

Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Пензенский государственный университет»

Юридический институт

Кафедра «ГПД»
(наименование)

Направление подготовки 40.04.01 «Юриспруденция»
(код и наименование)
Магистерская программа Конституционное право; муниципальное право
(наименование)

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему

Конституционно-правовые основы информационной безопасности
в Российской Федерации

Студент 17зюю1м Шамшин Сергей Сергеевич
номер группы подпись, дата фамилия, имя, отчество полностью
Научный руководитель к.ю.н., доцент Катомина В.А.
подпись, дата фамилия, инициалы

Консультанты:

по	наименование раздела, звание, должность	подпись, дата	фамилия, инициалы
по	наименование раздела, звание, должность	подпись, дата	фамилия, инициалы
Нормоконтролер:	доцент кафедры «ГПД»	<u>Логачева Н.В.</u>	Логачева Н.В.
	должность	подпись, дата	фамилия, инициалы

Рецензент:

главный специалист-эксперт Управления Министерства
юстиции по Пензенской области

должность

подпись, дата

Дегтярева А.А.

Работа допущена к защите в (протокол заседания кафедры от ____ 201 № ____)
Заведующий кафедрой Романовская О.В.
название подпись, дата фамилия, инициалы

Работа защищена с оценкой ____ (Протокол от ____ 201 г. № ____)
Секретарь ГЭК Антипкина Е.Г.
подпись, дата фамилия, инициалы

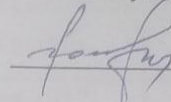
Пенза 2020 г.

УТВЕРЖДАЮ

Зав. кафедрой

Государственно-правовые

дисциплины

 /О.В. Романовская/
(инициалы и фамилия)

16 ноября 2017г.

ЗАДАНИЕ

на выпускную квалификационную работу студента (ки) гр.№17зюю1м

Шамшина Сергея Сергеевича

1. Тема работы Конституционно-правовые основы информационной безопасности в Российской Федерации

2. Научный руководитель к.ю.н., доцент Катомина Виктория Александровна

3. Дата выдачи задания 16 ноября 2017 г.

4. Срок сдачи студентом законченной работы 9 января 2020 г

5. Перечень подлежащих разработке вопросов:

- дать определение понятию «информационная безопасность» и определить его соотношение с понятием «безопасность»;
- проанализировать конституционно-правое регулирование информационной безопасности личности, организации, общества и государства в российском законодательстве;
- рассмотреть методы и средства криптографической защиты информации;
- рассмотреть различные аспекты правовой и технической защиты информации отдельных субъектов и объектов информационного права;
- исследовать основные тенденции развития института информационной безопасности в Российской Федерации;
- выявить основные направления информационной безопасности Российской Федерации как процесса обеспечения защищенности прав граждан, организаций, общества и государства.

6. Консультанты по работе, с указанием относящихся к ним разделов работы

Раздел	Консультант	Подпись, дата	
		Задание выдал	Выполненное задание принял
Введение		16 ноября 2017 Катомина В.А. <i>В.А.К.</i>	1 февраля 2018 Катомина В.А. <i>В.А.К.</i>
Понятие информационной безопасности		1 февраля 2018 Катомина В.А. <i>В.А.К.</i>	21 марта 2018 Катомина В.А. <i>В.А.К.</i>
Правовое обеспечение информационной безопасности		21 марта 2018 Катомина В.А. <i>В.А.К.</i>	12 июня 2018 Катомина В.А. <i>В.А.К.</i>
Криптографические методы и средства защиты информации		12 июня 2018 Катомина В.А. <i>В.А.К.</i>	1 сентября 2018 Катомина В.А. <i>В.А.К.</i>
Общая характеристика правовой защиты информации		1 сентября 2018 Катомина В.А. <i>В.А.К.</i>	25 декабря 2018 Катомина В.А. <i>В.А.К.</i>
Правовая характеристика организационно-правового и технического обеспечения отдельных субъектов и объектов информационной безопасности		25 декабря 2018 Катомина В.А. <i>В.А.К.</i>	1 февраля 2019 Катомина В.А. <i>В.А.К.</i>
Анализ развития информационного законодательства в Российской Федерации		1 февраля 2019 Катомина В.А. <i>В.А.К.</i>	30 мая 2019 Катомина В.А. <i>В.А.К.</i>
Тенденции развития института информационной безопасности в Российской Федерации		30 мая 2019 Катомина В.А. <i>В.А.К.</i>	30 октября 2019 Катомина В.А. <i>В.А.К.</i>
Заключение		30 октября 2019 Катомина В.А. <i>В.А.К.</i>	28 декабря 2019 Катомина В.А. <i>В.А.К.</i>

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	5
1.1 Истоки понятия информации.....	10
1.2 Понятие информационной безопасности	14
1.3 Правовое обеспечение информационной безопасности	17
1.4 Криптографические методы и средства обеспечения информационной безопасности	32
2 ПРАВОВАЯ ХАРАКТЕРИСТИКА ОРГАНИЗАЦИОННО- ПРАВОВОГО И ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ ОТДЕЛЬНЫХ СУБЪЕКТОВ И ОБЪЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	38
2.1 Понятие правовой защиты информации.....	38
2.2 Информационная безопасность адвокатской деятельности.....	42
2.3 Информационная безопасность налоговых органов	44
2.4 Информационная безопасность судебного производства	49
2.5 Информационная безопасность высших учебных заведений	58
3 ТЕНДЕНЦИИ РАЗВИТИЯ ИНСТИТУТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ.....	58
3.1 Тенденции развития информационного права в России.....	64
3.2 Развитие законодательства в области информационной безопасности как элемент системы национальной безопасности.....	67
3.3 Анализ направления реализации политики информационной безопасности на примере сравнения Доктрины информационной безопасности 2000 и 2016 годов.	76
3.4 Актуальные направления информационной безопасности Российской федерации.....	80
ЗАКЛЮЧЕНИЕ	85
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	87

ВВЕДЕНИЕ

Информационную безопасность можно определить как политико-правовое понятие, обозначающее состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Базовое представление об информационной безопасности можно изложить в следующих вопросах:

- соблюдение конституционных прав и свобод граждан;
- совершенствование отечественных информационно-телекоммуникационных технологий и повышение их конкурентоспособности на мировом рынке;
- создание гарантий безопасности информационных телекоммуникационных систем;
- информационное обеспечение деятельности государства, в условиях непрерывно меняющейся геополитической обстановки.

Совершенствование существующей системы информационной безопасности, развитие её составляющих и обеспечение функционирования для защиты интересов граждан, организаций общества и государства являются актуальной научной проблемой. Это обусловлено:

- исключительно растущей ролью информации и её влияния на все доступные сферы общественных отношений;
- изменением приоритетов безопасности государства и необходимостью теоретического и практического решения принципиально новых задач ее информационного обеспечения;
- появлением принципиально новых угроз и опасностей, воздействующих на информационно-коммуникационные системы государства, общественное и индивидуальное сознание его граждан.

Несмотря на непрерывную работу по разработке действующих и всеобъемлющих механизмов обеспечения информационной безопасности, а

также их правовую и методическую поддержку можно выделить целый ряд существующих на данный момент вопросов, таких как:

- постоянно меняющиеся черты, роли, характерные особенности отдельных аспектов информационной безопасности, их цели и задачи, области применения;
- ошибки прогнозирования тенденций развития информационной безопасности в процессе трансформации современного общества;
- существующие теоретико-правовые модели и схемы идеального информационного взаимодействия общественных и государственных институтов в сфере государственной безопасности не охватывают все возникающие в связи с этим взаимодействием вопросы;
- некорректная реализация отдельных аспектов информационного и методического обеспечения по вопросам информационной безопасности, связанных с деятельностью органов государственной власти в интересах решения возложенных на них задач.

Все вышеперечисленное подтверждает актуальность выбранной темы исследования.

Цель исследования. Целью магистерского исследования является конституционно-правовое осмысление и деконструкция теоретико-методологических основ концепции информационного обеспечения государственной безопасности России как сложной социальной системы в условиях перехода к постиндустриальному обществу, развитию социально ориентированной рыночной экономики, а также анализ существующих тенденций развития института информационной безопасности.

Достижению поставленной цели способствовало решение следующих задач:

- определить понятие информации;
- рассмотреть понятие информационной безопасности и её соотношение с иными видами безопасности;
- рассмотреть существующие особенности конституционно-правового

обеспечения информационной безопасности;

- дать определение криптографических методов и средств обеспечения информационной безопасности и предоставить их подробную классификацию;

- рассмотреть особенности организационно-правового и технического обеспечения отдельных субъектов и объектов информационной безопасности;

- дать характеристику правовой защиты информации;

- рассмотреть особенности обеспечения информационной безопасности адвокатской деятельности, налоговых органов, судебного производства и высших учебных заведений;

- выявить основные направления и проанализировать существующие тенденции развития института информационной безопасности Российской Федерации;

- проанализировать развитие информационного права в Российской Федерации за период 1990-2020 годов;

- рассмотреть развитие законодательства в области информационной безопасности как элемента развития системы национальной безопасности;

- выявить направление реализации политики информационной безопасности Российской Федерации на примере сравнения Доктрины информационной безопасности 2000 и 2016 годов;

- определить актуальные направления информационной безопасности Российской Федерации.

Объектом исследования являются общественные отношения в сфере обеспечения информационной безопасности, а также условия обеспечения информационной безопасности личности, общества и государства.

Предметом исследования выступает содержание и значение конституционно-правовых норм, обеспечивающих создание системы информационной безопасности личности, российского общества и государства.

Методологическая основа исследования образуют общенаучные методы юридической и философской науки, а именно: диалектический метод познания правовой действительности, формально-юридический метод, а также исторический и сравнительно-правовой методы исследования.

Степень разработанности проблемы. В отечественной и зарубежной литературе в последнее время немалое внимание уделяется проблемам информации, информационной безопасности, информационной войны, информационной культуры, функционирования геоинформационных систем, формирования информационного общества, информационных ресурсов. Значительный вклад в разработку перечисленного спектра проблем, связанных с функционированием информации в различных сферах общества, культуры, науки и техники, внесли такие ученые и исследователи, как А.Б.Агапов, А.С. Алексеев, И.Л.Бачило, А.В. Возженников, Ю.М. Горский, Г.Н. Горшенков, И.С. Даниленко, Н.В. Данилов, С.А. Дятлов, Г.В. Емельянов, Ю.А. Жданов, М.Ю. Захаров, В.П. Ильин, Г.Б. Кадомцев, К.К. Колин, В.И. Кузнецов, В.Н.Лопатин, И.А. Михальченко, С.А. Модестов, В.И. Мухин, В.К. Новиков, А.И. Палий, М.М.Рассолов, В.В. Ратиев, А.А. Силин, Л.В. Скворцов, Г.Г. Феоктистов, А. М. Яновский и другие.

Тем не менее конституционно-правовые аспекты проблемы информационной безопасности России требуют дальнейшего анализа. Это предполагает рассмотрение целого круга таких спорных вопросов, как выбор дефиниции «информация», адекватной правовому подходу к проблемам информационной безопасности, раскрытие нелинейного характера информационной безопасности, выделение информационной компоненты общественных процессов современного социума, установление роли информационной инфраструктуры в системе национальной безопасности России и места информационной составляющей в стратегии национальной безопасности России.

Теоретическая и практическая значимость результатов исследования. Научно-практическая значимость диссертации определяется тем, что она

посвящается целостному конституционно-правовому концептуальному исследованию реального процесса информационной безопасности России, его анализу как сложной социально-политической системы.

Структура диссертации. Диссертация состоит из введения, трех глав, заключения и списка используемых источников.

1 Конституционно-правовое регулирование информационной безопасности Российской Федерации

1.1 Истоки понятия информации

Рассматривая тот или иной объект, юридическая наука обращается к иным отраслям знаний, для которых этот объект является традиционным предметом исследования. Понятие «информация» может быть отнесено к абстрактным категориям и первичным понятиям.¹ Термин «информация» возник еще в древние времена вместе с письменностью и происходит от латинского слова «information», что в дословном переводе означает разъяснение, изложение, представление, понятие, сведения, осведомление, сообщение.

Понятие «информация» относится к числу таких общефилософских категорий, как пространство, время, движение, энергия. С позиций философии информация представляет собой отражение объектов материального мира в человеческом сознании или упорядоченное отражение реальной действительности.^{2 3} Согласно этому определению информация является уникальным предметом, который одновременно содержит в себе идеальное и материальное начало, в этом заключается дуализм информации.

Впервые как научное понятие термин «информация» стал применяться в теории журналистики в 30-х годах прошлого века, хотя в исследованиях по библиотечному делу он появился еще раньше. Под информацией понимались разнообразные сведения, данные, сообщения, передаваемые людьми устным, письменным или иным способом. Такое положение стало меняться с середины 20 века, когда в связи с появлением и развитием средств связи и телекоммуникаций, вычислительной техники и их использованием для обработки (формирования, изменения, приема, воспроизведения) и передачи

¹ Агапов А.Б. Основы государственного управления в сфере информатизации в Российской Федерации, - М.: Юрист, 1997,- С. 36; Бачило И.Л. Информация - объект права// НТК- Серия 1.-1999. - № 8. - С. 26.

² Нисневич Ю.А. Информация и власть. М.: Мысль, 2000. - С. 15.

³ Кулиев И.О. Информационное обеспечение деятельности органов местного самоуправления (муниципалитетов) в сфере правопорядка М., 2002, с. 26-27.

различного рода (радио, телевизионных) сигналов возникла необходимость измерять количественные характеристики информации. Появились разные теории, а содержание понятия «информация» стало активно развиваться, обогащаться новым содержанием и постепенно трансформировалось в общенаучную категорию, оказывающую методологическое воздействие на развитие самых разных отраслей научных знаний, включая юридическую науку.⁴

Одним из наиболее удачных признается определение информации, данное основателем науки кибернетики Нобертом Винером: «Информация – это обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособливания к нему наших чувств. Процесс получения и использования информации является процессом нашего приспособления к случайностям внешней среды и нашей жизнедеятельности в этой среде».

Как видим, в указанном определении информации отражены два важных признака этого понятия, которые признаются большинством исследователей информации. Во-первых, устанавливается, что информация нематериальна. Именно этот признак обуславливает специфику конституционноправового регулирования информационных отношений. Во-вторых, в определении Н. Винера указывается на то, что информация - это определенное содержание, то есть сведения, факты, получаемые из внешнего мира в процессе приспособления, а, следовательно, в процессе взаимодействия с внешним миром.

Определение современного понятия и содержания информации представляет определенную сложность, поскольку каждая из отраслей научных знаний предлагает свой вариант дефиниций.

По мнению Ермишиной Е.В., информация – это передача новостей, сообщений о событиях, а также научно-техническая информация, видеопленки и записи, различного рода печатная информация и т.д.

⁴ Васильев А.Н. Категория «информация» в понятийном аппарате юридической науки.. 2007. С. 73-75.

Различают понятие «информация» как средство, процесс и «информация» как конечный результат. Как видим, в этом определении Ермишиной Е.В. была предпринята попытка объединить в понятии информация два основных признака: во-первых, представить информацию как сведения, факты, во-вторых, рассматривать информацию как процесс передачи сведений.

Венгеров А.Б. впервые в российской юридической науке сформулировал признаки информации, к числу которых относятся: автономность информации по отношению к своему носителю; неисчерпаемые возможности использования одной и той же информации.⁵

Спецификой информации, отличающей ее от вещных, материальных объектов, являются ее сохраняемость у передающего субъекта, способность к хранению, агрегированию, интегрированию, накоплению и сжатию. Особенно важны для информации как элемента правоприменения и объекта правового регулирования такие ее свойства как системность и количественная определенность.

Бачило И.Л. выделяет следующие свойства информации как объекта правового регулирования:⁶

- свойство физической неотчуждаемости информации. Информация практически не может быть отчуждена от создателя или иного обладателя. То есть при передаче информации другому лицу (лицам) она по-прежнему остается у первоначального носителя;

- свойство обособляемости информации. Для включения в оборот информация должна быть овеществлена, то есть закодирована в виде волн, символов, знаков и т.п. Вследствие этого она обособляется от создателя (носителя) и существует независимо от него;

- свойство информационной вещи (информационного объекта). При

⁵ Венгеров А.Б. Право и информация в условиях автоматизации управления (теоретические вопросы). - М., 1978.-С. 19.

⁶ Бачило, И. Л. Информационное право : учебник для академического бакалавриата / И. Л. Бачило. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019.- С.33.

овеществлении и включении в оборот информация обычно закрепляется на каком-то материальном носителе и распространяется с его помощью;

- свойство тиражируемости (распространяемости). Информация может тиражироваться и распространяться в неограниченном количестве экземпляров без изменения ее содержания;

- свойство экзemplярности. Это свойство заключается в том, что информация распространяется, как правило, не сама по себе, а в виде материального или цифрового документа различной формы его организации.

К видам информации можно отнести следующие разновидности.

Документированная информация (документы) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. Понятие «документированная информация» основано на двуединстве - информации и материального носителя, на котором она отражена в виде символов, знаков, букв, волн или других способов отображения. В результате документирования происходит как бы материализация сведений. Информация «закрепляется» на материальном носителе или даже «привязывается» к нему и тем самым обособляется от своего создателя. В итоге в качестве документированной информации мы получаем книгу, статью в журнале, сборник статей, фонд документов, банк данных или иной массив данных на бумажном, машиночитаемом или иных носителях.⁷

Массовая информация – предназначенные для неограниченного круга лиц печатные, аудиосообщения, аудиовизуальные и иные сообщения и материалы. Данное определение содержится в Законе РФ «О средствах массовой информации».

Цифровая информация – информация на отчуждаемом машинном носителе, в ЭВМ, локальной или глобальной сети.

Также стоит отметить три основных свойства защищаемой от каких бы то ни было угроз информации: конфиденциальность, целостность,

⁷ Бачило, И. Л. Информационное право : учебник для академического бакалавриата / И. Л. Бачило. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. - С.54

доступность⁸:

конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

целостность – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

доступность – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

1.2 Понятие информационной безопасности

Наиболее правильный с методологической точки зрения подход к проблемам конституционно-правового регулирования информационной безопасности личности в РФ начинается с определения понятия «информационная безопасность». Понятие «информация» было рассмотрено в предыдущем параграфе, следовательно, рассмотреть необходимо понятие «безопасность».

Понятие «информационная безопасность» является видовым по отношению к родовому понятию «безопасность» и включает в свое содержание признаки, присущие понятию «безопасность», а также признаки, характеризующие видовое отличие и связанные с содержанием понятия «информация».

Безопасность — состояние защищённости жизненно важных интересов личности, общества, государства от внутренних и внешних угроз, либо способность предмета, явления или процесса сохраняться при разрушающих воздействиях.⁹

Понятие «информационная безопасность» приобрело актуальность и практическую значимость с того периода, когда началось бурное развитие информационных и телекоммуникационных технологий.

⁸ «ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» (утв. и введен в действие Приказом Ростехрегулирования от 18.12.2008 N 532-ст) из информационного банка «Отраслевые технические нормы» // URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=4460#023687718055429452> (дата обращения: 14.12.2017 г.)

⁹ Безопасность // Гражданская защита: Энциклопедия в 4-х томах. — Т. I. А—И. — М.: ФГБУ ВНИИ ГОЧС (ФЦ), 2015.

При определении информационной безопасности, очень важно понимать, что она представляет собой социальное, а не чисто техническое явление¹⁰. Безусловно, что информационная безопасность предполагает применение специальных технических средств и методов для защиты информации от несанкционированного доступа, похищения, уничтожения, но при этом не должно происходить отождествление указанных понятий. В противном случае, неоправданно сужается само понятие «информационная безопасность», а соответственно и проблема конституционно-правового регулирования информационной безопасности личности сводится исключительно к регулированию области применения технических средств и методов. Следовательно, информационная безопасность, это не только защита информации, но и организационные, правовые и другие меры, направленные на обеспечение устойчивого, стабильного развития личности, общества и государства.

Понятие «информационная безопасность» представляет собой довольно сложное явление, этим и обуславливается различие подходов к его формулированию.

На заре формирования информационной безопасности как концепции в докладе Генерального секретаря ООН говорилось, что информационная безопасность – состояние защищенности основных интересов личности, общества и государства в информационном пространстве, включая информационно-телекоммуникационную инфраструктуру и собственно информацию в отношении таких ее свойств как целостность, объективность, доступность и конфиденциальность. Что практически в полной мере раскрывает суть понятия и на сегодняшний день.

В Доктрине информационной безопасности Российской Федерации 2000 года под информационной безопасностью Российской Федерации собственно и понималось состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью

¹⁰ См.: Колобов О.А., Яснев В.Н. Информационная безопасность и антитеррористическая деятельность современного государства: проблемы правового регулирования и варианты их решения. — Н. Новгород: Фин. фак-т ННГУ, 2011.

сбалансированных интересов личности, общества и государства. В Доктрине информационной безопасности РФ 2016 года это определение отсутствует.

Стоит отметить, что понятие информационной безопасности в данном случае стоит рассматривать во взаимосвязи с таким его неотъемлемым компонентом, как защита информации. Если информационная безопасность – это состояние защищенности, то защита информации – это *процесс* обеспечения этой защищенности.

Защита информации; ЗИ: деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию¹¹.

Следует рассмотреть и иные возможные определения понятия «информационная безопасность».

В определении, предложенным Лопатиным В.Н., под информационной безопасностью следует понимать состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз.

Некоторые авторы определяют понятие «информационная безопасность» в широком и в узком смысле: информационная безопасность в широком смысле представляет собой состояние защищенности информационных ресурсов, информационных каналов и открытого доступа к любому источнику информации каждого гражданина, общественной организации, отдельного государства в целом. Информационная безопасность в узком смысле – компонент военной безопасности, относящийся к защите информационных ресурсов, каналов, баз данных и знаний, средств их переработки и хранения, используемый чисто в военных целях, защищающий жизненно важные интересы граждан, общества и государства.¹²

Правовое определение информационной безопасности содержалось раньше в ФЗ «Об участии в международном информационном обмене». В

¹¹ ГОСТ Р 50922-2006. Защита информации. Основные термины и определения // URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=25219#014315363912808288> (дата обращения 12.01.2018 г.)

¹² Везилов В.Н., Степанов В.Е., Красой Н.И., Бармин Л.В., Лисов О.М. Информационное противоборство - новая глобальная опасность для человечества. // Вопросы защиты информации № 4, 1999. - С. 8.

соответствии с которым информационная безопасность — это «состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование, и развитие в интересах граждан, организаций, государства»¹³. Однако в связи с тем, что данный закон утратил силу в настоящее время правового определения информационной безопасности в законодательстве РФ не существует.

Понятие «информационная безопасность» приобрело комплексное и неоднозначное значение в зависимости от используемого контекста. В современном мире его часто путают с понятием «кибербезопасности» (реализацией мер по защите систем, сетей и программных приложений от цифровых атак.), компьютерной безопасности и многими другими подразделами информационной безопасности.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества; в использовании информации и информационной инфраструктуры для разъяснения населению страны и международной общественности содержания и направленности государственной политики; в создании условий для гармоничного развития информационной инфраструктуры.

Также стоит добавить несколько определений, необходимых для понимания сущности понятия «информационная безопасность» личности, общества, государства.

¹³ Данный Федеральный закон утратил силу в связи с принятием Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, «Российская газета», № 165, 29.07.2006.

Угроза «информационной безопасности» – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется атакой на информационную систему. Лица, преднамеренно реализующие угрозы, являются злоумышленниками (в случае юридических, физических лиц) или же противниками (в случае реализации угрозы национальным интересам Российской Федерации).

Угрозы информационной безопасности классифицируются по нескольким признакам:

- по составляющим информационной безопасности (доступность, целостность, конфиденциальность), против которых, в первую очередь, направлены угрозы;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, персонал);
- по характеру воздействия (случайные или преднамеренные, действия природного или техногенного характера);
- по расположению источника угроз (внутри или вне рассматриваемой информационной системы).

Источники угроз информационной безопасности – понимаются как исходные основания (причины) опасного воздействия на жизненно важные интересы личности, общества и государства в информационной сфере.

Уязвимость (в информационной безопасности) – потенциально существующая брешь в режиме информационной безопасности гражданина, организации, общества государства, будь то пробелы в законодательстве или существующие потенциально опасные недостатки в каких-либо используемых технических средствах телекоммуникации, а также особенности личности. Данная брешь может быть использована источником угрозы (намеренно или непреднамеренно

1.3 Правовое обеспечение информационной безопасности

Под конституционно-правовым регулированием информационной безопасности личности понимается совокупность конституционных и иных правовых норм, регулирующих общественные отношения по защите ее жизненно важных интересов от угроз в информационной сфере.

Содержание конституционно-правового регулирования информационной безопасности личности определяется задачами и принципами его развития: обеспечение верховенства закона, целостность, внутривидовая иерархия и непротиворечивость, непротиворечивость подзаконных актов законодательным актам, гласность и общедоступность, минимизация новых законодательных актов, исключение дублирования и т.д.

Под источниками конституционно-правового регулирования информационной безопасности личности следует понимать Конституцию РФ, а также нормативно-правовые акты, принятые уполномоченными органами и содержащие правовые нормы, регулирующие отношения в сфере сбора, обработки, накопления, хранения, распределения, передачи и пользования информацией.

Поскольку информация проникает во все сферы деятельности граждан, юридических лиц, государства, то правовые нормы, составляющие конституционно-правовое регулирование информационной безопасности, можно систематизировать по вертикали (видам нормативно-правовых актов) и по горизонтали (отраслям законодательства).

При проведении анализа конституционно-правового регулирования информационной безопасности в первую очередь необходимо исследовать федеральное законодательство.

В соответствии с общими для всех отраслей законодательства принципами нормативно-правовые акты в области обеспечения информационной безопасности личности, на основании принципа субординации («по вертикали») различаются по своей юридической силе.

При вертикальном структурировании в основе иерархии нормативноправовых актов лежит Конституция РФ, которая занимает высшее место в системе конституционно-правового регулирования информационной безопасности личности. В ней содержатся как нормы, непосредственно посвященные проблемам обеспечения информационной безопасности личности, так и те, которые создают правовые предпосылки для регулирования отношений в данной сфере. Конституция РФ обладает верховенством над законами и иными актами, которые должны исходить из Конституции РФ и не противоречить ей. Причем соответствовать Конституции РФ должны не только акты федерального законодательства, но и акты органов государственной власти субъектов Федерации, а также органов местного самоуправления. Конституция РФ формирует и закрепляет отправные принципы правового регулирования информационной безопасности личности, имеет прямое действие, является базой всего законодательства и представляет собой акт, обладающий высшей юридической силой.

Конституционные положения конкретизируются в федеральных конституционных и федеральных законах, указах Президента РФ, постановлениях Правительства РФ, нормативно-правовых актах федеральных органов исполнительной власти, имеющих прямое отношение к информационной сфере и области информационной безопасности личности в частности.^{14 15}

Конституция РФ в п. «и» ст.71 закрепляет положение, согласно которому федеральные информация и связь находятся в ведении РФ. Указанная статья фактически определяет компетенцию РФ в решении вопросов об информации и связи, устанавливает федеральную собственность на важнейшие информационные ресурсы и объекты информационной инфраструктуры. Федерация регулирует отношения, связанные с информацией, информатизацией и информационной

¹⁴ Мелехин А.В. Теория права и государства. - Москва : Юстиция, 2019. - С. 41.

¹⁵ Конституция РФ принята всенародным голосованием 12.12.1993, «Российская газета», № 237, 25.12.1993.

безопасностью, которые возникают при: формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации, а также в рамках гражданских правоотношений, возникающих из авторского права и смежных прав. Объектами регулирования выступают документированная информация, информационные ресурсы, продукты, услуги и средства информационного обмена.

В соответствии со статьей 73 Конституции РФ региональная информатизация, связь и информационные ресурсы относятся к полномочиям субъектов РФ.

Обеспечение безопасности личности в информационной сфере является одним из наиболее важных вопросов, подлежащих конституционноправовому регулированию. Социальные интересы человека, которые необходимо охранять в информационном обществе, состоят в реальном обеспечении прав и свобод человека на доступ к открытой информации, на использование информации в интересах осуществления не запрещенной законом деятельности, а также в защите информации, обеспечивающей личную безопасность, духовное и интеллектуальное развитие.

Права и свободы в информационной сфере относятся к основным правам и свободам человека и гражданина. В соответствии со ст. 2 Конституции РФ: «Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина — обязанность государства». Информационная безопасность личности — это ни что иное, как защищенность основных конституционных прав и свобод человека, поэтому необходимость уровня конституционного регулирования указанной области очевидна.

В статье 29 Конституции РФ провозглашается и гарантируется свобода мысли и слова, свобода идей, мнений, убеждений и их гласного выражения. Соблюдать эти положения должна каждая отдельная личность, все структуры общества, органы государственной власти. Часть 4 статьи 29 гарантирует свободу информации, являющуюся важнейшим элементом прав и свобод человека, общепризнанной основой демократических механизмов взаимодействия власти и общества, различных структур гражданского общества и отдельных личностей. Реализация прав, провозглашенных в статье 29, возлагает на государство и общество обязанности по формированию информационной сферы, по созданию условий для оперативного, полного и достоверного обеспечения информацией каждого члена общества. В части 5 статьи 29 Конституции РФ содержится еще одна важная норма, которая гарантирует свободу массовой информации и запрещает цензуру.

Вопросы, связанные с реализацией права на доступ к информации регулируются ФЗ «Об информации, информационных технологиях и о защите информации». В соответствии с пунктом 3 статьи 3 данного ФЗ правовое регулирование отношений, возникающих в информационной сфере, основывается на принципе открытости и свободного доступа к информации о деятельности государственных органов и органов местного самоуправления, за исключением информации, отнесенной законом к категории ограниченного доступа.

Граждане наряду с органами государственной власти, органами местного самоуправления, организациями и общественными объединениями обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцем этих ресурсов необходимость получения запрашиваемой ими информации.¹⁶ Такое право на доступ к информации является основой осуществления общественного контроля за деятельностью органов государственной власти и местного

¹⁶ Федеральный закон от 27.07.2006 № 149-ФЗ, «Российская газета», № 165, 29.07.2006.

самоуправления, общественных, политических и иных организаций, а также за состоянием экономики, экологии и других сфер общественной жизни.

Для обеспечения конституционного права на информацию необходимо четкое правовое регулирование информационного взаимодействия граждан с государственными органами и органами местного самоуправления.

В Конституции определены некоторые конкретные источники информации, доступ к которым гарантирован государством. Так, пунктом 2 статьи 24 Конституции установлена обязанность органов государственной власти и местного самоуправления, их должностных лиц обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы.

Данное конституционное положение возлагает на органы государственной власти и местного самоуправления, их должностных лиц обязанность знакомить заинтересованных лиц с документами и материалами, непосредственно затрагивающими их права и свободы, однако его реализация содержит ограничения. Ознакомиться с соответствующими документами и материалами могут только лица, чьих прав и свобод они касаются. Следовательно, круг лиц ограничен непосредственно заинтересованными лицами, а круг документов и материалов — только теми, в которых затрагиваются права и свободы обращающихся за информацией лиц. Существует и еще одно ограничение — заинтересованное лицо может реализовать предоставленное ему право, если иное не предусмотрено законом и только законом, а не любым подзаконным актом. Поэтому, если отказ в ознакомлении обуславливается иным, чем закон, нормативным актом, то такой отказ противоречит Конституции, и, следовательно, может быть обжалован.

Кроме того, правовую основу обеспечения информационной безопасности образует и ряд указов Президента РФ. Так, согласно Указу Президента РФ «О дополнительных гарантиях прав граждан на информацию» деятельность государственных органов, организаций,

предприятий, общественных объединений, должностных лиц должна осуществляться на принципе информационной открытости¹⁷.

Право граждан на ознакомление с документами и материалами, непосредственно затрагивающими их права и свободы, закреплено в пункте 2 статьи 8 ФЗ «Об информации, информационных технологиях и о защите информации»¹⁸, согласно которому гражданам и организациям предоставлено право на получение информации о них¹⁹.

Пользование любыми свободами, включая свободу информации, налагает определенные ограничения и ответственность. Именно поэтому в части 2 статьи 29 Конституции РФ вводится запрет на распространение информации, содержание которой направлено на подрыв демократических основ гражданского общества, а УК РФ устанавливает нормы ответственности за правонарушения в области информационной безопасности.

Всю информацию с ограниченным доступом по условиям ее правового режима ФЗ «Об информации, информационных технологиях и о защите информации» подразделяет на информацию, отнесенную к сведениям составляющим государственную тайну²⁰, коммерческую тайну²¹, служебную

¹⁷ Принцип информационной открытости выражается в доступности для граждан информации, представляющей общественный интерес или затрагивающей их личные интересы; в систематическом информировании граждан о предполагаемых или принятых решениях; в осуществлении гражданами контроля за деятельностью государственных органов, организаций и предприятий, общественных объединений, должностных лиц и принимаемыми ими решениями, связанными с соблюдением, охраной и защитой прав и законных интересов граждан. Последний пункт является ключевым, поскольку поднимает доступ к информации до уровня гражданского контроля.

¹⁸ Федеральный закон от 27.07.2006 № 149-ФЗ, «Российская газета», № 165, 29.07.2006.

¹⁹ Иными словами, гражданин при реализации права на свободный поиск и получение информации может обратиться к органам государственной власти, органам местного самоуправления, общественным организациям (объединениям), хозяйствующим субъектам, их должностным лицам с запросом информации, затрагивающей его права и свободы, т.е. имеет право на получение, например, «достоверной информации» о состоянии окружающей среды, а также на «возмещение ущерба, причиненного его здоровью или имуществу экологическим правонарушением» (ст.42 Основного закона). За отказ в предоставлении гражданину данной информации, в соответствии со статьей 5.39 КоАП РФ предусмотрена административная ответственность.

²⁰ В Законе РФ «О государственной тайне» государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ. Закон не конкретизирует, а лишь устанавливает перечень сведений, относимых к государственной тайне. Перечень должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне, утверждается Президентом РФ.

²¹ В ФЗ «О коммерческой тайне» коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать

тайну²², профессиональную тайну²³ и персональные данные. Обязательным является^{24 25} соблюдение конфиденциальности информации ограниченного доступа. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. Конфиденциальность информации определяет и доверяет посторонним лицам обладатель этой информации. В отличие от конфиденциальной информации государственная тайна определяется государством через соответствующие государственные органы, получение и разглашение этой информации строго регламентировано нормативными актами, информация имеет гриф секретности.

В соответствии со статьей 313 НК РФ содержание данных налогового учета (в том числе данных первичных документов) является налоговой тайной, а статьей 26 «Банковская тайна» ФЗ «О банках и банковской деятельности»^{26 27} установлено, что кредитная организация, Банк России гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов.

Отдельные нормы, посвященные соблюдению конфиденциальности информации и защите различных видов тайн, содержатся также в статьях 15, 17 ФЗ «Об экспортном контроле»;²⁸ статьях 7, 9, 10 ФЗ «О противодействии

неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

²² Служебная тайна – это охраняемая законом конфиденциальная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости, а также ставшая известной в государственных органах и органах местного самоуправления только на законном основании и в силу исполнения их представителями служебных обязанностей, имеющая действительную или потенциальную ценность в силу неизвестности ее третьим лицам.

²³ Профессиональная тайна – это охраняемые законом конфиденциальные сведения, доверенные или ставшие известными лицу исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, незаконное получение или распространение которых может повлечь за собой вред правам и законным интересам другого лица, доверившего эти сведения, и привлечение к ответственности в соответствии с действующим законодательством.

²⁴ Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне», «Российская газета», № 182, 21.09.1993.

²⁵ Статья 9 Федерального закона от 27.07.2006 № 149-ФЗ, «Российская газета», № 165, 29.07.2006.

²⁶ Налоговый кодекс Российской Федерации (часть вторая) от 05.08.2000 № 117-ФЗ (ред. От 29.09.2019), «Собрание законодательства РФ», 02.12.2019, № 48, ст. 3340,

²⁷ Федеральный закон «О банках и банковской деятельности» от 02.12.1990 N 395-1 (последняя редакция) // URL: http://www.consultant.ru/document/cons_doc_LAW_5842/ (дата обращения 07.03.2018 г.)

²⁸ Федеральный закон от 18 июля 1999 г. N 183-ФЗ «Об экспортном контроле» в ред. от 13 июля 2015 г. // Российская газета от 29 июля 1999 г. N 146

легализации (отмыванию) доходов, полученных преступным путем»;²⁹ статьях 28, 55 ФЗ «Об инвестиционных фондах» и других нормативно-правовых актах.

Важное значение для развития конституционно-правового регулирования информационной безопасности имеют нормы, связанные с защитой информации, гарантирующие конфиденциальность формирования и использования информационных ресурсов, охватывающих сведения о личности (персональные данные). В 2006 году был принят закон «О персональных данных»³⁰, который наиболее детально урегулирует вопросы сбора и распространения информации о частной жизни граждан³¹. За преступления в рассматриваемой сфере предусмотрена уголовная ответственность.

К числу правовых норм, регулирующих отношения в информационной сфере, можно также отнести норму, содержащуюся в ч. 1 ст. 44 Конституции РФ, в которой говорится: «Интеллектуальная собственность охраняется законом», на том основании, что к объектам интеллектуальной собственности относятся программные средства для ЭВМ, базы данных и компьютерные технологии и иные вариации.

Признание прав и свобод в информационной сфере человека и гражданина непосредственно действующими (ст. 18 Конституции РФ), то есть их осуществление не зависит напрямую от того, признает их государство или нет. Государство не дарует человеку права и свободы, оно

²⁹ Федеральный закон от 7 августа 2001 г. N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» в ред. от 02.08.2019 г. // Собрание законодательства Российской Федерации от 13 августа 2001 г. № 33 (Часть I) ст. 3418.

³⁰ Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ в ред. от 31.12.2017 г. // Российская газета от 29 июля 2006 г. № 165.

³¹ В указанном законе устанавливаются общие унифицированные требования к обработке персональных данных во всех сферах, где используются эти данные, определяются права субъектов персональных данных и обязанности операторов, осуществляющих обработку данных, принципы трансграничной передачи персональных данных, а также меры государственного контроля за деятельностью государственных и муниципальных органов, юридических и физических лиц, связанной с обработкой персональных данных. Данным законом допускаются различные способы учета персональных данных в государственных и муниципальных информационных системах, в том числе различные способы обозначения принадлежности персональных данных конкретному лицу. Однако при этом устанавливается запрет на ограничение прав и свобод граждан по мотивам, связанным со способами учета и обозначения принадлежности персональных данных, включая запрет на использование таких способов обозначения, которые оскорбляли бы чувства граждан или унижали человеческое достоинство.

лишь познает и закрепляет их в своем законодательстве. Именно права и свободы человека и гражданина определяют смысл, содержание и применение законов, деятельность законодательной и исполнительной власти, местного самоуправления и обеспечиваются правосудием. Благодаря своим юридическим свойствам, нормативности Конституция, ее положения о правах и свободах оказывают непосредственное регулирующее воздействие на общественные отношения. При этом права и свободы признаются непосредственно действующими независимо от того, существуют или еще нет законодательные акты, призванные при необходимости их конкретизировать, определять правила, механизмы и процедуры для их наиболее эффективного осуществления. Каждый субъект права – государственный, муниципальный или общественный орган, должностное лицо, государственный служащий или гражданин – должен сверять свои юридически значимые действия прежде всего с Конституцией, руководствоваться ею. Она является правовым основанием для отмены актов и пресечения действий, которые ей противоречат. При защите в суде, ином органе своих прав и свобод правомерна ссылка непосредственно на конституционные нормы, как правомерна такая ссылка и со стороны этих органов при принятии ими решения.

Таким образом, проведенный анализ конституционно-правового регулирования информационной безопасности личности показывает, что основная часть правовых норм, регулирующих отношения в рассматриваемой области, закрепляется нормативно-правовыми актами федерального уровня, что, видимо, обусловлено отнесением вопросов безопасности, а также федеральной информации и связи к ведению РФ.

Конституционно-правовые нормы, образующие правовое закрепление общественных отношений, связанных с обеспечением информационной безопасности личности, регулируют данные отношения в области прав человека и гражданина: на доступ к информации; на неприкосновенность частной жизни; на информацию с ограниченным доступом; на объекты

интеллектуальной собственности; на защиту от воздействия недоброкачественной информации.

Что же касается правовых документов регламентирующих основы государственной политики Российской Федерации в сфере информационной безопасности, то прежде всего необходимо выделить Стратегию развития информационного общества в Российской Федерации на 2017 – 2030 годы³² утв. указом Президента РФ от 09.05.2017 N 203. Данный документ:

- определяет цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в области информационно-коммуникационные технологии, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов

- стремится обеспечить следующие национальные интересы, такие как развитие человека, обеспечение безопасности граждан и государства, повышение роли России в мировом гуманитарном и культурном пространстве, развитие свободного, устойчивого и безопасного взаимодействия граждан и организаций, органов государственной власти России и местного самоуправления; повышение эффективности государственного управления, экономического и социального развития; формирование цифровой экономики;

- определяет приоритет областей, которые считаются важными для успешного развития российских информационных и коммуникационных технологий, в том числе нового поколения электронных сетей, эффективной обработки больших массивов данных, искусственного интеллекта, электронной идентификации и аутентификации (с особым акцентом на банковском деле), облачных и туманных вычислений, Промышленного Интернета и Интернета вещей (Internet of Things), робототехники и

³² Указ Президента РФ от 9 мая 2017 г. N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // Собрание законодательства Российской Федерации от 15 мая 2017 г. № 20 ст. 2901.

биотехнологии; и информационной безопасности.

Следующим документом в сфере информационной безопасности является Доктрина информационной безопасности Российской Федерации³³ утв. указом Президента РФ от 05.12.2016 N 646. Данный документ определяет следующие ключевые направления обеспечения информационной безопасности в сфере национальной безопасности:

- обеспечение стратегического сдерживания и предотвращение военных конфликтов, которые могут быть вызваны использованием информационных технологий;
- модернизацию системы информационной безопасности Вооруженных Сил, других войск, воинских формирований и органов, включая силы и средства информационного противостояния;
- прогнозирование, выявление и оценка информационных угроз, в том числе угроз Вооруженным Силам Российской Федерации в информационной сфере;
- продвижение интересов союзников Российской Федерации в информационной сфере;
- противодействие информационно-психологическим действиям, в том числе направленным на подрыв исторических устоев и патриотических традиций, связанных с защитой родины.

В Стратегии национальной безопасности Российской Федерации утв. указом Президента РФ от 31.12.2015 N 683³⁴ ряд важных положений, к числу которых можно отнести:

- усиливающееся противостояние на мировой информационной арене оказывает все большее влияние на характер международной обстановки;
- определение основных угроз безопасности России, включающих действия, связанные с использованием информационных и

³³ Указ Президента РФ от 5 декабря 2016 г. N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации от 12 декабря 2016 г. № 50 ст. 7074.

³⁴ Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации» // URL: http://www.consultant.ru/document/cons_doc_LAW_191669/ (дата обращения: 5.06.2018 г.)

коммуникационных технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, а также для угроз гражданскому миру и политической и социальной стабильности в обществе.

- совершенствование системы выявления и анализа угроз в информационной сфере и противодействия им;

- принятие мер по усилению защиты граждан и общества от воздействия разрушительной информации от экстремистских и террористических организаций, иностранных спецслужб и пропагандистских структур.

- повышение уровня технологической безопасности, в том числе в информационной сфере, как одно из основных направлений обеспечения национальной безопасности.

В Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом РФ 12.12.2014 N К 1274)³⁵ определены цель, функции и принципы создания государственной системы обнаружения, предотвращения и устранения последствий компьютерных атак на информационные ресурсы.

В Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013 N Пр-1753)³⁶ определены:

- основные угрозы в области международной информационной безопасности, цели, задачи и приоритетные направления государственной политики в области международной информационной безопасности, а также механизмы реализации до 2020 года;

³⁵ Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (утв. Президентом РФ 12.12.2014 N К 1274) // URL: http://www.consultant.ru/document/cons_doc_LAW_181661/ (дата обращения: 11.07.2018 г.)

³⁶ «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» (утв. Президентом РФ 24.07.2013 N Пр-1753)» // URL: <http://base.garant.ru/70641072/> (дата обращения: 20.08.2018 г.)

– угрозы в этой области: информационное оружие для военных и политических целей; терроризм; вмешательство во внутренние дела; и преступления;

– основные направления государственной политики на двустороннем, многостороннем, региональном и глобальном уровнях.

Помимо перечисленных правовых документов, следует назвать также и Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом РФ 03.02.2012 N 803)³⁷. Названный документ направлен на повышение безопасности информационных и телекоммуникационных систем и критических инфраструктур и объектов путем снижения любого риска неконтролируемых помех в работе этих систем до минимально возможного уровня.

Также разработана Государственная программа Российской Федерации «Информационное общество (2011 – 2020 годы)»³⁸, которая включает шесть подпрограмм, в т.ч. безопасность в информационном обществе

В названном документе определены цели и задачи, которые заключаются в том, чтобы:

- улучшить качество жизни и условий для ведения бизнеса;
- обеспечить работу электронного правительства и эффективного государственного управления;
- развить российский рынок информационно-коммуникационных технологий и принять меры по переходу на цифровую экономику;
- устранить цифровой разрыв и создание базовой инфраструктуры информационного общества.

³⁷ «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» (утв. Президентом РФ 03.02.2012 N 803) // URL: http://www.consultant.ru/document/cons_doc_LAW_150730/ (дата обращения 02.08.2018 г.)

³⁸ Федеральный закон от 02.12.2013 N 349-ФЗ (ред. от 26.12.2014) «О федеральном бюджете на 2014 год и на плановый период 2015 и 2016 годов» // URL: http://www.consultant.ru/document/cons_doc_LAW_155198/ (дата обращения: 02.08.2018 г.)

– обеспечить безопасность в информационном обществе;

Федеральный проект «Информационная безопасность» (часть Национальной программы «Цифровая экономика Российской Федерации»³⁹) включает в себя ряд целей и мероприятий на период с ноября 2018 года по декабрь 2024 года, основной целью которых является обеспечение информационной безопасности на основе национальных изобретений для передачи, обработки и хранения данных для обеспечения защиты интересов личности, бизнеса и государства.

1.4 Криптографические методы и средства обеспечения информационной безопасности

По поручению Правительства Российской Федерации разработаны Требования по защите информации в информационных системах общего пользования. В них, в частности, определены такие виды средств защиты информации, как СЗИ от неправомерных действий (в том числе — средства криптографической защиты информации), средства обнаружения вредоносных программ (в том числе — антивирусные средства), средства контроля доступа к информации (в том числе — средства обнаружения компьютерных атак), средства фильтрации и блокирования сетевого трафика (в том числе — средства межсетевого экранирования). Использование таких СЗИ должно обеспечить требуемый уровень защищенности.

Средства защиты информации, реализующие алгоритмы криптографического преобразования информации, относят к криптографическим средствам защиты информации⁴⁰. Разработка, изготовление и распространение их является лицензируемым видом деятельности. Средства криптографической защиты активно используются

³⁹ «Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 N 7) // URL: http://www.consultant.ru/document/cons_doc_LAW_328854/ (дата обращения: 04.08.2018 г.)

⁴⁰ ГОСТ Р 50922-2006. Защита информации. Основные термины и определения // URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=25219#014315363912808288> (дата обращения 20.08.2018 г.)

для защиты различных информационных систем органов государственной власти Российской Федерации, содержащих персональные данные граждан, информацию для служебного пользования, сведения, отнесенные к государственной тайне, сведения, классифицируемые как иная тайна (врачебная, налоговая и тд) согласно действующему законодательству и любую другую информацию ограниченного доступа.

Согласно постановлению Правительства РФ от 16.04.2012 N 313 (ред. от 18.05.2017) «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств....» принято различать:

- средства шифрования;
- средства имитозащиты;
- средства электронной подписи;
- средства кодирования;
- средства изготовления ключевых документов;
- ключевые документы;
- аппаратные шифровальные (криптографические) средства;
- программные шифровальные (криптографические) средства;
- программно-аппаратные шифровальные (криптографические) средства.

В первом случае речь идет о криптографических СЗИ, обеспечивающих возможность разграничения доступа к ней. Средства шифрования, в которых часть криптопреобразований осуществляется с использованием ручных операций или автоматизированных средств, предназначенных для выполнения таких операций, называют средствами кодирования.

Электронные документы, содержащие ключевую информацию, необходимую для выполнения криптографических преобразований с помощью средств шифрования, принято называть ключевыми документами.

Средства шифрования, обеспечивающие создание ключевых

документов, называют средствами изготовления ключевых документов. Защиту от навязывания ложной информации, возможность обнаружения изменений информации с помощью реализованных в СЗИ криптографических механизмов предоставляют средства имитозащиты.

Криптографические СЗИ, обеспечивающие создание электронной цифровой подписи с использованием закрытого ключа, подтверждение с использованием открытого ключа подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи относят к средствам электронной подписи.

Суть различий последних трех видов шифровальных средств, указанных выше, очевидно следует из их названий⁴¹.

ФСБ России определены⁴² классы криптографических СЗИ: КС1, КС2, КС3, КВ и КА.

К основным особенностям СЗИ класса КС1 относится их возможность противостоять атакам, проводимым из-за пределов контролируемой зоны. При этом подразумевается, что создание способов атак, их подготовка и проведение осуществляется без участия специалистов в области разработки и анализа криптографических СЗИ. Предполагается, что информация о системе, в которой применяются указанные СЗИ, может быть получена из открытых источников.

Если криптографическое СЗИ может противостоять атакам, блокируемым средствами класса КС1, а также проводимым в пределах контролируемой зоны, то такое СЗИ соответствует классу КС2. При этом допускается, например, что при подготовке атаки могла стать доступной

⁴¹ Приказ ФСБ РФ от 09.02.2005 N 66 (ред. от 12.04.2010) «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (Зарегистрировано в Минюсте РФ 03.03.2005 N 6382) // URL: <http://base.garant.ru/187947/> (дата обращения: 16.10.2018 г.).

⁴² Приказ ФСБ России от 10.07.2014 N 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (Зарегистрировано в Минюсте России 18.08.2014 N 33620) // URL: http://www.consultant.ru/document/cons_doc_LAW_167862/ (дата обращения: 16.10.2018 г.).

информация о физических мерах защиты информационных систем, обеспечении контролируемой зоны и пр.

В случае возможности противостоять атакам при наличии физического доступа к средствам вычислительной техники с установленными криптографическими СЗИ говорят о соответствии таких средств классу КСЗ.

Если криптографическое СЗИ противостоит атакам, при создании которых участвовали специалисты в области разработки и анализа указанных средств, в том числе научно-исследовательские центры, была возможность проведения лабораторных исследований средств защиты, то речь идет о соответствии классу КВ.

Если к разработке способов атак привлекались специалисты в области использования недеklarированных (скрытых, нигде не описанных) возможностей системного программного обеспечения, была доступна соответствующая конструкторская документация и был доступ к любым аппаратным компонентам криптографических СЗИ, то защиту от таких атак могут обеспечивать средства класса КА.

Средства электронной подписи в зависимости от способностей противостоять атакам принято сопоставлять со следующими классами: КС1, КС2, КС3, КВ1, КВ2 и КА1. Эта классификация аналогична рассмотренной выше в отношении криптографических СЗИ.

На основании рассмотренного теоретического материала по конституционно-правовому регулированию информационной безопасности Российской Федерации было установлено следующее.

Информационная безопасность – это состояние защищенности основных интересов личности, общества и государства в информационном пространстве.

Интересы общества в информационной сфере заключаются в создании правового государства, обеспечении интересов личности в указанной сфере, а также социальной стабильности и экономического процветания.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в создании условий для гармоничного развития информационной инфраструктуры.

Права и свободы в информационной сфере относятся к основным правам и свободам человека и гражданина. Информационная безопасность личности - это ни что иное, как защищенность основных конституционных прав и свобод человека, этим обусловлена необходимость уровня конституционного регулирования указанной области.

Основная часть правовых норм, регулирующих отношения в рассматриваемой области, закрепляется нормативно-правовыми актами федерального уровня, что обусловлено отнесением вопросов безопасности, а также федеральной информации и связи к ведению РФ.

Из документов, регламентирующих государственную политику в области информационной безопасности следует выделить Стратегию развития информационного общества в Российской Федерации на 2017 – 2030 годы, Доктрину информационной безопасности Российской Федерации 2016 года, Стратегию национальной безопасности Российской Федерации утв. указом Президента РФ от 31.12.2015 N 683. Все они направлены на обеспечение защиты интересов личности, общества и государства в информационной сфере, на развитие и совершенствование информационного общества в Российской Федерации и защиту интересов России на международной арене.

Среди прочих методов и средств защиты стоит отметить получившие на настоящий момент значительное распространение криптографические методы и средства защиты информации, реализующие криптографическое

преобразования информации (шифрование). Криптографические методы и средства защиты информации классифицируются в зависимости от их способности противостоять атакам

2 Организационно-правовое и техническое обеспечение отдельных субъектов и объектов информационной безопасности

2.1 Понятие правовой защиты информации

Ни одна сфера жизни современного общества не может функционировать без развитой информационной структуры. Проникая во все сферы деятельности государства, информация приобретает политическое, материальное и стоимостное выражение. Идет объективный процесс развития информационного общества, в котором информационная деятельность является основой экономического процветания и благополучия.

Однако именно через информационную сферу зачастую осуществляются угрозы национальной безопасности в разных областях деятельности государства. Глобальная информатизация и развитие Интернета привели к тому, что информационная инфраструктура страны, национальные информационные ресурсы, права и свободы личности оказались весьма уязвимыми объектами воздействия со стороны недружественных государств, террористических организаций, преступных групп и отдельных злоумышленников. Угроза международного информационного терроризма и информационных войн стали важными геополитическими факторами. Информационная сфера все более превращается в арену международного соперничества, противоправных действий криминальных структур, создающих опасные угрозы национальным интересам РФ и ее субъектов, реализации законных интересов личности. Выявление и анализ угроз информационной безопасности личности, выработка^{43 44} и принятие мер, необходимых для адекватного ответа на них, должны рассматриваться как важнейшие приоритеты национальной безопасности.

⁴³ Вирковский В.В. «Безопасность информационных технологий. Методология создания систем защиты». Издательство «ВелЭкспенс», Ростов, 2012 г. - С. 14.

⁴⁴ В.И. Бажуков. «Информационные войны: теория и практика». Издательство «МГУ», Москва, 2014г. - С. 34.

Но для понимания общего состояния информационной безопасности в Российской Федерации следует рассматривать её не только целостную систему, но и как отдельные компоненты этой системы на примере различных субъектов и объектов информационного взаимодействия.

Прежде всего следует отметить, что определение «правовая защита информации» не встречается ни в предыдущей, ни в действующей Доктрине информационной безопасности Российской Федерации. Строгое определение данному понятию дает ГОСТ 50922-2006: «Правовая защита информации: защита информации правовыми методами, включая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов, а также надзор и контроль за их исполнением»

Обратившись к Федеральному закону от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», можно расширить содержание правовой защиты информации, дополнив его описанием мер, которые составляют защиту информации и направлены на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации, соблюдение конфиденциальности информации ограниченного доступа и реализацию права на доступ к информации. Правовые меры в приведенном в ст. 16 Федерального закона «Об информации, информационных технологиях и о защите информации» списке при перечислении предшествуют организационным и техническим мерам.

Вместе с описанием в Федеральном законе «Об информации, информационных технологиях и о защите информации» мер ПЗИ гармонично дополняла характеристику содержания рассматриваемой категории утратившая силу Доктрина Информационной безопасности Российской Федерации 2000 года, во второй главе которой были раскрыты

методы обеспечения Информационной безопасности. Так, в п. 5 в числе общих методов вместе с организационно-техническими и экономическими отмечались и правовые (рис. 1).

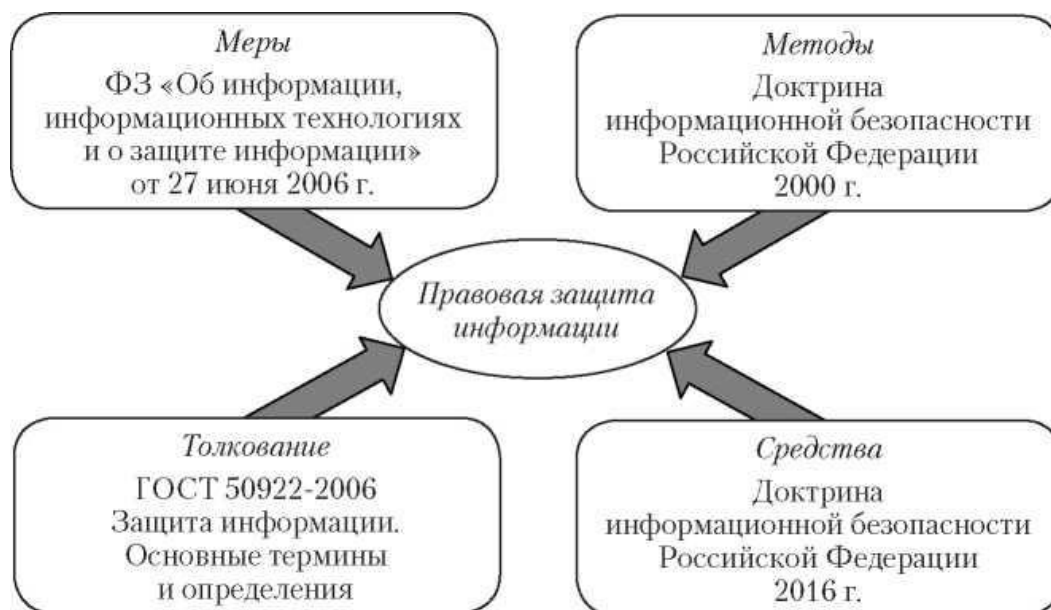


Рисунок 1. Структура правовой защиты информации

К правовым методам обеспечения информационной безопасности относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации.

Наиболее важными направлениями этой деятельности являются:

– внесение, изменений, и дополнений, в законодательство, РФ, регулирующее, отношения, в области, обеспечения, информационной, безопасности, в целях, создания и совершенствования, системы, обеспечения, информационной, безопасности Российской Федерации, устранения, внутренних, противоречий, в федеральном, законодательстве, противоречий, связанных, с международными, соглашениями, к которым, присоединилась, Российская Федерация, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации, а также, в целях, конкретизации, правовых, норм, устанавливающих, ответственность, за правонарушения, в области,

обеспечения информационной безопасности Российской Федерации;

- законодательное, разграничение, полномочий, в области, обеспечения, информационной безопасности Российской Федерации между, федеральными, органами, государственной, власти, и органами, государственной, власти, субъектов, Российской Федерации, определение, целей, задач и механизмов, участия, в этой, деятельности, общественных, объединений, организаций, и граждан;

- разработка, и принятие, нормативных, правовых, актов, Российской Федерации, устанавливающих, ответственность, юридических, и физических, лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;

- уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;

- законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;

- определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории РФ, и правовое регулирование деятельности этих организаций;

- создание правовой базы для формирования в Российской Федерации региональных, структур, обеспечения, информационной безопасности».

2.2 Информационная безопасность адвокатской деятельности

Адвокатская тайна представляет собой не просто любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю, а есть состояние запрета доступа к информации, составляющей ее содержание, посредством установления специального правового режима⁴⁵.

Таким образом, адвокатская тайна очень тесно связана с понятием «информация». Также необходимо отметить, что работа с информацией - наиболее важная, основополагающая часть работы адвоката, занимающая основную часть его рабочего времени.

В соответствии с пунктом 2 статьи 6 Кодекса профессиональной этики адвоката соблюдение профессиональной тайны является безусловным приоритетом деятельности адвоката⁴⁶. Также не вызывает сомнения и утверждение, содержащееся в пункте 1 той же статьи: «Доверия к адвокату не может быть без уверенности в сохранении профессиональной тайны».

Следовательно, с одной стороны, адвокат большую часть рабочего времени оперирует информацией, составляющей предмет адвокатской тайны. С другой - он должен обеспечить соблюдение профессиональной тайны адвоката, то есть создать достаточные условия для реализации указанного выше состояния запрета доступа к информации.

Информационная безопасность деятельности адвоката – состояние защищённости информации, составляющей предмет адвокатской тайны, при котором обеспечиваются её конфиденциальность, целостность и доступность.

В случае нарушения конфиденциальности защищаемой информации ключевым негативным последствием инцидента информационной безопасности является нарушение адвокатской тайны. В свою очередь, нарушение адвокатской тайны, то есть в данном случае получение иными

⁴⁵ Рекомендации по обеспечению адвокатской тайны и гарантий независимости адвоката при осуществлении адвокатами профессиональной деятельности // ФПА РФ. 2009. 30 ноября. Протокол № 3.

⁴⁶ Кодекс профессиональной этики адвоката (принят первым Всероссийским съездом адвокатов 31 января 2003 г. с изменениями от 22 апреля 2013 г. // Сборник законодательных и нормативных актов РФ «Экспресс-закон», декабрь 2003 г., № 45..

лицами несанкционированного доступа к информации, составляющей ее предмет, а также ее разглашение или иное неправомерное использование данной информации, может нанести существенный вред охраняемым законом правам и интересам (адвоката, доверителя и других лиц).

В случае если нарушается целостность или доступность информации, составляющей предмет адвокатской тайны, то, скорее всего, в качестве ключевого негативного последствия будет выступать не нарушение адвокатской тайны, а возможная утрата или искажение важной информации (документов, данных, сведений) по делу, что может повлечь за собой в дальнейшем оказание квалифицированной юридической помощи доверителю не в полном объеме и, как следствие, прочие негативные последствия как для доверителя, так и для адвоката.

Таким образом, обеспечение информационной безопасности деятельности адвоката гарантированно реализует и сохранение адвокатской тайны (которая, в свою очередь, представляет собой состояние запрета доступа к информации, составляющей ее содержание, т. е. состояние конфиденциальности данной информации).

Обратное не всегда верно: нарушение одной из трех составляющих информационной безопасности адвоката далеко не всегда приводит к нарушению адвокатской тайны.

Если ввести понятие политики информационной безопасности адвоката, то есть совокупности руководящих принципов, правил, процедур и практических приёмов в области безопасности информации, которыми руководствуется адвокат в своей деятельности, обеспечивающих (на допустимом уровне) информационную безопасность деятельности адвоката⁴⁷, то можно переформулировать указанный вывод следующим образом: политика информационной безопасности адвоката – это реализация на практике института адвокатской тайны.

Информационная безопасность деятельности адвоката включает в

⁴⁷ Гусятников П.П., Гусятникова П.П. Информационная безопасность адвоката: основные понятия // Пробелы в российском законодательстве. 2016. № 1.

себя не только обеспечение конфиденциальности, но и обеспечение целостности и доступности защищаемой информации, которые не охватываются понятием адвокатской тайны.

Правовой режим адвокатской тайны как института общественных отношений является, безусловно, фундаментом, без которого само его существование было бы невозможно.

Однако его практическое использование невозможно без применения адвокатом сочетания не только правовых, но и организационно-технических мер. Именно для этого Советом Федеральной палаты адвокатов Российской Федерации утверждены Рекомендации по обеспечению адвокатской тайны и гарантий независимости адвоката при осуществлении адвокатами профессиональной деятельности⁴⁸ (включая Приложение № 2⁴⁹ к указанным рекомендациям, озаглавленное «Рекомендуемые практические меры по защите информации, составляющей предмет адвокатской тайны» (далее – Рекомендации по обеспечению адвокатской тайны, или просто Рекомендации)).

Вопросы обеспечения целостности и доступности этой информации в Рекомендациях затрагиваются лишь опосредованно. С одной стороны, это видится разумным, так как это рекомендации по обеспечению именно адвокатской тайны. С другой стороны, целостность и доступность информации, составляющей предмет адвокатской тайны, не менее важна.

Закон об адвокатуре и Кодекс профессиональной этики адвоката не только обязывают адвоката сохранять профессиональную тайну (т. е. обеспечивать конфиденциальность информации, составляющей ее предмет). Адвокат также должен полностью обеспечить безопасность этой

⁴⁸ Рекомендации по обеспечению адвокатской тайны и гарантий независимости адвоката при осуществлении адвокатами профессиональной деятельности утвержден решением Совета ФПА РФ от 30 ноября 2009 года (протокол N 3) // URL: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=498244#0006254504286688278> (дата обращения 21.11.2018 г.)

⁴⁹ Указанное Приложение № 2 к Рекомендациям как раз и представляет собой рекомендованный набор практических организационно-технических мер по защите информации. Фактически это и есть в некотором виде комплекс мер по обеспечению информационной безопасности деятельности адвоката, но в первую очередь направленных на реализацию института адвокатской тайны, то есть на обеспечение конфиденциальности информации, составляющей ее предмет.

информации, то есть обеспечить еще и ее целостность и доступность, так как без обеспечения целостности и доступности информации невозможно говорить о разумном и добросовестном отстаивании прав доверителя. Иными словами, в процессе своей профессиональной деятельности адвокат обязан обеспечить ее информационную безопасность именно в смысле данного выше определения понятия.

Таким образом, можно подвести следующие итоги. Во-первых, используемое понятие информационной безопасности деятельности адвоката тесно связано с понятием адвокатской тайны, но является более широким. Если адвокатская тайна – это состояние запрета доступа к информации, составляющей ее предмет, то информационная безопасность деятельности адвоката – состояние защищенности той же информации, которое включает в себя наравне с вышеуказанным запретом доступа (конфиденциальностью) еще и требования обеспечения ее целостности и доступности. Как следствие, обеспечение информационной безопасности деятельности адвоката гарантированно реализует и сохранение профессиональной тайны адвоката.

Во-вторых, адвокат не просто обязан хранить адвокатскую тайну. Адвокат в силу Закона об адвокатуре и Кодекса профессиональной этики обязан обеспечить безопасность информации, составляющей ее предмет, то есть обеспечить ее конфиденциальность, целостность и доступность. Таким образом, адвокат обязан обеспечить информационную безопасность своей профессиональной деятельности.

В-третьих, реализация в действительности и адвокатской тайны, и информационной безопасности деятельности адвоката возможна только при помощи сочетания правового регулирования и организационно-технических мер, принимаемых как Федеральной палатой адвокатов Российской Федерации и адвокатскими палатами субъектов Российской Федерации (как минимум на уровне создания единых рекомендаций), так и каждым адвокатским образованием и адвокатом в отдельности.

2.3 Информационная безопасность налоговых органов

Налоговые органы России — это система государственных органов, на которых базируется бюджет России, и поэтому организация защиты информации в них стоит наиболее актуально.

При организации любой сети (информационных ресурсов) необходимо закладывать прочный фундамент информационной безопасности, исходя из возможных реальных угроз, от которых придется защищаться. Лучшую систему защиты предлагается построить, используя при организации информационных ресурсов выделенные каналы связи, однако это достаточно дорогой проект для системы налоговых органов России особенно при использовании выделенных междугородных каналов.

Для обеспечения необходимой информационной безопасности и надежности информационных ресурсов налоговые органы строят свою сеть с использованием многоуровневой системы защиты. Особенностью информационных ресурсов налоговых органов является формирование, хранение и передача информации, составляющей служебную и персональную тайну.

Настоящая Концепция⁵⁰ информационной безопасности Федеральной налоговой службы определяет систему взглядов на проблему обеспечения безопасности информации, обрабатываемой в ФНС России, ее территориальных органах и подведомственных организациях, а также при осуществлении информационного взаимодействия налоговых органов между собой, с федеральными органами государственной власти, при оказании государственных услуг юридическим и физическим лицам.

Концепция устанавливает требования и практические правила управления обеспечением ИБ, базовый уровень и режим защиты информации, обязательный к исполнению налоговыми органами, а также взаимодействующими организациями и налогоплательщиками,

⁵⁰ Приказ ФНС России от 13.01.2012 N ММВ-7-4/6@ «Об утверждении Концепции информационной безопасности Федеральной налоговой службы» // URL: http://www.consultant.ru/document/cons_doc_LAW_256498/ (дата обращения: 25.11.2018 г.)

пользующимися информационными ресурсами ФНС России.

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

При реализации функций государственного управления и оказания государственных услуг ФНС России обрабатывается информация, содержащая сведения, составляющие:

- государственную тайну;
- налоговую тайну;
- персональные данные;
- коммерческую и банковскую тайны;
- служебную тайну ФНС России и других органов государственной власти;
- сведения, на основании которых принимаются управленческие решения в системе финансово-кредитной и банковской деятельности, отнесенные к сведениям ключевой системы информационной инфраструктуры;
- открытые сведения, подмена, искажение или уничтожение которых может нанести ущерб интересам отдельных граждан, организаций, обществу и государству в целом.

Главная цель системы информационной безопасности заключается в обеспечении устойчивого функционирования объекта: предотвращении угроз его безопасности, защите законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, предусмотренных Уголовным кодексом РФ.

В рамках обеспечения комплексной информационной безопасности налоговых информационных систем и налоговых информационных ресурсов, прежде всего, следует выделить ключевые проблемы, которые

включают: защиту информации при ее передаче по каналам связи; защиту компьютерных систем, баз данных и электронного документооборота; обеспечение долгосрочного хранения информации в электронном виде; секретность конфиденциальной информации, аутентификацию, защиту персональных данных и др.

Налоговая информационная система в своей работе требует построения политики безопасности информации, которая строится на определенных математических моделях, определяющих права доступа того или иного пользователя к информационным ресурсам.

Объектом защиты являются информационные ресурсы налоговых органов (библиотеки, архивы и фонды; банки, базы и файлы данных; отдельные документы на традиционных носителях), содержащие зафиксированные на материальном носителе (независимо от его формы) сведения, используемые в процессе сбора, обработки, накопления, хранения, распространения, взаимодействия в рамках исполнения возложенных на ФНС России функций и оказания государственных услуг.

Важной задачей автоматизации работы налоговых органов является не только возложение на средства вычислительной техники задач контроля, обработки и хранения информации по начислению и уплате различных налогов, ведению нормативно-правовой базы по налоговому законодательству, формирование отчетности по налоговым органам, но и создание автоматизированного интерфейса с банками, таможенными органами и другими внешними структурами, а также полное правовое обеспечение вышеупомянутых информационных систем и их правовая защита.

Для нормального функционирования корпоративной сети и ее информационных ресурсов необходимо принять ряд мер по обеспечению ее надежной защиты, поэтому в налоговых органах РФ реализованы следующие положения:

- создана многоуровневая система прав пользователей по работе с

корпоративной информацией, посредством системы паролей и идентификаций пользователей;

- обеспечены мероприятия по регулярному резервированию информации корпоративных файл-серверов посредством каждодневного копирования информации на магнитные носители;

- создана эффективная антивирусная сеть информационного ресурса, с использованием новейших разработок антивирусных программ;

- организована при помощи системы паролей на каждом конкретном компьютере и в каждой конкретной локальной сети защита от хищения информации с использованием удаленного доступа;

- обеспечена безопасность серверных помещений и резервных копий информации файл-серверов, посредством непроникновения в эти помещения третьих лиц;

- организован контроль за интернет-трафиком;

- организован контроль за почтовым трафиком налоговых органов;

- внедрена система контроля за местонахождением сотрудников и посетителей в помещениях, где есть доступ к информационным ресурсам, с использованием сложной системы доступа в эти помещения, например по магнитной карте.

2.4 Информационная безопасность судебного производства

Обеспечение защиты информации в сфере судопроизводства организуется на каждой стадии процесса с учетом специфики конституционного, административного, гражданского, арбитражного и уголовного процесса. Методы и средства защиты информации выбираются в рамках проектов развития информационных технологий органов судебной и исполнительной власти с учетом особенностей процессуальных действий участников судебного процесса и совместных правил оформления процессуальных электронных документов.

Особенности организационно-правового обеспечения информационной безопасности в сфере судопроизводства обусловлены

следующими требованиями.

– Требования по использованию систем видеоконференц-связи в судебных заседаниях с защитой информации ограниченного доступа (регламентируется участие в судебном заседании обвиняемого, подсудимого, находящегося под стражей или осужденного, отбывающего наказание в виде лишения свободы; устанавливается порядок проведения судебного заседания с привлечением лиц, участвующих в деле, их представителей, а также свидетелей, экспертов, специалистов, переводчиков; определяется порядок допроса свидетелей, экспертов, получение объяснений сторон и третьих лиц, консультаций специалистов; организуется передача письменных доказательств по каналу видеоконференц-связи с использованием электронной подписи).

– Требования к содержанию информации и аппаратно-программным средствам официальных сайтов участников судопроизводства в сети Интернет (информирование с помощью официального сайта участников судебного процесса путем размещения на нем соответствующих судебных документов и информации в электронном виде по установленному регламенту; обеспечение круглосуточного доступа участникам процесса судебной информации; обеспечение доступности информации для граждан и организаций с различным процессуальным статусом).

– Требования к информации о деятельности суда в занимаемых им зданиях (помещениях) на информационных табло и в информационно-справочных киосках.

– Требования к судебным системам электронного документооборота, обеспечивающим межведомственное взаимодействие в сфере судопроизводства с использованием систем межведомственного электронного взаимодействия (СМЭВ) Минкомсвязи России и межведомственного электронного документооборота (МЭДО) ФСО России с комплексами средств защиты информации в полном объеме их функциональных возможностей (обеспечение целостности обрабатываемых

данных в контуре информационного взаимодействия; обеспечение антивирусной защиты информации во всех звеньях контура информационного взаимодействия; применение электронной подписи по единым правилам межведомственного взаимодействия и др.).

– Требования к защите АС судопроизводства в условиях формирования единого информационного пространства⁵¹ и комплексной системы информационной безопасности, предусматривающей:

- защиту от НСД с обеспечением идентификации и аутентификации субъектов доступа и объектов доступа;
- обнаружение вторжений, соблюдение конфиденциальности информации ограниченного доступа; обеспечение целостности, устойчивости функционирования и безопасности АС с незамедлительным восстановлением информации в случае нарушения безопасности;
- обеспечение использования электронной подписи;
- контроль привилегированных пользователей;
- защиту файловых серверов;
- защиту баз данных;
- защиту активно развиваемых мобильных и «облачных» технологий;
- контроль несанкционированной передачи данных;
- защиту внешнего информационного обмена;
- внутреннее межсетевое экранирование сегментов локальных вычислительных сетей;
- резервное (аварийное) хранение и восстановление данных;
- антивирусную защиту;
- контроль состояния, обработки и анализа событий

⁵¹ Ловцов Д. А., Ниесов В. А. Развитие судебной системы России и создание единого информационного пространства — двуединая задача // Российское правосудие. Специальный выпуск к VIII Всероссийскому съезду судей. М., 2012. С. 77—89

информационной безопасности АС судопроизводства в условиях формирования единого информационного пространства;

– обеспечение защиты машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные.

Что же касается информационной безопасности судьи как участника информационного процесса, то необходимо подчеркнуть, что безопасность является важнейшей государственной гарантией независимости судей, установленной Законом Российской Федерации от 26 июня 1992 г. № 3132-І «О статусе судей в Российской Федерации» (ст. 9) в соответствии с Конституцией Российской Федерации (ст. 120) и Федеральным конституционным законом от 31 декабря 1996 г. № 1-ФКЗ «О судебной системе Российской Федерации» (ст. 5). Соответственно, обеспечение информационной безопасности судьи как составляющей его безопасности следует отнести к одному из приоритетных направлений в данной области.

Из всех возможных информационных воздействий на судью как на должностное лицо (в отличие от воздействия непосредственно на сам процесс судопроизводства) следует выделить оказание информационного давления любым доступным способом. Наиболее распространенным в текущих реалиях является воздействие на судью, а также на общественное мнение касательного судопроизводства и конкретных процессов в целом при помощи СМИ.

Так как в числе важнейших форм работы по повышению уровня правосознания граждан, формирования доверия к правосудию можно назвать информационную открытость и взаимодействие со средствами массовой информации, сегодня все суды имеют свои официальные сайты, на которых публикуются вступившие в законную силу судебные решения. Регулярно проводятся пресс-конференции, где журналисты могут задать вопросы по интересующим общество правовым вопросам, наиболее резонансным делам, высказать конструктивные критические замечания и получить на них ответы. Пресс-служба суда размещает пресс-релизы, обзоры судебной практики,

разъясняет новеллы законодательства, взаимодействует со СМИ. Понимая взаимную ответственность судов и СМИ за стабильность общественных процессов, формирование уважения к праву, признание правового государства как единственного возможного пути демократического развития, журналисты работают в соответствии с Конституцией РФ, Федеральным законом «О средствах массовой информации» (в ред. от 5 апреля 2016 г.)⁵², соблюдая нормы журналистской этики.

Однако современная действительность обозначила новую проблему в системе взаимодействия со СМИ. Она затрагивает различные стороны правового регулирования обеспечения независимости судей, особенно их информационной защиты и связана с участвовавшими явлениями попыток вмешательства в судебную деятельность в корыстных интересах, умышленной дискредитации судей и судебной системы РФ. Такие материалы противоречат правовым и конституционным нормам и никакого отношения к профессиональной журналистике не имеют. Более того, анализируя происходящие сегодня информационные атаки на государственных и политических деятелей России, общественные движения, государственные институты, можно предположить, что клеветнические публикации в адрес судей и судов также носят заказной характер и направлены на подрыв авторитета государственной власти.

Подобные информационные атаки на суды стали носить не единичный, а системный характер, что вызывает тревогу на высшем государственном уровне. Это подтвердило выступление Президента страны В.В. Путина на Всероссийском совещании судей РФ 16 февраля 2016 г. Он отметил, что «проигравшие в судебном процессе нередко продолжают состязаться и после вступления решения суда в законную силу, организуют давление на суд по всем каналам, включая заказанные информационные кампании, не жалеют эпитетов и черных красок не только в отношении конкретного судьи или суда, но и всей судебной системы». Президент также

⁵² Ведомости СНД и ВС РФ. 1992. № 7, ст. 300; Собр. законодательства Рос. Федерации. 2016. № 15, ст. 2056.

подчеркнул, что «подрывать авторитет суда, судебной власти, а часто это делается в корыстных интересах, недопустимо»⁵³.

Сегодня этот вопрос приобретает особую актуальность, т.к. затрагивает понятие информационной безопасности, которая входит в систему национальной безопасности Российской Федерации и захватывает различные сферы жизнедеятельности общества и государства, в т.ч. и такую важнейшую сферу, как правосудие.

В соответствии с положениями разд. IV «Стратегии национальной безопасности Российской Федерации»⁵⁴ одним из основных показателей, необходимых для оценки состояния национальной безопасности, являются удовлетворенность граждан степенью защищенности своих конституционных прав и свобод, личных и имущественных интересов, в т.ч. от преступных посягательств. Содержание ст. 18 Конституции РФ прямо указывает, что права и свободы человека и гражданина являются непосредственно действующими и обеспечиваются правосудием. Для того чтобы судебная власть могла эффективно защищать законные права и интересы любых субъектов, ряд статей гл. 2 Основного Закона посвящены основополагающим принципам осуществления правосудия, а в гл. 7 закреплены основы гарантий независимости судей и их обязанность подчиняться только Конституции РФ и федеральному закону. Эти конституционные нормы значимы не только для судебной власти, но и для человека и гражданина, общества, государства. Они призваны не допустить дестабилизации общественных отношений, обеспечить разрешение конфликтов только правовым путем, содействовать обеспечению национальной безопасности России.

Следует вновь отметить, что понятие «информационная безопасность» давно вышло за рамки привычного обеспечения безопасности самой

⁵³ URL: <http://www.kremlin.ru/events/president/news/51343> (дата обращения: 07.10.2019 г.).

⁵⁴ Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации»
// URL: http://www.consultant.ru/document/cons_doc_LAW_191669/
(дата обращения: 07.10.2019 г.)

информации. В результате эволюции к основным целям информационной безопасности общества были отнесено обеспечение человека и общества достоверной и полной информацией. А к объектам, которым следует обеспечить информационную безопасность, были отнесены различные информационные ресурсы, в т.ч. средства массовой 30 информации. Следовательно, информационные войны в отношении судебной власти ведутся объектами вопреки утвержденной Стратегии безопасности государства. Нарушается понятие целостности информации, т.е. достоверности и полноты освещения судебной деятельности. Учитывая преднамеренность распространения ложной, искаженной информации на большую аудиторию, такие действия можно расценивать как внутреннюю угрозу, направленную на подрыв общественно-политической стабильности в государстве.

Несмотря на существующие правовые гарантии независимости, в отношении судов и судей стали применяться классические методы ведения информационной войны: искажение информации от откровенной лжи до дезинформации, подтасовка фактов, частичное освещение, подача информации в определенном виде и т.д. Показательно, что давление ведется в связи с конкретными делами, затрагивающими коммерческие интересы. Вопреки положениям Конституции РФ без следствия и судебного решения, в отдельных программах граждане и судьи предполагались виновными, заслуживающими высшей меры наказания. Презумпция невиновности при этом становится презумпцией виновности. От судей требуют пояснений, приглашают для участия в программах по делам, которые еще не были предметом рассмотрения в суде, заведомо зная, что судья не имеет право давать такие комментарии. Освещается это как отказ в сотрудничестве, с дальнейшими угрозами подготовки новых фильмов и материалов. Под информационным давлением и шантажом судьям указывают на необходимость принятия определенного решения. Расценивать подобное можно только как давление на суд.

Положения ст. 51 Федерального закона «О средствах массовой информации» запрещают использовать права журналиста в целях распространения слухов под видом достоверных обращений, фальсификации общественно значимых сведений. Однако они не являются сегодня препятствием для журналистов, готовящих заказные материалы с целью дискредитации любого человека, в т.ч. и представителей судебной власти.

На сегодняшний день в соответствии с ч. 5 ст. 57 Федерального закона «О средствах массовой информации» редакция, главный редактор телеканала не несет ответственности за распространение сведений, не соответствующих действительности и порочащих честь и достоинство граждан, если они содержатся в авторских произведениях, идущих в эфир без предварительной записи. Такие авторы могут не являться штатными сотрудниками, поэтому их тексты не подлежат редактированию. Сетка телеэфира предоставляется им на условиях договора. Телевизионный канал выпускает их программы без проверки на достоверность. Некоторые авторы таким положением безнаказанно пользуются, злоупотребляя свободой массовой информации и правами журналистов. При этом размещение недостоверных, клеветнических материалов отражается на репутации канала и его штатных журналистах, которые являются высокопрофессиональной командой, для которой этические, моральные и законодательные нормы журналистики служат непреложной основой.

Понимая повышенную опасность дезинформации в СМИ, направленной против правосудия, предполагается, что в случае, установленном судом или контролирующим органом, неоднократного злоупотребления свободой массовой информации и умышленном размещении недостоверной информации в отношении судей и судебной системы, необходимо предусмотреть дисквалификацию автора. Она должна устанавливаться на определенный срок, без права размещения им своих материалов. Также следует рассматривать вопрос о приостановлении деятельности средства массовой информации, размещающего подобную

информацию. Только тогда, соответствующие авторы перестанут представлять интерес для заказчиков.

Не случайно информационной безопасности уделяется со стороны государства повышенное внимание. Доктрина информационной безопасности Российской Федерации 2016 года обозначает в качестве целей в области государственной и общественной безопасности укрепление государственного суверенитета, поддержание политической и социальной стабильности в обществе, реализацию основных прав и свобод человека и гражданина, а также защиту критической информационной инфраструктуры Российской Федерации. Поэтому ведение информационной войны в отношении судов и судей можно расценивать как определенный вызов обществу и государству.

Если общество понимает, что решения должны приниматься в соответствии с законом, оно должно постепенно прийти и к осознанию нетерпимости к попыткам информационного давления на судью с целью получения удобного кому-то решения

Можно сделать вывод, что присутствует необходимость постановки вопроса об информационной угрозе и информационной защите судей в современной России как одного из важнейших условий осуществления справедливого правосудия. При этом информационная защита должна, прежде всего, быть направлена на предотвращение противоправных попыток воздействовать на судей и суды, установление правового механизма обязательности исполнения установленных норм в этой сфере.

2.5 Информационная безопасность высших учебных заведений

Российская высшая школа переживает период адаптации не только к объективным процессам информационного общества, но и к новым социально-политическим условиям с разноплановыми проявлениями конкурентной борьбы.

Создание эффективных механизмов управления информационными ресурсами системы высшего образования в современных условиях невозможно без научного обоснования и практической реализации сбалансированной политики информационной безопасности вуза, которая может быть сформирована на основе решения следующих задач:

- анализ процессов информационного взаимодействия во всех сферах основной деятельности российского технического вуза: информационных потоков, их масштаба и качества, противоречий, конкурентной борьбы с выявлением собственников и соперников;
- разработка качественного и простого количественного (математического) описания информационного взаимодействия;
- введение количественных индикаторов и критериев открытости, безопасности и справедливости информационного обмена;
- разработка сценариев необходимости и значимости баланса в информационной открытости и конфиденциальности;
- определение роли и места политики информационной безопасности в управлении информационными ресурсами вуза и выработка согласующихся принципов и подходов;
- формулировка основных составляющих политики: целей, задач, принципов и ключевых направлений обеспечения информационной безопасности;
- разработка базовых методик управления процессом обеспечения политики информационной безопасности;
- В современном вузе хранится и обрабатывается огромное количество различных данных, связанных не только с обеспечением

учебного процесса, но и с научно-исследовательскими и проектно-конструкторскими разработками, персональные данные студентов и сотрудников, служебная, коммерческая и иная конфиденциальная информация.

Рост количества преступлений в сфере высоких технологий диктует свои требования к защите ресурсов вычислительных сетей учебных заведений и ставит задачу построения собственной интегрированной системы безопасности. Ее решение предполагает наличие нормативно-правовой базы, формирование концепции безопасности, разработку мероприятий, планов и процедур по безопасной работе, проектирование, реализацию и сопровождение технических средств защиты информации (СЗИ) в рамках образовательного учреждения. Эти составляющие определяют единую политику обеспечения безопасности информации в вузе.

Особенности вуза как объекта информатизации связаны также с многопрофильным характером деятельности, обилием форм и методов учебной работы, пространственной распределенностью инфраструктуры (филиалы, представительства). Сюда же можно отнести и многообразие источников финансирования, наличие развитой структуры вспомогательных подразделений и служб (строительная, производственная, хозяйственная деятельность), необходимость адаптации к меняющемуся рынку образовательных услуг, потребность в анализе рынка труда, отсутствие общепринятой формализации деловых процессов, необходимость электронного взаимодействия с вышестоящими организациями, частое изменение статуса сотрудников и обучаемых.

Несколько облегчает проблему то, что вуз представляет собой стабильную, иерархическую по функциям управления систему, обладающую всеми необходимыми условиями жизнедеятельности и действующую на принципах централизованного управления (последнее означает, что в управлении задачами информатизации может активно

использоваться административный ресурс).

Указанные выше особенности обуславливают необходимость соблюдения следующих требований. Необходимо:

- комплексно проработать задачи информационной безопасности, начиная с концепции и заканчивая сопровождением программно-технических решений;
- привлекать большое число специалистов, владеющих содержательной частью деловых процессов;
- использовать модульную структуру корпоративных приложений, когда каждый модуль покрывает взаимосвязанную группу деловых процедур или информационных сервисов при обеспечении единых требований к безопасности;
- применять обоснованную последовательность этапов в решении задач информационной безопасности;
- документировать разработки на базе разумного применения стандартов, что гарантирует создание успешной системы;
- использовать надежные и масштабируемые аппаратно-программные платформы и технологии различного назначения, обеспечивающих необходимый уровень безопасности.

В составе массивов охраняемой законом информации, находящейся в распоряжении высшего образовательного учреждения, можно выделить три группы:

- персональные сведения, касающиеся учащихся и преподавателей, оцифрованные архивы;
- ноу-хау образовательного процесса, носящие характер интеллектуальной собственности и защищенные законом;
- структурированная учебная информация, обеспечивающая образовательный процесс (библиотеки, базы данных, обучающие программы).

Все эти сведения не только могут стать объектом хищения.

Намеренное проникновение в них может нарушить сохранность оцифрованных книг, уничтожить хранилища знаний, внести изменения в код программ, используемых для обучения.

Обязанностями лиц, ответственных за защиту информации, должно стать сохранение данных в целостности и неприкосновенности и обеспечение их:

- доступности в любое время для любого авторизованного пользователя;
- защиты от любой утраты или внесения несанкционированных изменений;
- конфиденциальности, недоступности для третьих лиц.

Особенностью угроз становится не только возможность хищения сведений или повреждение массивов какими-либо сознательно действующими хакерскими группировками, но и сама деятельность студентов, намеренно, по злему умыслу или ошибочно способных повредить компьютерное оборудование или внести вирус.

Анализ нормативно-правового и технического обеспечения отдельных субъектов и объектов информационной безопасности позволил прийти к следующим выводам.

Выявление и анализ угроз информационной безопасности личности, выработка и принятие мер, необходимых для адекватного ответа на них, должны рассматриваться как важнейшие приоритеты национальной безопасности.

К правовым методам обеспечения информационной безопасности относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации. Правовые методы обеспечения информационной безопасности включают в себя множество направлений, призванных регулировать отношения в информационной сфере в целях создания и

совершенствования системы обеспечения информационной безопасности Российской Федерации.

Адвокатская тайна – это состояние запрета доступа к информации, составляющей ее содержание, посредством установления специального правового режима.

Адвокат в силу Закона об адвокатуре и Кодекса профессиональной этики обязан обеспечить безопасность информации, составляющей ее предмет, то есть обеспечить ее конфиденциальность, целостность и доступность.

Реализация адвокатской тайны и информационной безопасности деятельности адвоката возможна только при помощи сочетания правового регулирования и организационно-технических мер, принимаемых Федеральной палатой адвокатов Российской Федерации и адвокатскими палатами субъектов Российской Федерации, так и каждым адвокатским образованием и адвокатом в отдельности.

Особенностью информационных ресурсов налоговых органов является формирование, хранение и передача информации, составляющей служебную и персональную тайну. Для обеспечения необходимой информационной безопасности и надежности информационных ресурсов налоговые органы строят свою сеть с использованием многоуровневой системы защиты.

Обеспечение защиты информации в сфере судопроизводства организуется на каждой стадии процесса с учетом специфики конституционного, административного, гражданского, арбитражного и уголовного процесса.

Безопасность является важнейшей государственной гарантией независимости судей, присутствует необходимость постановки вопроса об информационной угрозе и информационной защите судей в современной России как одного из важнейших условий осуществления справедливого правосудия.

Особенности Высшего учебного заведения как объекта информатизации связаны с многопрофильным характером деятельности, обилием форм и методов учебной работы, пространственной распределенностью инфраструктуры.

Создание эффективных механизмов управления информационными ресурсами системы высшего образования в современных условиях невозможно без научного обоснования и практической реализации сбалансированной политики информационной безопасности высшего учебного заведения.

3 Тенденции развития института информационной безопасности в Российской Федерации

3.1 Тенденции развития информационного права в России

Тенденции (лат. *tendentia* — направленность) — это важнейшие направления становления и развития информационно-правовых норм, а также доктрины информационного права, обусловленные общими закономерностями существования самой информационной сферы и информационных технологий как в России, так и в других странах. Разумеется, мы коснемся не всех, а лишь некоторых тенденций становления комплексной отрасли и научного направления «информационное право».

Тенденции формирования норм информационного права, отдельных его институтов рассматриваются в единстве прошлого, настоящего и будущего развития науки и отрасли российского информационного права.

Сегодня существуют все предпосылки, для того чтобы признать информационное право в качестве комплексной отрасли права и нового научного направления, формирующейся юридической науки.

Начальная стадия развития информационного законодательства на основе Конституции Российской Федерации 1993 г. относится ко времени принятия в феврале 1995 г. первого комплексного Федерального закона «Об информации, информатизации и защите информации». Еще раньше были приняты законы «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального собрания» (1994); «Об обязательном экземпляре документов» (1994). Уже на основе этих законов стала формироваться теория и практика института информационных ресурсов.⁵⁵ Наиболее активно велась работа по формированию ресурсов правовой информации и созданию общероссийской автоматизированной системы РЛСИПО, что подкреплялось рядом указов Президента Российской Федерации. Несколько лет первый закон об

⁵⁵ Парошин, А.А. Информационная безопасность: стандартизированные термины и понятия. - М.: Норма. - 2017. - С.511.

информации оставался основной опорой развития информационных технологий, их включения в ткань реальной жизни страны.

Данный этап развития информационного законодательства и участие в нем специалистов сектора информационного права ИГП РАН способствовал становлению информационного права как отрасли.

Первые законы в Российской Федерации в области информационного законодательства вполне соответствовали требованиям международного права в части обеспечения прав и свобод человека в информационно-коммуникационной сфере. Отметим, что и прецеденты Европейского Суда по правам человека и ряд других актов, и практика применения уже принятых российских законов стимулировали развитие правовой основы в реализации прав и свобод человека и гражданина. Однако кризис 1990-х гг. значительно ослабил внимание к сфере информационных отношений на основе информационно-коммуникационных технологий. И следующая активная законотворческая волна в России относится ко второму пятилетию нового XXI в., когда наиболее активно стала реализовываться Стратегия развития информационного общества в Российской Федерации.⁵⁶

Основными актами периода 2000—2019 гг. являются Федеральные законы от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; от 27 июля 2006 г. № 152-ФЗ «О персональных данных»; от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»; от 28 декабря 2010 г. № 390-ФЗ «О безопасности»; от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».⁵⁷

В правовой лексикон прочно вошла аббревиатура «ИКТ», раскрываемая как «информационно-коммуникационные технологии» и используемая как технологическая основа социальных процессов сбора, обработки и использования информационных ресурсов. Предмет внимания

⁵⁶ Галицкий, Е.А., Сидорова, А.А. Интернет в России: Методика и основные результаты исследования // Юридические науки: проблемы и перспективы. - 2016. - №1. - С.23.

⁵⁷ Рассолов, И.М. Право и интернет // Законодательство и экономика. -2010. - № 9. - С.7.

правового регулирования сосредоточился на таком феномене, как информационные технологии – совокупность всех технологических средств и приемов работы с информацией, используемой во всех направлениях жизни общества.²¹ Появились и феномены «электронное государство» и «электронное правительство» (управление) – комплексные носители и измерители включенности информационных технологий в структуру всех институтов общества и государственных институтов.⁵⁸

На примере общих результатов по применению законодательства можно судить о зависимости социальных процессов от состояния системы правового регулирования отношений в области информационной безопасности.

Непрерывно ведется работа по совершенствованию законодательства Российской Федерации и переводу операций законотворческого процесса на электронную форму. Самостоятельным участком работы в этом направлении является и обеспечение доступа к правовой информации в электронной форме, что повышает уровень ее достоверности и воспитания правосознания более широкого круга субъектов. Согласно части 3 статьи 15 Конституции Российской Федерации Законы подлежат официальному опубликованию. Неопубликованные законы не применяются. Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения. В этом аспекте важно обеспечить официальное опубликование в электронном виде.

Так, в рейтинге ООН по развитию электронного правительства позиции России серьезно укрепились. Это свидетельствует о значимости правового регулирования в решении задач общего социально-экономического развития страны как базы для преодоления информационного неравенства и более уверенных шагов к формированию и развитию информационного общества.⁵⁹

⁵⁸ Наумов, В.Б. Право и Интернет: Очерки теории и практики. - М.:Книжный дом «Университет». - 2017. -

⁵⁹ Куняев, Н.Н. Национальные интересы Российской Федерации в информационной сфере на современном этапе развития Российского государства // Российская юстиция. - 2010. - № 1. - С.6.

Несмотря на недостатки в организации правотворчества, имеющийся массив законов и опыт правоприменения позволил за последние 20 лет оформить блоки нормативно-правового материала по основным институтам информационного права. Это институт права на информацию и формы его реализации преимущественно через открытый доступ и использование открытых данных для повышения уровня участия граждан в управлении и законотворчестве; институт правового режима информационных ресурсов, технологий и систем, массовых коммуникаций, Интернета; правового обеспечения информационной безопасности, институт тайн и т.д. На примере Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» можно проследить, насколько внимание к потребностям граждан, реализуемым на основе использования информационно-коммуникационных технологий, повлияло на изменение, а главное, на понимание важности и сложности создания реальных условий для взаимодействия органов власти с конкретным человеком, а также на общую направленность развития деятельности государственных администраций.

3.2 Развитие законодательства в области информационной безопасности как элемент системы национальной безопасности

Сфера развития законодательства в области обеспечения информационной безопасности, выявление складывающихся тенденций и основных проблем стало предметом исследования многих российских ученых^{60 61}.

Первый закон по защите информации был принят в 1995 г.⁶², Доктрина информационной безопасности — в 2000⁶³ г., а в 2006 г. вступил в силу Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»⁶⁴, который действует и сегодня.

За прошедшие годы произошли большие изменения в информационной сфере, в применении информационных технологий, в развитии электронного правительства, что усилило значимость информационной безопасности. Все изменения отражались в нормативно-правовых актах по защите информации, в частности, в Законе № 149-ФЗ. На конец 2019 г. принято 37 его редакций.

Вообще первые изменения были внесены в 2010 г., — через четыре года после его принятия. Введено понятие электронного документа, в связи с чем изменена ст. 11 «Документирование информации». Усилена роль электронного документа, подписанного электронной цифровой подписью. Ее законодательное закрепление как основного и практически единственного IT-решения по обеспечению подлинности позволяет сделать электронные документы равно значимыми документам на бумажном носителе, если иное не предусмотрено федеральным законодательством.

⁶⁰ Асланов Р.М. Зарубежный опыт правового регулирования обеспечения информационной безопасности // Политика и общество. 2012. № 2 (86).

⁶¹ Терещенко Л.К. Модернизация информационных отношений и информационного законодательства. М., 2013.

⁶² Об информации, информатизации и защите информации: Федер. закон от 20 февр. 1995 г. № 24-ФЗ // СЗ РФ. 1995. № 8. Ст. 609.

⁶³ Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сент. 2000 г. № Пр-1895) // URL: <http://base.garant.ru/182535/> (дата обращения: 05.03.2019 г.)

⁶⁴ Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ в ред. от 02.12.2019 // Российская газета, № 165, 29.07.2006.

Государственным органам и органам местного самоуправления теперь вменяется в обязанность обеспечение доступа к информации о своей деятельности и с использованием информационно-телекоммуникационных сетей, в частности Интернета (ст. 8). Изменена ст. 14 «Государственные информационные системы». Содержащаяся в сетях информация признается официальной, а соответствующие государственные органы должны обеспечить ее достоверность и актуальность, а также доступ к ней и ее защиту. Указанные поправки направлены на дальнейшее развитие Доктрины информационной безопасности Российской Федерации, закрепляющей приоритеты по правовому обеспечению информационной безопасности Российской Федерации на принципах законности, баланса интересов граждан, общества и государства в информационной сфере и обеспечении гарантий конституционных прав и свобод человека и гражданина на доступ к информации и предоставление полноценных возможностей для деятельности в информационной сфере.

Дальнейшие изменения были внесены Федеральным законом от 21 июля 2011 г. № 252-ФЗ⁶⁵. В ст. 12 о государственном регулировании применения информационных технологий был добавлен п. 4 об обеспечении информационной безопасности детей, что, несомненно, является актуальным компонентом в системе национальной безопасности, отвечающим за информационно-психологическую безопасность и создающим правовую основу для развития и реализации мер, направленных на поддержание и укрепление здоровья нации и защиту индивидуальной психики и общественного сознания.

Следующим шагом по усилению информационной безопасности стало

⁶⁵ Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» от 21.07.2011 N 252-ФЗ

введение Федеральным законом от 28 июля 2012 г. № 139-ФЗ⁶⁶ ст. 15.1. «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты, содержащие информацию, распространение которой в Российской Федерации запрещено». В ней говорится о создании автоматизированной информационной системы с включением в нее доменных имен и сетевых адресов соответствующих сайтов, определены органы, осуществляющие создание, формирование и ведение такого реестра — это федеральные органы исполнительной власти, контролирующие средства массовой информации, массовых коммуникаций, информационных технологий и связи. Прописаны основания для включения в реестр. Это порнографические материалы, связанные с несовершеннолетними, информация, касающаяся наркотических и психотропных средств (способы и методы изготовления, использования и распространения), а также призывы к самоубийству и способы его совершения⁶⁷.

Федеральным законом от 7 июня 2013 г. № 112-ФЗ⁶⁸ введено понятие информации в форме открытых данных — это общедоступная в Интернете информация, допускающая автоматизированную обработку для ее повторного использования, регламентировано ее размещение. В связи с этим изменены ст. 13 «Информационные системы» и ст. 14 «Государственные информационные системы». Оператор информационных систем должен обеспечить возможность размещения информации в форме открытых

⁶⁶ Федеральный закон от 28 июля 2012 г. N 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» // Российская газета от 30 июля 2012 г. № 172.

⁶⁷ С изменением в обществе и развитием информационных технологий эта статья менялась, в частности, добавлялись следующие основания для включения в реестр: информация о пострадавшем от противоправных действий несовершеннолетнем, распространение которой запрещено федеральным законодательством; информация, нарушающая требования федерального законодательства по государственному регулированию организации и проведения азартных игр, о запрете проведения азартных игр с использованием Интернета; информация о способах, методах разработки, изготовления и использования различных наркотических средств; информация о розничной продаже дистанционным способом алкогольной, различной спиртосодержащей продукции, розничная продажа которой ограничена или запрещена законодательством.

⁶⁸ Федеральный закон от 7 июня 2013 г. N 112-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Российская газета от 11 июня 2013 г. № 124.

данных. Доступ к информации из государственных информационных систем дается только тем, кто прошел авторизацию в единой системе идентификации и аутентификации, тем самым повышается ответственность пользователей.

В декабре 2013 г. были внесены изменения в статью о государственных информационных системах (ст. 14). Согласно этим изменениям государственные информационные системы создаются и эксплуатируются в соответствии с законодательством о контрактной системе в сфере закупок. Введена ст. 15.3 «Порядок ограничений доступа к информации, распространяемой с нарушением закона» напрямую связанная с обеспечением национальной безопасности. Имеется ввиду информация, размещаемая в информационно-коммуникационных сетях, о призывах к массовым беспорядкам, экстремистской деятельности, участию в массовых мероприятиях, проводимых с нарушением закона.

С развитием информационно-коммуникационных технологий и Интернета появилась необходимость регламентирования информации, размещенной в сети и в информационных системах. В связи с этим в Закон № 149-ФЗ были внесены изменения Федеральным законом от 5 мая 2014 г. № 97-ФЗ⁶⁹, в частности, добавлена ст. 10.1 «Об обязанностях организатора распространения информации в сети Интернет». Дано определение организатора информации как лица, обеспечивающего работу информационных систем и программ, предназначенных для приема, передачи, обработки электронных сообщений пользователей в Интернете. О начале своей деятельности он должен уведомить соответствующий орган. Информацию о фактах таких действий и информацию о пользователях он обязан хранить в течение шести месяцев с момента окончания их и предоставлять соответствующим органам в целях безопасности Российской Федерации или для

⁶⁹ Федеральный закон от 5 мая 2014 г. N 97-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей» // Российская газета от 7 мая 2014 г. № 101.

оперативно-розыскной деятельности, исполнять требования к оборудованию и программам. Прописано, на кого положения данной статьи не распространяются.

В июле 2016 г. Федеральным законом от 6 июля 2016 г. в Закон № 374-ФЗ⁷⁰ были внесены изменения в ст. 10.1 об обязанностях организатора распространения информации. В ч. 3 ст. 10.1 введен п. 2, вступающий в силу с 1 июля 2018 г., обязывающий хранить электронные сообщения пользователей Интернета до шести месяцев после окончания их приема, передачи, доставки, обработки. При дополнительном кодировании сообщений организатор распространения информации обязан представлять в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений.

В связи с введением ст. 10.1 в июле 2014 г. появилась ст. 15.4, регламентирующая порядок ограничения доступа к информационному ресурсу организатора распространения информации в Интернете.

Федеральный закон от 24 ноября 2014 г. № 364-ФЗ⁷¹ изменил ст. 10, обязав владельцев сайтов размещать на них информацию о своем местонахождении, адресе, наименованиях, адресе электронной почты для направления ему заявления о нарушении авторских и (или) смежных прав. Этот же закон ввел ст. 15.6 о порядке ограничения доступа к сайтам, где неоднократно размещалась информация, нарушающая авторские и (или) смежные права, ст. 15.7 — о внесудебных мерах по прекращению нарушения авторских прав в информационно-коммуникационных сетях, в которой прописаны меры и сроки, в которых их можно предпринимать.

⁷⁰ Федеральный закон от 6 июля 2016 г. N 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // Российская газета от 8 июля 2016 г. № 149.

⁷¹ Федеральный закон «О внесении изменений в статьи 9 и 16 Федерального закона «О войсках национальной гвардии Российской Федерации» и Кодекс Российской Федерации об административных правонарушениях» от 11.10.2018 N 364-ФЗ // URL: <http://www.garant.ru/hotlaw/federal/1223226/> (дата обращения: 10.04.2019 г.)

В декабре 2014 г. внесены изменения в статьи, касающиеся информационных систем. В частности, информационные системы, используемые государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями, государственными и муниципальными учреждениями должны размещаться на территории Российской Федерации. Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации, вывода из эксплуатации государственных информационных систем утверждает Правительство Российской Федерации.

Защиту персональных данных регулирует новая ст. 15.5, ограничивающая доступ к информации, которая обработана с нарушением законодательства о персональных данных. Согласно этой статье должна быть создана информационная система «Реестр нарушителей прав субъектов персональных данных» и прописан порядок его ведения. В ч. 4 ст. 16 «Защита информации» введен пункт 7, обязывающий базы данных с персональными данными граждан Российской Федерации хранить на территории Российской Федерации.

В 2015 г. введены ст. 10.3 об обязанностях оператора поисковой системы, ст. 12.1, регламентирующая государственное регулирование в сфере использования российских программ для электронных вычислительных машин и баз данных. В последней прописано создание единого реестра российского программного обеспечения, необходимое для расширения использования российских программ и баз данных и для оказания их владельцам (правообладателям) господдержки. Прописаны требования, которым должно удовлетворять программное обеспечение для включения в реестр.

В 2017 г., данный Закон дополнен новыми статьями. Так, в ст. 10.4 дано определение новостного агрегатора (обработка и распространение новостной информации, доступ более миллиона пользователей Интернета в течение суток) и требования, которые они должны соблюдать. Нельзя до-

пускать использование новостного агрегатора в целях разглашения государственной или иной охраняемой законом тайны, распространения публичных призывов к осуществлению террористической деятельности, экстремистских материалов, а также материалов, пропагандирующих порнографию, насилие и жестокость.

Статья 10.5 теперь содержит определение владельца аудиовизуального сервиса (распространения в Интернете совокупности аудиовизуальных произведений, находящихся на территории Российской Федерации, доступ более миллиона пользователей Интернета в течение суток) и требования, которые необходимо соблюдать. Нельзя допускать использование аудиовизуального сервиса для разглашения государственной или иной тайны, охраняемой законом, для призывов к террористической деятельности, распространения экстремистских материалов, материалов, пропагандирующих порнографию, насилие и жестокость, осуществлять классификацию аудиовизуальных произведений, чтобы не причинить вред детям.

С октября 2017 г. начала действовать ст. 15.6-1 о порядке ограничения доступа к копиям заблокированных сайтов, а с 1 ноября — ст. 15.8, регламентирующая меры для противодействия использованию информационных ресурсов и сетей, через которые осуществляется доступ к ресурсам и сетям, ограничен на территории РФ.

Федеральным законом от 23.04.2018 N 102-ФЗ⁷² Часть 5 статьи 15.1 ФЗ № 149 была дополнена пунктом три, который дополняет основание для включение сайтов сети Интернет в список содержащих информацию, запрещенную к распространению на территории РФ «постановлением судебного пристава-исполнителя об ограничении доступа к информации, распространяемой в сети «Интернет», порочащей честь, достоинство или деловую репутацию гражданина либо деловую репутацию юридического

⁷² Федеральный закон от 23 апреля 2018 г. N 102-ФЗ «О внесении изменений в Федеральный закон «Об исполнительном производстве» и статью 15.1 Федерального закона «Об информации, информационных технологиях и о защите информации» // Российская газета от 25 апреля 2018 г. N 88.

лица.».

Пунктом 4 Федеральный закон от 01.05.2019 N 90-ФЗ⁷³ в ФЗ № 149 была внесена статья 14.2, предполагающая создание национальной системы доменных имен, которая представляет собой совокупность взаимосвязанных программных и технических средств, предназначенных для хранения и получения информации о сетевых адресах и доменных именах, в целях обеспечения устойчивого и безопасного использования на территории Российской Федерации доменных имен.

Таким образом, изменения в Законе № 149-ФЗ направлены на усиление информационной безопасности, а следовательно, развитие и совершенствование всей системы национальной безопасности страны по таким направлениям, как защита каналов связи, сетевая и эксплуатационная безопасность, компьютерная безопасность, административная безопасность. Нормативно-правовое усиление по этим направлениям способно комплексно решать ключевые задачи по сохранению и защите информационных ресурсов России, укреплению ее международного авторитета, повышению эффективности работы по снижению криминальной напряженности, защите прав, свобод и безопасности российских граждан в системе их информационно-коммуникационных взаимодействий. В результате компонент информационной безопасности в системе национальной безопасности приобретает особый вес и актуальность по сравнению с другими ее элементами.

⁷³ Федеральный закон от 1 мая 2019 г. N 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» // Российская газета от 7 мая 2019 г. № 97

3.3 Анализ направления реализации политики информационной безопасности на примере сравнения Доктрины информационной безопасности 2000 и 2016 годов.

Несмотря на предварительное выдвижение Советом Безопасности РФ на общественное обсуждение проекта Доктрины, принятая система официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере была и все еще подвергается критике со стороны экспертов.

Выигрышными (в области правовой защиты информации) в утратившей силу Доктрине ИБ смотрелись постулаты первой главы, касающиеся состояния ИБ РФ и основных задач по ее обеспечению.⁷⁴

Так, отмечался старт формирования базы правового обеспечения ИБ: принятие ряда фундаментальных законов (например, федеральные законы «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», Закон РФ «О государственной тайне») и динамичная работа по созданию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Кроме того, Доктрина⁷⁵ раскрывала и недостатки в этой сфере. Отмечалось, что уровень ИБ РФ не в полной мере соответствует потребностям общества и государства. Приводились следующие отрицательные моменты:

противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере;

недостаточность нормативного правового регулирования отношений в области реализации возможностей конституционных ограничений свободы массовой информации в интересах защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения

⁷⁴ Пакляченко М.Ю. Новая доктрина информационной безопасности: вопросы правовой защиты информации. *История и архивы*. 2017;(2):96-103.

⁷⁵ «Доктрина информационной безопасности Российской Федерации» (утв. Президентом РФ 09.09.2000 N Пр-1895) // URL: <http://base.garant.ru/182535/> (дата обращения: 12.09.2019 г.)

обороноспособности страны и безопасности;

несовершенство нормативного правового регулирования отношений в области массовой информации.

В документе приводилось описание задач, требующих безотлагательного решения. В части ПЗИ такой задачей явилось совершенствование нормативной правовой базы обеспечения ИБ РФ, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации.

Таким образом, раскрытие категории ПЗИ в рамках Доктрины от 09.09.2000 г. можно охарактеризовать как достаточное и полноценное: были отмечены положительные и отрицательные моменты состояния ИБ РФ, определены цели и задачи в данной сфере, дана характеристика правовым методам. Отдельно определялась приоритетность направления государственной политики в области обеспечения ИБ РФ путем совершенствования правовых механизмов регулирования общественных отношений.

Можно утверждать, что при комплексном восприятии всего содержания Доктрины от 09.09.2000 г. значение прерогативы правового аспекта если не доминирует, то уверенно находится в числе наиболее важных факторов обеспечения ИБ государства.

Перейдем к анализу Доктрины от 05.12.2016 г.

Первое изменение, бросающееся в глаза, затрагивает структуру документа — появляется дополнительная пятая глава. В содержание «Основных положений» включены дефиниция Доктрины, основные понятия, используемые в ней, правовая основа, сущность и значение этого документа для государственной политики и общественных отношений в области обеспечения ИБ.

Такое изложение, распространенное в структуре большинства законодательных актов, представляется предпочтительным с точки зрения

удобства восприятия предназначения документа в общем поле законодательства, а также усвоения его понятийно-категориального аппарата.

Положения, затрагивающие вопросы ПЗИ, фигурируют в п. 2 первой главы Доктрины, где к средствам обеспечения ИБ относят наряду с техническими и организационными правовые средства.

В отличие от систематизированного представления четырех основных составляющих национальных интересов РФ в информационной сфере и следующего за каждой такой составляющей перечня действий для их достижения, как это приводилось в Доктрине ИБ 2000 г., утвержденный Указом Президента от 05.12.2016 г. № 646 документ распределяет области национальных интересов в информационной сфере⁷⁶, а также стратегических целей и основных направлений обеспечения ИБ по одноименным главам.

Хочется отметить отсутствие описания в новой Доктрине источников угроз ИБ. В первых пунктах третьей главы документа в общих чертах обрисовывается текущее состояние информационной безопасности, главным образом с позиции международно-правовых отношений. Далее следует описание состояния ИБ и информационных угроз в различных областях и сферах государства (государственная и общественная безопасность, экономика, наука, технологии и образование и др.).

Представляется, что такой стиль изложения обоснован прежде всего сменой приоритетов политики государства в области ИБ. Если ранее важность проработки правовых аспектов информационной безопасности как одной из составляющих национальной безопасности РФ не вызывала сомнения, то теперь очевидно стремление государства вывести всю информационную сферу, компонентом которой является в том числе и ИБ, на качественно новый уровень в рамках международных отношений.

Доминирующими категориями теперь выступают также информационные технологии и их совершенствование в направлении

⁷⁶ Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ 05.12.2016 г. № 646) // URL: http://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения: 10.10.2019 г.)

конкурентоспособности с помощью отечественных специалистов.

Хотелось бы отметить, что сравнивать содержание доктрин 2000 г. и 2016 г. можно по множеству категорий, так как данные документы, являясь системой (совокупностью) официальных взглядов, по своей природе комплексны и многоаспектны. Однако наиболее очевидно изменения прослеживаются именно на примере ПЗИ. Сравнительно-правовой анализ доктрин в части ПЗИ (рис. 2) показал следующее.

С точки зрения раскрытия понятия ПЗИ Доктрина ИБ, утвержденная Президентом РФ от 09.09.2000 г. и утратившая силу, представляется более подходящей, поскольку в ней была отмечена прерогатива правового аспекта ИБ, которая выражается в описании состояния ИБ и основных задач по ее



Рисунок 2. Выдержки из Доктрин информационной безопасности Российской Федерации, затрагивающие вопросы правовой защиты информации

обеспечению в части правового регулирования, характеристике внутренних угроз, причиной которых выступают недостатки в правовой базе, перечислении правовых методов обеспечения ИБ РФ, а также целей и задач в части совершенствования законодательной базы РФ.

Причины отступления от досконального описания правового регулирования ИБ в тексте Доктрины 2016 г., явного выдвижения на первый

план вопросов развития национальных информационных технологий на качественно новом уровне, а также стремления России к лидирующим позициям на международной арене могут заключаться в следующем. Разница в утверждении Доктрин составляет 16 лет, и очевидно, что за это время проведена колоссальная работа во всех сферах национальных интересов и приоритетов РФ, которые обозначены в том числе и в Доктрине 2000 г.

Развитие государства предопределяет динамику в актуализации законодательных документов, затрагивающих перечень приоритетных направлений обеспечения ИБ..

3.4 Актуальные направления информационной безопасности Российской Федерации

Главной целью Доктрины⁷⁷ информационной безопасности названа совместная охрана интересов личности, общества и страны в информационной сфере. Деятельность организаций в области защиты информации опирается на созданную государством прочную основу в виде контроля за российским сектором Интернета, развития отечественного рынка программного обеспечения и электронного оборудования. В этих условиях появляются новые основные направления информационной безопасности. Эксперты, работающие в этой сфере утверждают, что в ближайшие пять лет ситуация изменится еще более радикально. С учетом быстрого развития в сфере защиты информации сейчас выделяется несколько актуальных направлений.

Безопасность критически важных объектов. Принятый в ходе реализации Доктрины информационной безопасности Российской Федерации закон о критической информационной инфраструктуре ввел понятие критически важных объектов (КВО). Эксперты иногда определяют их как критически важные информационные системы. К ним относятся:

– системы управления государственными и правоохранительными

⁷⁷ Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ 05.12.2016 г. № 646) // URL: http://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения: 15.10.2019 г.)

органами, МЧС, системы обеспечения пожарной и военной безопасности;

- информационная инфраструктура кредитно-финансовых учреждений;

- системы связи, спутниковые, географические, навигационные системы;

- системы управления ресурсоснабжающими организациями (электростанциями, водоканалами);

- системы управления транспортом;

- системы управления опасными объектами.

Представляющие высокую значимость для страны и, соответственно, интерес для потенциальных противников объекты и автоматизированные системы управления ими требуют особого внимания к выстраиванию концепции защиты информации и обеспечению безопасности, как экономической, так и экологической. Информационно-телекоммуникационные системы, действующие в составе КВО, защищаются по нормативам, установленным приказами ФСТЭК РФ. Попытки перехвата управления такими системами и увеличение количества объектов и их сложности в процессе экономического роста требуют повышенного внимания к развитию этого направления защиты информации и обеспечения безопасности объектов критической инфраструктуры.

Разработка кибероружия. Информационная безопасность базируется не только на создании нескольких уровней защищенности, но и на разработке превентивных мер, которые снизят риск посягательства на критически важные системы. Разработка собственного кибероружия гарантирует обеспечение безопасности, так как риск ответного удара может оказаться серьезным. Поэтому при наличии собственных инструментов нападения количество внутренних и внешних угроз может снизиться.

Помимо решения текущих методологических и кадровых задач, которые требуют высокой компетенции от специалистов, необходимы новые разработки. Одной из них может стать аналог программных

продуктов компании Ntrepid, позволяющих моделировать сетевые дискуссии. Такое решение актуально перед выборами или голосованием по вопросам, существенно важным для государства.

Облачная безопасность. Многие компании отказываются от хранения информации на серверах и перемещают ее в облако. Там же чаще всего находится информация, обрабатываемая при работе программных продуктов для малого бизнеса, бухгалтерских и CRM-систем. Часто, особенно при размещении в облачных системах персональных данных, возникает вопрос об их защищенности в соответствии с требованиями законодательства и возможности несанкционированного доступа к информации. Эта задача пока не решается на законодательном уровне и становится вопросом частной договоренности между предприятием и владельцем облачной системы хранения.

В этой сфере существует множество нерешенных вопросов в области:

- нормативно-правового регулирования;
- технического обеспечения, разработки новых средств защиты информации;
- организационного взаимодействия.

Регулирование защиты информации в облаке и обеспечение безопасности данных является одним из важнейших направлений развития информационной безопасности для корпоративного сектора в ближайшее время.

Противодействие мошенничеству в финансово-кредитной сфере. Фишинг и другие мошеннические методы списания средств с платежных карт граждан стали повседневной реальностью. Информационные системы банков постоянно страдают от хакерских атак. Разработка стандартов обеспечения их информационной безопасности возложена на ЦБ РФ, но выбор средств и методов остается за кредитным учреждением.

Развитие информационной безопасности в финансовой сфере

актуально и для банков⁷⁸, и для компаний, желающих дополнительно обезопасить активы и массивы конфиденциальной информации, содержащие архив финансовых транзакций. Эти же меры, технические и аппаратные средства, могут быть использованы для защиты электронной коммерции.

Противодействие угрозам предполагает:

- защиту каналов удаленного доступа, трафика передачи финансовой конфиденциальной информации;
- разработку и внедрение процессов борьбы с мошенничеством, направленным на воровство средств;
- мониторинг всех транзакций, который среди сотен тысяч проходящих через банковскую систему операций может обнаружить мошеннические.

Защита личных данных. Разработанная государственными органами система защиты персональных данных не полностью закрывает все потребности физического лица. Защита информации осуществляется в отношении только тех сведений, которые были переданы компаниям и обрабатываются в рамках их информационных систем. При этом крайне плохо защищена медицинская информация, особенно данные, передаваемые по электронным каналам связи. Никак не регулируются попытки кражи личности, например, взломы аккаунтов в социальных сетях. Рынок информационных услуг только начинает развиваться, но это направление должно стать более актуальным с повышением уровня знаний граждан об их информационных правах.

Безопасность медицинских систем. Новым решением в здравоохранении стала телемедицина или предоставление услуг в режиме телеконференции. Передаваемые данные не всегда защищены надлежащим образом, что вызывает необходимость решить эту задачу. Новое

⁷⁸ Банк России. Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019 – 2021 годов. Москва, 2019

направление безопасности коснется не только защиты персональных данных граждан, но и систем управления медицинскими учреждениями, каналами связи, каналами передачи документированной медицинской информации, например, между медицинским центром и лабораторией, проводящей исследования. Комплексная безопасность медицинских систем становится насущной необходимостью при охране интересов личности.

Безопасность мобильных устройств. Эксперты в области информационной безопасности считают, что смартфон – это информационная бомба, содержащая полную и исчерпывающую информацию о человеке, его передвижениях, покупках, связях, увлечениях. Не только попадание телефона в чужие руки, но и проникновение в него вируса угрожают конфиденциальности информации.

Основная доля рынка по защите мобильных устройств приходится на крупных игроков, но отдельные антивирусные решения и средства защиты информации разрабатывают небольшими компаниями или научно-исследовательскими организациями. Так, одно из решений в области MDM (Mobile Device Management) в России был разработано НИИ СОКБ по заказу «Газпрома».

Обеспечение достоверности информации в глобальных информационных системах. Это направление только развивается, но в ситуации, когда большая часть сведений при анализе различных объектов и явлений берется в Интернете, вопрос их достоверности становится актуальным. Необходимо внедрить в практику повсеместное проявление такого свойства безопасности, как безотказность, и использовать возможности электронного интеллекта для проверки достоверности данных.

Регулярный мониторинг новых направлений развития электронного мира и экономики порождает и новые направления для развития технологий в сфере информационной безопасности, при этом в основе всех разработок должна лежать защита интересов личности, общества и государства.

Исследование тенденций развития института информационной

безопасности в Российской Федерации позволяет прийти к следующим выводам.

Информационное право - комплексная отрасль права и новое научное направления формирующейся юридической науки.

Имеющийся массив законов и опыт правоприменения позволил за последние 20 лет оформить блоки нормативно-правового материала по основным институтам информационного права. Это институт права на информацию и формы его реализации, институт правового обеспечения информационной безопасности, институт тайн.

Нормативно-правовое усиление по таким направлениям, как защита каналов связи, сетевая и эксплуатационная безопасность, компьютерная безопасность, административная безопасность способно комплексно решать ключевые задачи по сохранению и защите информационных ресурсов России, укреплению ее международного авторитета, повышению эффективности работы по снижению криминальной напряженности, защите прав, свобод и безопасности российских граждан в системе их информационно-коммуникационных взаимодействий.

Главная тенденция, на которую следует обратить внимание – это обозначение законодателем особой роли государства в системе защиты культурно-исторических и демократических ценностей общества.

Доктрина информационной безопасности 2016 года отличается отсутствием расширенного описания правового регулирования информационной безопасности, выдвижением на первый план вопросов развития национальных информационных технологий и стремлением России к лидирующим позициям на международной арене. За период в 16 лет, разделяющий Доктрины, была проведена значительная работа во всех сферах национальных интересов и приоритетов Российской Федерации.

Актуальными направлениями политики России в области информационной безопасности являются: обеспечении безопасности критической информационной инфраструктуры, разработка кибероружия,

развитие безопасности облачных хранилищ данных, противодействие угрозам информационной безопасности в финансово-кредитной сфере и защита персональных данных граждан. Их актуальность обусловлена созданной государством основой в виде контроля за российским сектором Интернета, развитием отечественного рынка программного обеспечения и электронного оборудования, совершенствованием информационного законодательства и нормативно-правовой базы в области информационной безопасности, а также постоянным ростом количества существующих угроз безопасности личности, общества и государства в информационной сфере.

ЗАКЛЮЧЕНИЕ

В заключение работы необходимо обобщить результаты исследования и сформулировать на этой основе ряд положений и выводов.

Информационная безопасность Российской Федерации – это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В работе рассмотрено большое количество нормативных правовых актов Российской Федерации, регулирующих различные аспекты информационной безопасности. Основопологающим документом в данной сфере выступает Конституция Российской Федерации.

Исследован вопрос правовых методов обеспечения информационной безопасности, заключающийся в разработке нормативно-правовых актов, регламентирующих отношения в информационной сфере и нормативно-методических документов по вопросам обеспечения информационной безопасности Российской Федерации.

В Российской Федерации в настоящее время реализуется целый комплекс мероприятий, направленных на совершенствование нормативно-правового обеспечения информационной безопасности: формируются механизмы противодействия внутренним и внешним угрозам в информационной сфере, непрерывно дополняется законодательство, регулирующее информационные правоотношения и область обеспечения информационной безопасности Российской Федерации. Это находит законодательное закрепление в документах стратегического планирования и нормативных правовых актах различного уровня.

В выпускной квалификационной работе рассмотрены различные аспекты организационно-правового и технического обеспечения информационной безопасности отдельных субъектов и объектов информационных правоотношений. Существующая в работе выборка

призвана подчеркнуть репрезентативность и уникальность каждой отдельной структуры в контексте обеспечения её информационной безопасности.

Рассмотрены ключевые моменты развития информационного права и действующего законодательства в области информационной безопасности и защиты информации. Законодательство в указанной области представляет собой динамично развивающуюся нормативно-правовую базу, призванную отвечать современным требованиям обеспечения национальной безопасности Российской Федерации в информационной сфере и подчеркнуть стремление России к лидерству в области информационных технологий.

В условиях непрерывного развития нормативно-правового обеспечения информационной безопасности в Российской Федерации можно выделить следующие приоритетные задачи нормативно-правового и иного регулирования данной области:

- Устранение несогласованности между информационно-коммуникационными технологиями (большие данные, облачные технологии, суперкомпьютеры, искусственный интеллект и т.д.) и законодательством Российской Федерации, регулирующим вопросы безопасности в этой сфере, развития и использования цифровых технологий. Например, несмотря на лавинообразный рост возможностей для сбора в Интернете личных данных граждан (персональные данные являются их частью) и использования их массивов (больших данных), до сих пор эта сфера не упорядочена и не введена в правовое поле. При этом такие информационные массивы могут использоваться во вредоносных целях и перепродаваться, например, для слежки, шантажа, пропаганды и т.д. Кроме того, эти данные накапливаются и могут быть использованы против человека спустя много лет. Таким образом, законодательное регулирование таких процессов — часть информационной безопасности государства.

- Ликвидация неоднозначности положений некоторых законов, которые по-разному трактуются государственными регуляторами и

операторами и которые требуют конкретизации, уточнений и разъяснений. Кроме того, существует проблема терминологии. Например, в ООН по инициативе России используется компромиссный термин «информационно-коммуникационные технологии». В официальных документах Российской Федерации также отсутствует термин «кибербезопасность». Вместе с тем в технических регламентах и ГОСТах приставка «кибер» активно используется.

- Снижение стоимости и общей сложности систем технической защиты информационных систем персональных данных. Как органы государственной власти, так и граждане России и различные организации ежедневно сталкиваются с вопросом дороговизны и сложности процесса обеспечения информационной безопасности своих интересов.

- Ликвидация зависимости информационной безопасности Российской Федерации от иностранных поставщиков программно-аппаратных компонентов программного обеспечения и оборудования. Так, большинство интернет-технологий (браузеры, поисковики, социальные сети, операционные системы) находится вне пределов российского контроля. Это создает дополнительные угрозы безопасности. Поэтому для обеспечения своего суверенитета государству следует иметь полную технологическую цепочку, начиная от процессора и заканчивая конечным программным обеспечением. Разработка современных программно-аппаратных компонентов как направление закреплена в Доктрине информационной безопасности 2016 года и различных стратегиях информационного развития, однако отсутствует реальная видимая правовая, финансовая и методическая поддержка отечественных разработок в сфере информационных технологий.

- Совершенствование информационной безопасности в социальной и образовательной сферах.

- Снижение вероятности рисков ущерба репутации государства в связи с вредоносным использованием информационно-коммуникационных

технологий в политической конкуренции, что может выражаться и в финансовых потерях.

– Адаптации законодательства государства к глобальным угрозам информационной безопасности на международном уровне. В частности, разработка и принятие Стратегии информационной безопасности России на период после 2020 года; совершенствование законодательства Российской Федерации, способствующего созданию международной нормативно-правовой базы по борьбе с угрозами информационной безопасности.

Ввиду истечения срока действия Стратегии информационной безопасности Российской Федерации до 2020 года решение существующих задач можно сократить до трёх рекомендаций:

– регулярно вносить изменения в существующее законодательство, исходя из анализа практики применения и новых условий, связанных с ускоренным развитием сферы обеспечения информационной безопасности;

– вести работу по подготовке новой Стратегии информационной безопасности РФ с учетом современных проблем и требований к обеспечению защищенности интересов Российской Федерации и, что самое главное, интересов её граждан;

– начать подготовку новых нормативно-правовых актов на основе новой Стратегии информационной безопасности РФ.

Реализуемые направления информационной безопасности соответствуют интересам Российской Федерации в сфере информационных правоотношений, их реализация способствует устранению существующих угроз и защите прав граждан в непрерывно развивающемся потоке глобального информационного обмена.

Положения данной магистерской работы могут служить для дальнейших исследований проблем конституционно-правового регулирования информационной безопасности Российской Федерации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно-правовые акты:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства Российской Федерации от 4 августа 2014 г. № 31. – Ст. 4398.
2. Федеральный конституционный закон от 31 декабря 1996 г. N 1-ФКЗ «О судебной системе Российской Федерации» (в ред. от 30 октября 2018 г.) // Собрание законодательства Российской Федерации от 6 января 1997 г. № 1 ст. 1.
3. Федеральный конституционный закон от 26 февраля 1997 г. N 1-ФКЗ «Об Уполномоченном по правам человека в Российской Федерации» (в ред. от 31 января 2016 г.) // Собрание законодательства Российской Федерации от 3 марта 1997 г. № 9 ст. 1011.
4. Федеральный конституционный закон от 17 декабря 1997 г. N 2-ФКЗ «О Правительстве Российской Федерации» (в ред. от 28 декабря 2016 г.) // Собрание законодательства Российской Федерации от 22 декабря 1997 г. № 51 ст. 5712.
5. Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ (в ред. от 02.12.2019 г.) // Собрание законодательства Российской Федерации от 17 июня 1996 г. № 25 ст. 2954.
6. Часть вторая Налогового кодекса Российской Федерации от 5 августа 2000 г. N 117-ФЗ (в ред. от 19.12.2019 г.) // Российская газета от 10 августа 2000 г. № 153-154.
7. Кодекс профессиональной этики адвоката, принят первым Всероссийским съездом адвокатов 31 января 2003 г. (в ред. от 22 апреля 2013 г.) // Сборник законодательных и нормативных актов РФ «Экспресс-закон»,

декабрь 2003 г., № 45.

8. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 N 395-1 (в ред. от 02.12.2019 г.) // Ведомости съезда народных депутатов РСФСР от 6 декабря 1990 г. N 27 ст. 357.

9. Закон РФ от 27.12.1991 N 2124-1 «О средствах массовой информации» (в ред. от 02.12.2019) // Российская газета от 8 февраля 1992 г. № 32.

10. Закон РФ от 21 июля 1993 г. N 5485-1 «О государственной тайне (в ред. от 29.07.2018) // Российская газете от 21 сентября 1993 г. № 182.

11. Федеральный закон от 17 июля 1999 г. N 176-ФЗ «О почтовой связи» (в ред. от 29.06.2018) // Российская газета от 22 июля 1999 г. № 140-141.

12. Федеральный закон от 18 июля 1999 г. N 183-ФЗ «Об экспортном контроле» (в ред. от 13 июля 2015 г.) // Российская газета от 29 июля 1999 г. N 146.

13. Федеральный закон от 7 августа 2001 г. N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (в ред. от 02.08.2019 г.) // Собрание законодательства Российской Федерации от 13 августа 2001 г. № 33 (Часть I) ст. 3418.

14. Федеральный закон от 29.07.2004 № 98-ФЗ, «О коммерческой тайне» (в ред. от 18.04.2018 г.) // Российская газета, № 166, 05.08.2004.

15. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ в ред. от 02.12.2019 // Российская газета, № 165, 29.07.2006.

16. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (в ред. от 31.12.2017 г.) // Российская газета от 29 июля 2006 г. № 165.

17. Федеральный закон от 27 июля 2010 г. N 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (в ред. от 01.04.2019 г.) // Российская газета от 30 июля 2010 г. № 168.

18. Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности» // Собрание законодательства Российской Федерации от 3 января 2011 г. № 1 ст. 2.

19. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» (в ред. от 23.06.2016) // Российская газета от 8 апреля 2011 г. № 75.

20. Федеральный закон от 21 июля 2011 г. N 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» // Российская газета от 26 июля 2011 г. № 161.

21. Федеральный закон от 28 июля 2012 г. N 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» // Российская газета от 30 июля 2012 г. № 172.

22. Федеральный закон от 7 июня 2013 г. N 112-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Российская газета от 11 июня 2013 г. № 124.

23. Федеральный закон от 5 мая 2014 г. N 97-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей» // Российская газета от 7 мая 2014 г. № 101.

24. Федеральный закон от 6 июля 2016 г. N 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и

обеспечения общественной безопасности» // Российская газета от 8 июля 2016 г. № 149.

25. Федеральный закон от 1 мая 2017 г. N 87-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации» // Российская газета от 3 мая 2017 г. N 94.

26. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Российская газета от 31 июля 2017 г. N 167.

27. Федеральный закон от 29 июля 2017 г. N 241-ФЗ «О внесении изменений в статьи 10.1 и 15.4 Федерального закона «Об информации, информационных технологиях и о защите информации» // Российской газете» от 4 августа 2017 г. № 172.

28. Федеральный закон от 29 июля 2017 г. N 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» // Российская газета от 4 августа 2017 г. N 172.

29. Федеральный закон от 23 апреля 2018 г. N 102-ФЗ «О внесении изменений в Федеральный закон «Об исполнительном производстве» и статью 15.1 Федерального закона «Об информации, информационных технологиях и о защите информации» // Российская газета от 25 апреля 2018 г. N 88.

30. Федеральный закон от 1 мая 2019 г. N 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» // Российская газета от 7 мая 2019 г. № 97.

31. Указ Президента РФ от 31 декабря 1993 г. N 2334 «О дополнительных гарантиях прав граждан на информацию» // Российская газета от 10 января 1994 г. № 4.

32. Указ Президента РФ от 5 декабря 2016 г. N 646 «Об утверждении

Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации от 12 декабря 2016 г. № 50 ст. 7074.

33. Указ Президента РФ от 9 мая 2017 г. N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // Собрание законодательства Российской Федерации от 15 мая 2017 г. № 20 ст. 2901.

34. Указ Президента РФ от 8 августа 2019 г. N 372 «О внесении изменения в перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента Российской Федерации от 30 ноября 1995 г. N 1203» // Российская газета от 9 августа 2019 г. № 99.

Учебная и научная литература

35. Агапов А. Б. Основы государственного управления в сфере информатизации в Российской Федерации/ А.Б. Агапов. М.: Юристъ. – 2007. – 284 с.

36. Бачило И.Л. Информационные проблемы в сфере государственного управления. Информационные проблемы в сфере административной реформы / И.Л. Бачило. – М.: Сборник трудов. – 2015. – 704 с.

37. Бачило И.Л. Организационно-правовые условия обеспечения информационной безопасности / И.Л. Бачило. М.: Проспект. – 2016. – 118 с.

38. Ботуз С. Правовая защита объектов интеллектуальной собственности в «Интернете» /С. Ботуз.- М.: ИНФРА Профобразование. – 2014. – 411 с.

39. Венгеров А.Б. Право и информация в условиях автоматизации управления (теоретические вопросы). / Венгеров А.Б.- М.: Юрид. лит., 1978. – 208 с.

40. Волков Ю. В. К вопросу о методе информационного права / Ю.В. Волков. – М.: Либроком. – 2015. – 168 с.

41. Волчинская Е. К. О стратегии и проблемах развития

законодательства в сфере обеспечения информационной безопасности/ Е.К. Волчинская. – М.: Флинта. – 2015. – 189 с.

42. Гатчин, Ю. А. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. А. Гатчин, В. В. Сухостат. - СПб. : Санкт-Петербургский государственный университет информационных технологий, механики и оптики, 2010. - 98 с.

43. Гатчин, Ю. А. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю. А. Гатчин, Ю. В. Донецкая, А.С. Куракин, В. В. Сухостат. - 2-е изд., испр. и доп. - СПб. : Университет ИТМО, 2018. - 100 с.

44. Городов О.А. Информационное право: учебник для бакалавров/ О.А. Городов. – М.: Эксмо. – 2011. – 316 с.

45. Дозорцев В.А. Информация как объект исключительного права. «Дело и право». / Дозорцев В.А. – М.: Октябрь. – 1966г. – 139 с.

46. Зорькин, В. Д. Современный мир, право и Конституция / В. Д. Зорькин. - М. : Норма, 2010. - 545 с.

47. Информационная безопасность России : колл. монография / Е. А. Ерофеев, Ю. С. Уфимцев, В. Г. Шевченко и др. - М. : 4-й филиал Воениздата, 2001. - 624 с.

48. Колобов О.А., Ясенев В.Н. Информационная безопасность и антитеррористическая деятельность современного государства: проблемы правового регулирования и варианты их решения. / Колобов О.А., Ясенев В.Н. – М.:Н. Новгород: Фин. фак-т ННГУ, 2011.

49. Колоткина, О. А. Теория государства и права: учебное пособие / О. А. Колоткина, И. Д. Ягофарова. - Екатеринбург : Уральский институт коммерции и права, 2015. - 176 с.

50. Копылов В.А. Информационное право / В.А. Копылов. - Издательство: «Юридический центр Пресс». - 2015. - 187 с.

51. Копылов В.А. Информационное право / В.А. Копылов. – Издательство: «Юридический центр Пресс». – 2015. – 187 с.

52. Кузнецов П.У. Основные положения государственной политики в сфере информационной безопасности на региональном уровне / П.У. Кузнецов. – М.: Статут. – 2013. – 312 с.
53. Кузнецов П.У. Проблемы предупреждения преступлений в информационной сфере: межотраслевые аспекты (в соавторстве) / П.У. Кузнецов - М.: Юстиция. - 2016. - 624 с.
54. Куняев Н.Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере / Н. Н. Куняев. – М.: Книжный мир. – 2017. – 684 с.
55. Лапина М.А. Актуальные проблемы информационного права/ М.А. Лапина. - М.:Юстиция. - 2016. - 214 с.
56. Лопатин В.Н. Информационная безопасность в России: Проблемы, поиски решений. 2008. №2 ГИСДВ.
57. Оксамытный, В. В. Общая теория государства и права: учебник / под ред. В. В. Оксамытного. - М. : ЮНИТИ-ДАНА, 2012. - 511 с.
58. Рассолов, М. М. Теория государства и права : учебник для вузов / М. М. Рассолов. - М. : Юрайт, 2010. - 635 с.
59. Сёмкин А.Н. Основы правового обеспечения защиты информации. Учебное пособие для вузов / А.Н. Сёмкин. – Уфа: АН РБ, Гилем. – 2010. – 136 с.
60. Тедеев А.А. Информационное право (право Интернета): Учебное пособие /А.А. Тедеев – М.: Юрайт. – 2015. – 468 с.
61. Шиверский А. А. Защита информации: проблемы теории и практики. / А.А. Шиверский.-М. : Юристъ. – 2016. – 112 с.
62. Чеботарева, А. А. Личность и ее безопасность в глобальном информационном обществе (правовой аспект) : монография / А.А. Чеботарева. - М., 2017. - 202 с.
63. Артамонова, Я. С. Информационная безопасность российского общества: теоретические основания и практика политического обеспечения : дис. ... д-ра полит. наук: 23.00.02 / Ярославна Сергеевна Артамонова. - М.,

2014. - 359 с.

64. Бородин, А. С. Информационная безопасность в современной России: политологический анализ : дис. ... канд. полит. наук: 23.00.02 / Алексей Сергеевич Бородин. - СПб. , 2009. - 211 с.

65. Борисов, А. Ю. Государственная политика в области информационной безопасности на современном этапе : дис. ... канд. полит. наук: 23.00.02 / Алексей Юрьевич Борисов. - М., 2006. - 166 с.

66. Виноградова, Н. В. Правовой механизм защиты информационных прав и свобод человека и гражданина в Российской Федерации : дис. ... канд юрид. наук: 12.00.01 / Наталья Владимировна Виноградова. - Саратов, 2011. - 196 с.

67. Тамодлин, А. А. Государственно-правовой механизм обеспечения информационной безопасности личности : дис. . канд. юрид. наук: 12.00.01 / Александр Анатольевич Тамодлин. - Саратов, 2004. - 175 с.

Научные статьи

68. Алешкова, И. А. Понятие и особенности права на безопасность личности, место в системе других прав и свобод / И. А. Алешкова // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. - 2011. - № 10 (16). - С. 86-93.

69. Алиева, М. Ф. Информационная безопасность как элемент информационной культуры / М. Ф. Алиева // Вестник Адыгейского государственного университета. - 2012. - № 4 (108). - С. 97-102.

70. Анохина, С. Ю. Информационная безопасность как основной элемент системы национальной безопасности государства / С. Ю. Анохина, Т. Д. Логинова // Алтайский юридический вестник. - 2016. - № 4 (16). - С. 2-125.

71. Ардашев, А. И. Конституционно-правовое обеспечение права человека на безопасность в Российской Федерации / А. И. Ардашев // Современное право. - № 1. - 2008. - С. 39-45.

72. Баринов, С. В. О правовом определении понятия

«информационная безопасность личности» / С. В. Баринов // Актуальные проблемы российского права. - 2016. - № 4 (65). - С. 97-105.

73. Бекетов, Н. В. Информационная безопасность развития государства / Н. В. Бекетов // Информационные ресурсы России. - 2004. - № 6. - С. 32-35.

74. Галушкин А.А. «К вопросу об информационной безопасности и предоставлении государственных и муниципальных услуг посредством сети» Интернет/ Галушкин А.А. // Правозащитник. 2015. № 3. С. 9.

75. Гриценко, А. А. Теоретико-методологические подходы к определению понятия безопасности / А. А. Гриценко // Вестник Новосибирского государственного университета. Сер.: Философия. - 2008. - Т. 6. - №3. С. 8691.

76. Закупень, Т. В. Понятие и сущность информационной безопасности и ее место в системе обеспечения национальной безопасности Российской Федерации / Т. В. Закупень // Информационные ресурсы России. - 2009. - № 4 (110). - С. 28-34.

77. Коровяковский Д.Г. «Коммерческая тайна. Доступ к сведениям, составляющим коммерческую тайну» / Д.Г.Коровяковский // Вестник Челябинского государственного университета. – 2014. – №3. – С. 30 – 36.

78. Кусова, Е. А. Правовое обеспечение информационной безопасности органов государственной власти / Е. А. Кусова // Вестник Тамбовского государственного университета им. Г. Р. Державина. - 2011. - Вып. 7 (99). - С. 210-213.

79. Логинова, Т. Д. Государство как субъект обеспечения информационной безопасности личности / Т. Д. Логинова // Проблемы правоохранительной деятельности и образования: сборник научных трудов. - 2018. - Вып. 15. - С. 35-40.

80. Марков, А. А. Некоторые аспекты информационной безопасности в контексте национальной безопасности / А. А. Марков // Вестник Санкт-Петербургского ун-та. Сер.: Психология. Социология. Педагогика. - 2011. -

№ 1. - С. 43-48.

81. Пакляченко М.Ю. Новая доктрина информационной безопасности: вопросы правовой защиты информации. / Пакляченко М.Ю. // История и архивы. 2017;(2):96-103.

82. Рыженкова, О. Ю. Информационная безопасность: определение понятия, место в системе национальной безопасности / О. Ю. Рыженкова // Закон и право. - 2009. - № 1. - С. 50-52.

83. Самохвалов А.А. «Информация как объект гражданских прав» /А.А. Самохвалов// Правовая мысль: история и современность. - 2015. - №2. - С. 4-18.

84. Чеботарева, А. А. Проблема информационной безопасности личности в механизме взаимодействия государства и информационного общества / А. А. Чеботарева // УрФО. Безопасность в информационной сфере. - 2016 - № 1 (19). - С. 56-60.

85. Элькин В.Д. «К вопросу об оценке уровня информационной безопасности» / В.Д. Элькин// Юрист. – 2016. – №6. – С. 11 – 18.