-2. С. 151-155.

57. Полякова Т.А. Базовые принципы как основные начала правового обеспечения информационной безопасности / Т.А. Полякова // Труды института государства и права Российской академии наук. 2016. № 3. С.17-40.

58. Филатов, В.В. Зарубежный опыт правового регулирования информационной безопасности / В.В. Филатов // Wschodnioeuropejskie Czasopismo Naukowe (East European Scientific Journal). 2018. № 3(31). С.69.

59. Чубукова, С.Г. Стратегии развития информационного общества и направления развития законодательства / С.Г. Чубукова // Правовая информатика. 2017. № 2. С. 67-72.

60. Шиганова, М.В. Романова, Н.А. Домрачева, Т.С. Гусев, И.В. Методы обеспечения информационной безопасности на объектах национальной важности / М.В. Шиганова, Н.А. Романова, Т.С. Домрачева, И.В. Гусев // Аллея Науки. 2018. № 5(21).С. 915-919.

61. Щедрин Д.Н., Некоторые аспекты правового регулирования кибербезопасности на территории Российской Федерации и зарубежных стран / Д.Н. Щедрин // Инновационные тенденции развития российской науки. Часть II. мат-лы XII междунар. науч.-практ. конф. молод. учен. (8-9апреля 2019 г.) / Краснояр. гос. аграр. ун-т. Красноярск, 2019. С. 324.

62. Electronic Communications Privacy Act of 1986. URL: https:law.comell.edu/uscode/text/18/2510.

63. International Strategy for cyberspace (Prosperity, Security and Openness in a Networked World URL: https:whitehouse.gov/sites/default/rss_viewer/international_strategy_for_cyberspace.pdf. (дата обращения: 04.03.2020)

64. Cyber-Sicherheitsstategie fur Deutsthland 2016 [Электронный ресурс] URL: https://www.bmi.bund.de/cybersicherheitsstrategie-/BMI_CyberSicherheitsStrategie.pdf

65. Merion School District. URL: https://en.wikipedia.org/wiki/Robbins_v._Lower_Merion_School_District

66. Microsoft Corp. против Соединенных Штатов. – Microsoft Corp. v. United States. URL: https://ru.qwe.wiki/wiki/Microsoft_Corp._v._United_States

67. Stored Communications Act URL: www.law.cornell.edu/uscode/text/18/2701

РАЗДЕЛ III ПОСТАНОВЛЕНИЯ ВЫСШИХ СУДЕБНЫХ ИНСТАНЦИЙ И МАТЕРИАЛЫ ЮРИДИЧЕСКОЙ ПРАКТИКИ.

1. Определение Конституционного Суда РФ от 18.01.2011 № 8-О-П «По жалобе открытого акционерного общества «Нефтяная компания «Роснефть» на нарушение конституционных прав и свобод положением абзаца

первого пункта 1 статьи 91 Федерального закона «Об акционерных обществах»».

2. Постановление Конституционного Суда РФ от 29.11.2010 № 20-П «По делу о проверке конституционности положений статей 20 и 21 Федерального закона «О содержании под стражей подозреваемых и обвиняемых в совершении преступлений» в связи с жалобами граждан Д.Р. Барановского, Ю.Н. Волохонского и И.В. Плотникова» и т.д.

3. Microsoft Corp. против Соединенных Штатов. – Microsoft Corp. v. United States. [Электронный ресурс] URL: https://ru.qwe.wiki/wiki/Microsoft_Corp._v._United_States

4. Robbins v. Lower Merion School District. [Электронный ресурс] URL: https://en.wikipedia.org/wiki/Robbins_v._Lower_Merion_School_District

ПРИЛОЖЕНИЕ 1

Тестирование по теме: «Государственное регулирование информационной безопасности».

Тестирование проводилось в различных группах: 1. Группа, лица, которые непосредственно сталкиваются каждый день с информационной безопасностью, ознакомленные с правовым регулированием информационной безопасности в РФ. 2. Группа, лица, которые не осуществляют деятельность по обеспечению информационной безопасности, но ознакомленные с правовым регулированием информационной безопасности. 3. Группа, лица, которые не ознакомлены с правовым регулированием информационной безопасности в РФ.

Было протестировано 100 человек по 33 человека в каждой группе. Результаты представлены в форме таблицы.

1. Масштабы компьютерной преступности в РФ

а. Неуклонно снижаются;

б. Возрастают;

в. Остаются из года в год неизменными;

2. Статья 23 Конституции РФ определяет:

а. Право на получение достоверной информации о состоянии окружающей среды;

б. Право на неприкосновенность частной жизни, личную и семейную тайну и иные сообщения;

в. Отказ в предоставлении гражданину информации.

3. Федеральный закон «Об информации, информационных технологиях и о защите информации»:

а. пока не принят;

б. принят в 2000 году;

в. принят в 2006 году.

4. Доктрина Информационной безопасности принята в

А. 2012 году

Б. 2014 году

В. 2016 году

5. В организационную основу системы обеспечения информационной безопасности РФ входит:

а. Совет безопасности РФ;

б. Министерство образования и науки РФ;

в. ЦРУ США.

6. К актам федерального законодательства по ИБ в РФ входят:

А. Приказы ФСБ;

Б. Международные стандарты;

В. Конституция РФ.

7. Правовое обеспечение ИБ означает:

а. Защиту интересов физических и юридических лиц;

б. Защиту интересов государства и общества;

в. Все вышеперечисленное.

8. В какой статье УК предусматривается наказание за «Неправомерный доступ к компьютерной информации»?

а. в ст.272;

б. в ст.273;

в. в ст.274.

9. Федеральный закон «О персональных данных» принят:

а. в 2006 году с изменениями на 1 января 2017 года;

б. в 2009 году;

в. в 2016 году.

10. В политике безопасности основным принципом является усиление самого слабого звена?

а. нет:

б. да;

в. отчасти.

11. В политике безопасности не должна быть:

а. невозможность миновать защитные средства;

б. разделение обязанностей;

в. возможность перехода в небезопасное состояние.

12. Контроль целостности программного обеспечения НЕ проводится с помощью:

а. внешних средств (программ контроля целостности);

б. внутренних средств (встроенных в саму программу);

в. криптографических средств.

13. Организационное обеспечение информационной безопасности – это..?

а. реализация защиты информации, осуществляемая службами безопасности режима, защита информации техническими средствами и др.;

б. совокупность средств, обеспечивающих удобства работы пользователей;

в. нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения.

14. К организации конфиденциального делопроизводства относится:

а. организация документооборота;

б. использование сертифицированных технических и программных средств;

в. проверка надежности сотрудников.

15. Минимизация утечки информации через персонал это:

а. организационно-технические средства защиты информации;

б. организационно-экономические меры;

в. организационно-административные меры.

Вопросы \ результаты	**Респонденты, которые ответили верно, на поставленный вопрос**	**Респонденты, которые ответили неверно, на поставленный вопрос**
1. Масштабы компьютерной преступности в РФ	91	9
2. Статья 23 Конституции РФ определяет:	85	15
3. Федеральный закон «Об информации, информационных технологиях и о защите информации»:	77	33
4. Доктрина информационной безопасности принята в:	84	16
5. В организационную основу системы обеспечения информационной безопасности РФ входит:	73	27
6. К актам федерального законодательства по ИБ в РФ входят:	56	44
7. Правовое обеспечение ИБ означает:	51	49
8. В какой статье УК предусматривается наказание за «Неправомерный доступ к компьютерной информации»?	75	35
9. Федеральный закон «О персональных данных» принят:	83	17
10. В политике безопасности основным принципом является усиление самого слабого звена?	89	11
11. В политике безопасности не должна быть:	76	24
12. Контроль целостности программного обеспечения НЕ проводится с помощью:	63	37
13. Организационное обеспечение информационной безопасности – это..?	83	17
14. К организации конфиденциального делопроизводства относится:	78	22
15. Минимизация утечки информации через персонал это:	84	26