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

ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
Кафедра государственного и муниципального управления

Заведующий кафедрой
канд. юрид. наук, доцент
О.В. Алиева

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
магистра

ТЕМА
ЗАЩИТА ИНФОРМАЦИИ, ОГРАНИЧЕННОЙ В ДОСТУПЕ, В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ (НА ПРИМЕРЕ ЯМАЛО-НЕНЕЦКОГО АВТОНОМНОГО ОКРУГА)

38.04.04Государственное и муниципальное управление
Магистерская программа «Публичное управление»

Выполнил работу студент 3 курса заочной формы обучения	Пиджаков Вадим Витальевич
Научный руководитель к.ю.н., доцент	Хвощин Алексей Александрович
Рецензент Директор департамента специальных мероприятий Ямало-Ненецкого автономного округа	Гринь Константин Константинович

Тюмень
2020 год

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ

АРМ	-	автоматизированное рабочее место
АС	-	автоматизированная система
ГИС	-	государственная информационная система
ГНИИИ ПТЗИ	-	Государственный научно-исследовательский испытательный институт проблем технической защиты информации
ГосСОПКА	-	государственная система обнаружения, предотвращения и ликвидации компьютерных атак
ГСЗИ	-	Государственная система защиты информации
ГТК	-	Государственная техническая комиссия при Президенте Российской Федерации
ИБ	-	информационная безопасность
ИКТ	-	информационно-коммуникационные технологии
ИСПДн	-	информационная система персональных данных
ИТ	-	информационные технологии
КИИ	-	критическая информационная инфраструктура
НКЦКИ	-	Национальный координационный центр по компьютерным инцидентам
НСД	-	несанкционированный доступ
ОС	-	операционная система
ПДн	-	персональные данные
РД	-	руководящие документы
СЗИ	-	система защиты информации
ТЗИ	-	техническая защита информации
ФСБ	-	Федеральная служба безопасности России
ФСТЭК	-	Федеральная служба по техническому и экспортному контролю

ВВЕДЕНИЕ

Актуальность исследования. Гражданско-правовые отношения могут возникать в отношении различных объектов, очевидно и в отношении нематериальных благ. Само название указанных объектов гражданских правоотношений заключает в себе смысл указанных ценностей.

Нематериальные блага достаточно тесно связаны с таким понятием как личные права и свободы человека и гражданина. Поэтому их защита и охрана являются первоочередными вопросами при регулировании государством общественных отношений. Значение нематериальных благ, а равно вопроса по их защите и осуществлению надзора за их соблюдением является достаточно высоким и признается в различных сферах деятельности человека. Если обратиться к правовой системе Российской Федерации, то такие блага являются ценностью в рамках гражданского права, конституционного права, уголовного права и в рамках других отраслей.

Информация является одной из категорий, которая необходима каждому человеку для нормального и полноценного существования. При этом, информация подразделяется на несколько видов, в сущности от того, какую ценность она имеет и какой смысл несет. Так, помимо положительной информации, которая содержит в себе полезные свойства, принято выделять и такую информацию, которая может приносить определенный вред не только психике, моральному и материальному состоянию людей, но и их физическому здоровью.

При этом, следует говорить о том, что в обществе существуют отдельные группы лиц, которые являются наиболее незащищенными, поэтому могут быть подвергнуты наибольшему влиянию со стороны различных средств информации, причиняющих им вред (особое место среди указанных групп людей занимают дети, так как их психологическое восприятие мира не до конца сформировано, и они подвержены негативному влиянию средств массовой информации).

В рамках рассмотрения информации достаточно важно уделить внимание правовым режимам различных видов информации, таким как: тайна государства, тайна коммерции, семейная тайна, тайна банковских вкладов и другие.

Существенно важна защита информации и непосредственно в органах государственной власти. Данные, которыми располагают государственные органы, очевидно носят закрытый характер. Доля информационного массива является секретной, поэтому недопустимо ее распространение куда бы то ни было. На сегодняшний день существуют различные способы защиты информации, в том числе обеспечение определенных режимов для служебного пользования, секретности, шифровка, компьютерная защита и так далее.

В прошлом веке, примерно до середины 70-х годов, государству не удавалось максимально обеспечить защиту информации. Но уже сейчас существует множество механизмов ее защиты, технологические процессы не стоят на месте, появились новые системы, которым по силе предотвратить информационные посягательства, однако, зачастую, и они оказывается недостаточно эффективными (так, например, некоторые государства отключают свои информационные ресурсы от всемирной паутины-Интернет, так как в последнее время возросли атаки на государственные ресурсы информации, в частности, так поступили спецслужбы США).

На государство работают различные IT-специалисты, которые создают специальное программное обеспечение, обеспечивающее высокий уровень защиты информации, хранящейся на компьютерных носителях. Однако появляются все новые и новые способы атаки на государственные, в том числе секретные, ресурсы. В некоторых государственных организациях, которые используют секретные сведения, предусмотрены свои методы защиты (так, например, во многих правоохранительных органах запрещено подключать компьютеры к системе Интернет, использовать флеш-носители в целях сохранения информации и конфиденциальных сведений; кроме того, во многих органах, например, в системе МВД, существуют свои подразделения в сфере

защиты информации, которые реализуют функции по охране конфиденциальной информации.

В целях обеспечения национальной безопасности России сегодня производятся определенные действия (рисунок 1):

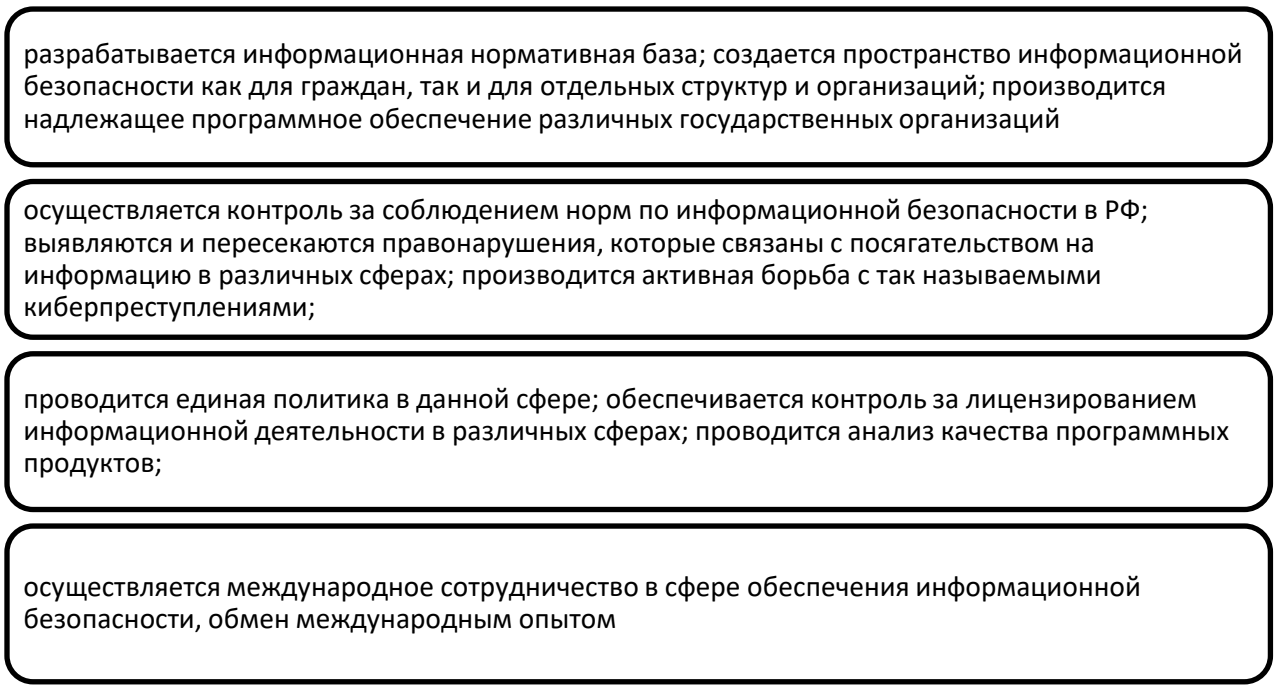


Рис. 1. Мероприятия по обеспечению национальной безопасности России.

Однако не смотря на предпринимаемые усилия, в настоящее время нельзя сказать о полном обеспечении информационной безопасности на территории России. Ежедневно обычные пользователи сталкиваются с постоянно обновляемыми вирусами, с помощью которых осуществляется отслеживание, передача конфиденциальной информации граждан. Так почему же другое будет происходить в органах государственной власти. То тут, то там в сети Интернет всплывает конфиденциальная информация, которую взламывают хакеры и выставляют на всеобщее обозрение. В настоящее время действующее законодательство не предусматривает достаточного набора инструментов для борьбы с киберпреступлениями. Все программные средства, которыми владеют на сегодняшний день правоохранительные органы, недостаточны для эффективной борьбы с правонарушителями в данной сфере.

Для того, чтобы обеспечить эффективное функционирование правоохранительных органов, необходимо не только обеспечить их надлежащим техническим оборудованием и программным обеспечением, но и соответствующими кадрами, а именно программистами, которые позволили бы внедрить эффективные системы защиты информации.

Объектом исследования являются общественные отношения, которые связаны с защитой информации и правовыми режимами её использования.

Предметом исследования являются отношения по ограниченной в доступе информационной защите в деятельности органов государственной власти в Российской Федерации.

Цель – изучить деятельность по защите информации, ограниченной в доступе, в государственных структурах страны и выявить возможности ее совершенствования, в том числе, на примере конкретного субъекта Федерации – Ямало-Ненецкого автономного округа.

Задачами работы являются:

- раскрыть понятие и свойства информации. Понятие информационной безопасности;

- рассмотреть функции и полномочия органов власти по защите информации;

- определить правовой режим информации, предназначенной для служебного пользования;

- проанализировать правовое поле режима конфиденциальной информации;

- охарактеризовать правовое регулирование информации, несущей вредное воздействие для общества.

Значимость исследования заключается в подробном исследовании защиты информации, ограниченной в доступе, в деятельности государственных органов власти в России.

Информационная база исследования. При написании работы применялся метод обобщения и классификации, метод анализа нормативно-правовых актов и научной литературы.

Теоретическая база исследования. При проведении исследования были проанализированы труды и работы авторов, которые занимались изучением защиты информации, ограниченной в доступе, в деятельности властных сруктур в Российской Федерации её составляющих, а также иные работы, отвечающие теме исследования. В науке есть исследования, которые посвящены рассмотрению определенных вопросов информационной безопасности – это работы Грошевой Екатерины Константиновны, также работы по правовому обеспечению информационной безопасности - работы Жигулина Г.П. Эти научные работы в своем большинстве проводят анализ определенных тайн, показывая наличие тех либо других правовых проблем информации конфиденциального характера в области государственного управления. Систему информационной безопасности в Российской Федерации рассматривала Ефанова Е.А. Ограничение свободы массовой информации в соответствии с Конституцией РФ можно найти в работе у В.А. Туманской. Проблемы монополизации функций исполнительными органами власти в информационной среде были проанализированы Черепановой Ю.Е.

Теоретико-методологическая основа. В рамках исследования были использованы следующие методы научного познания: апробированные методы познания, которые выявлены, а также разработаны юридической наукой. Применены общенаучный диалектический метод познания, и частнонаучные методы, которые выходят из него: логический, историко-юридический, сравнительно-правовой, системно-структурный и системно-функциональный, компаративный. Проведен обзор и анализ научных источников. Их использование дало возможность провести исследование объектов во взаимосвязях и взаимозависимостях, выявить конкретные тенденции, сделать выводы.

Апробация работы. Углубленное изучение темы информационной защиты в органах государственной власти позволило мне победить в конкурсе на формирование кадрового резерва государственной гражданской службы в департаменте специальных мероприятий Ямало-Ненецкого автономного округа. В связи с чем, положения работы планирую непосредственно использовать в своей дальнейшей деятельности.

Структура работы состоит из введения, основной части, заключения и списка литературы.

ГЛАВА 1. ПОНЯТИЕ И ОСНОВНЫЕ НАПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ

1.1. ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Бурное развитие информационных технологий в современном мире, проникновение ИТ во все области человеческой деятельности дает не только новые возможности для развития общества, но и ставит новые проблемы перед человечеством. В условиях всевозрастающего влияния цифровизации на все сферы жизни возрастает роль информационной безопасности личности, общества и государства, а ее обеспечение занимает особое место в деятельности всех государственных институтов.

Категория «информационная безопасность» является одним из наиболее поздних введенных в научный обиход понятий, сложившимся на рубеже XX-XXI веков. Категориальный понятийный аппарат информационной безопасности, изучение теоретических основ данного понятия осложняется тем, что собственно предмет, безопасность которого определяется – то есть информация – также многозначен и сложен, что придает дополнительные трудности при изучении его структуры и внутренних свойств, а также выработки требований к безопасности информации.

Новизна категории «информационная безопасность», нечеткость терминологии (в том числе и в связи с недостаточной точностью перевода), обширность области и размытость границ применения понятий, связанных с информационной безопасностью, приводит к множеству сложностей при попытках более точно очертить круг вопросов, входящих в эту категорию, при изучении теоретических основ категориального аппарата информационной безопасности.

А.В. Шободоева отмечает, что термин «информационная безопасность» понимается в настоящее время в «узком» и «широком» смысле. С этой точки зрения автор определяет в узком смысле информационную безопасность как «набор аппаратных и программных средств для обеспечения сохранности,

доступности и конфиденциальности данных в компьютерных сетях», а в широком смысле – как «состояние защищенности национальных интересов страны в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» [Шободоева, с.74].

Необходимо также подчеркнуть, что под «безопасностью» традиционно понимается «состояние защищенности», что выражается во всех определениях «информационной безопасности» (рисунок 2).

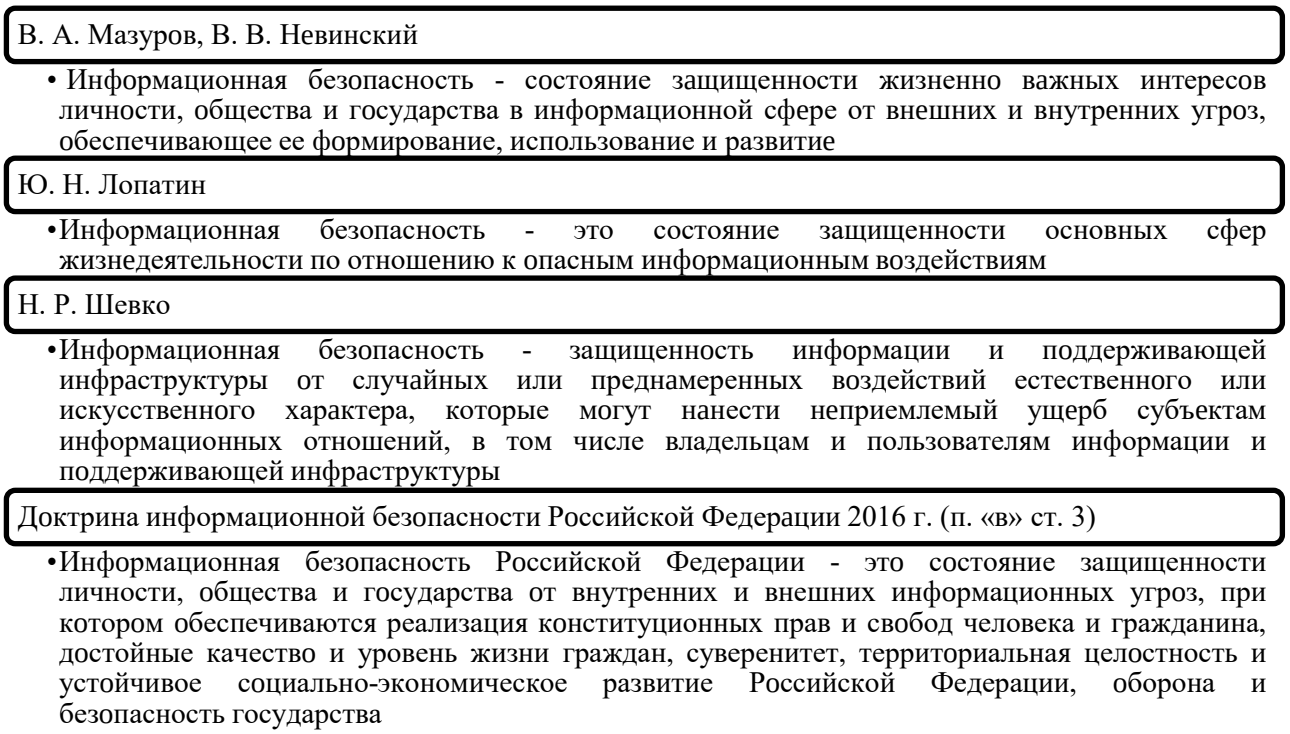


Рис. 2. Основные определения понятия «информационная безопасность».

Следует заметить, что многими специалистами термины «ИТ-безопасность» (IT security), «информационная безопасность» (information security) и «кибербезопасность» (cybersecurity) используются взаимозаменяемо, как синонимы. Так, в частности, Ясенев В.Н. отмечает, что «под информационной безопасностью в более общем виде следует понимать совокупность средств, методов и процессов (процедур), обеспечивающих защиту информационных активов и, следовательно, гарантирующих сохранение эффективности и практической полезности как технической

инфраструктуры информационных систем, так и сведений, которые в таких системах хранятся и обрабатываются» [Ясенев, с.7]. Тем не менее, эти три понятия не синонимичны.

Джеймс Стэнджер рассматривает понятие «ИТ-безопасность» как категорию, включающую три составляющие – физическую безопасность, информационную безопасность и кибербезопасность (рисунок 3) [Стейнджер].

Рис. 3. Составляющие ИТ-безопасности.

Физическая безопасность включает в себя обеспечение безопасности людей и инфраструктуры (защита зданий, серверных комнат, кабельных шкафов и т.п). Информационная безопасность подразумевает обеспечение безопасности собственно информации – в этом случае под информацией понимаются как данные на физических носителях, так и электронные активы. Обеспечение информационной безопасности включает в себя методы резервирования и хранения информации, а также методы мониторинга, позволяющие убедиться, что никто не изменял исходные данные, либо информацию, полученную в результате их обработки. Таким образом, с точки зрения информационной безопасности наибольшее значение имеет безопасность самих данных и полученной информации, а используемому оборудованию и вычислительным ресурсам придается меньшее значение. Под кибербезопасностью обеспечение защищенности данных от несанкционированного доступа к ним путем использования электронных

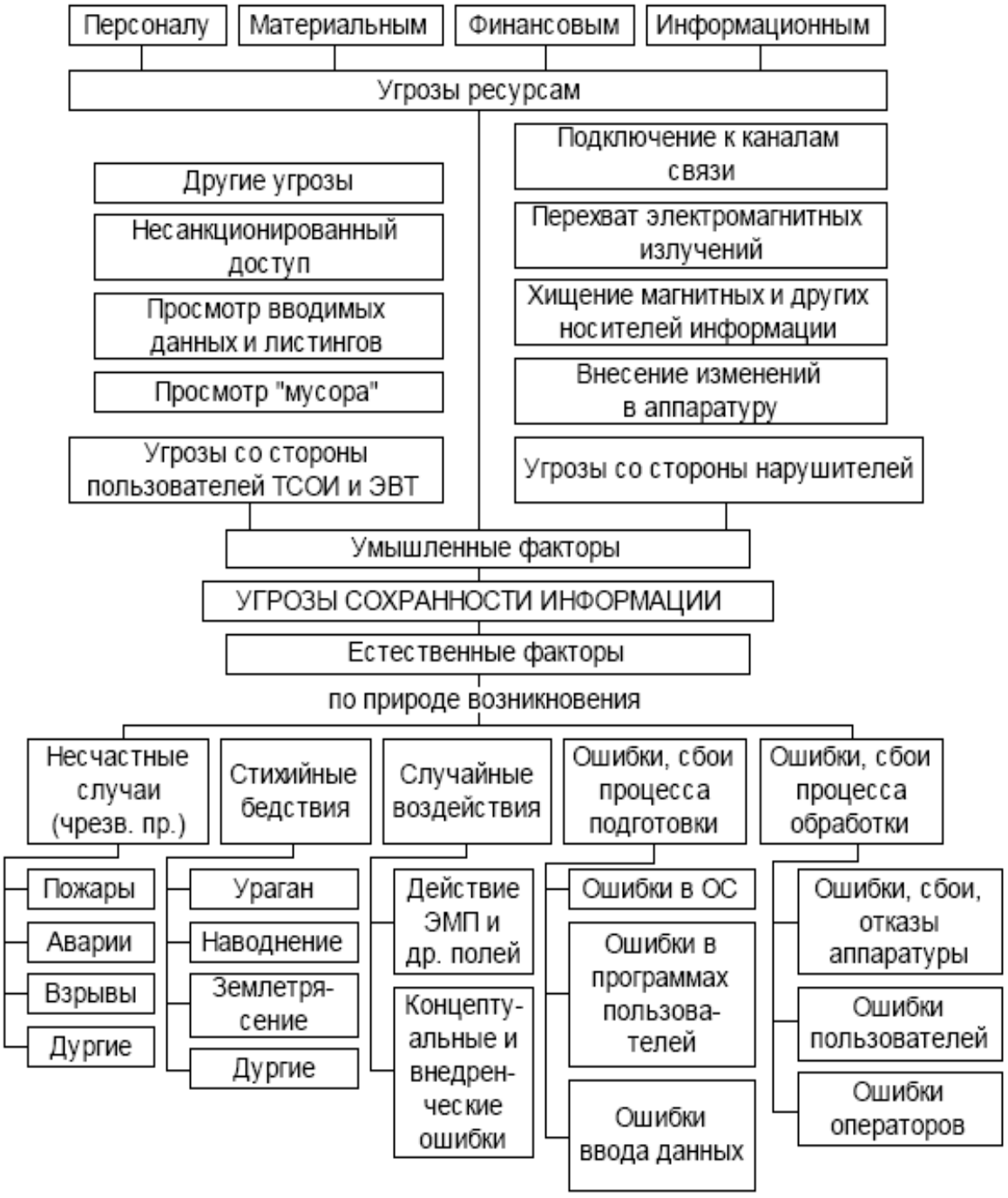
средств и сетевых ресурсов. Таким образом, кибербезопасность – это своего рода «физическая безопасность в электронном мире».

Часть специалистов ИТ, выделяя отдельно физическую безопасность, тем не менее, отождествляет кибербезопасность и информационную безопасность. Это также неверно, поскольку в кибербезопасности информационные и информационно-коммуникационные технологии (ИКТ) являются основной причиной уязвимости. Единственной наиболее определяющей характеристикой кибербезопасности является тот факт, что все активы, которые должны быть защищены, должны быть защищены от уязвимостей, которые существуют в результате использования ИКТ, составляющих основу киберпространства. Эти уязвимости могут также повлиять на нематериальные активы, информацию – и именно из-за таких нюансов кибербезопасность зачастую воспринимают как информационную безопасность. Так, например, такие проблемы, как киберзапугивание (кибербуллинг, интернет-травля, кибермоббинг), возникают именно из-за использования уязвимостей ИКТ, дающих возможность доступа к личной (персональной) информации. Таким образом, кибербезопасность (риски, связанные со взаимодействием с киберпространством) и информационная безопасность (безопасность данных и информации) тесно связаны, но, тем не менее, не являются тождественными понятиями.

Следовательно, можно сделать вывод, что информационная безопасность (ИБ) – это снижение рисков несанкционированного доступа к информации, уменьшение вероятности ее потери, искажения, кражи, а также возможное снижение негативных последствий таких действий.

Таким образом, основное внимание в области информационной безопасности уделяется сбалансированной защите конфиденциальности, целостности и доступности данных. Это означает, что данные можно получить и использовать их (доступность), они недоступны для несанкционированного доступа (конфиденциальность), а в процессе хранения и передачи данные остаются неизменными (целостность), при этом комплекс мер, обеспечивающий сохранение всех этих свойств информации, называется

защитой информации, а степень защищенности свойств информации – информационной безопасностью. Различные виды угроз информационной безопасности приведены в Приложении № 1 [Круликовский, с.126].



Приложение № 1. «Виды угроз информационной безопасности».

В комплекс мер по защите информации входят организационно-правовые и технические мероприятия (рисунок 4).

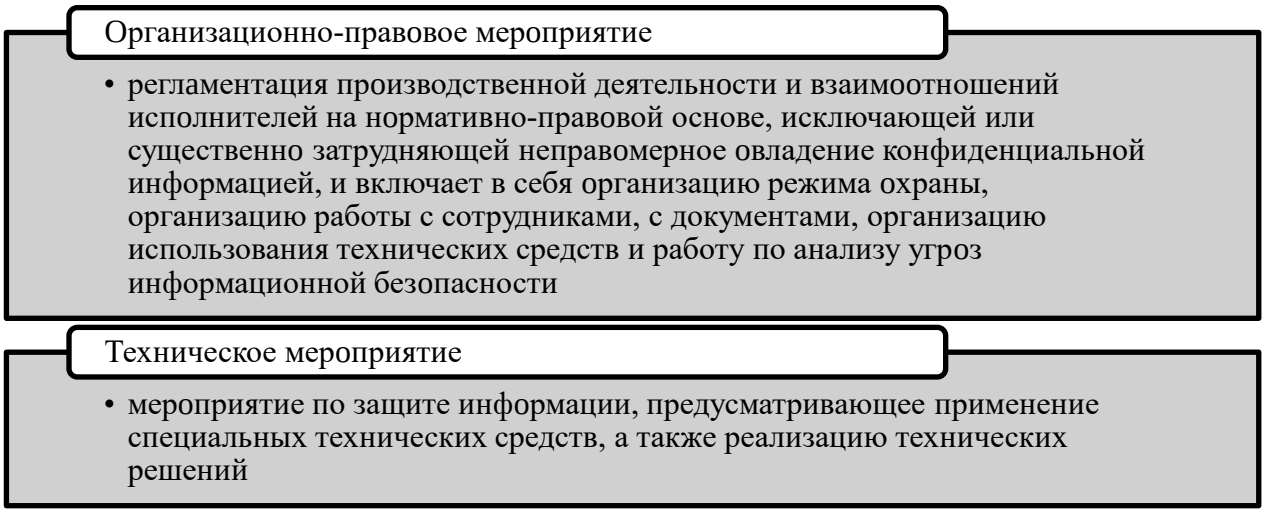


Рис. 4. Основные мероприятия по защите информации.

Развитие и широчайшее распространение информационных технологий стало, помимо прочего, одним из факторов, повлиявших на изменение концепции национальной безопасности. Так, если прежде в концептуальные рамки национальной безопасности входило сохранение территориальной целостности и суверенитета страны, а также его устойчивость перед угрозой военного вторжения, то на современном этапе информационная безопасность является одной из важнейших составляющих национальной безопасности. Это связано с широчайшим распространением цифровой составляющей в экономике, социальной жизни и других сферах человеческой деятельности в современном мире. При этом следует заметить, что информационная безопасность все больше влияет на безопасность в любой области жизни, в том числе возрастает зависимость национальной безопасности страны от информационной безопасности. Таким образом, обеспечение ИБ в настоящее время становится одной из ключевых мер и базовым элементом национальной безопасности, в связи с чем регламентация мер информационной безопасности объектов передана на федеральный уровень законодательства [Круликовский, с.194].

В общем смысле под информацией понимают сведения (сообщения, данные), независимо от формы их представления. Таким образом, одним из основных направлений обеспечения ИБ в области общественной безопасности является обеспечение защиты информации ограниченного доступа за счет повышения защищенности соответствующих информационных технологий. Принимаемые на практике меры по защите информации, реализуемые в рамках системы защиты информации (СЗИ) ИС, в зависимости от структуры ИС, вида и объемов данных, содержащихся в ИС, функционала и задач, должны быть направлены на обеспечение основных свойств информации - конфиденциальности, доступности и целостности. Угрозы безопасности информации определяются по результатам оценки возможностей нарушителей (внешних и внутренних), анализа возможных уязвимостей ИС, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности). К основным регулирующим документам в этой области относятся, в частности, следующие документы (рисунок 5).

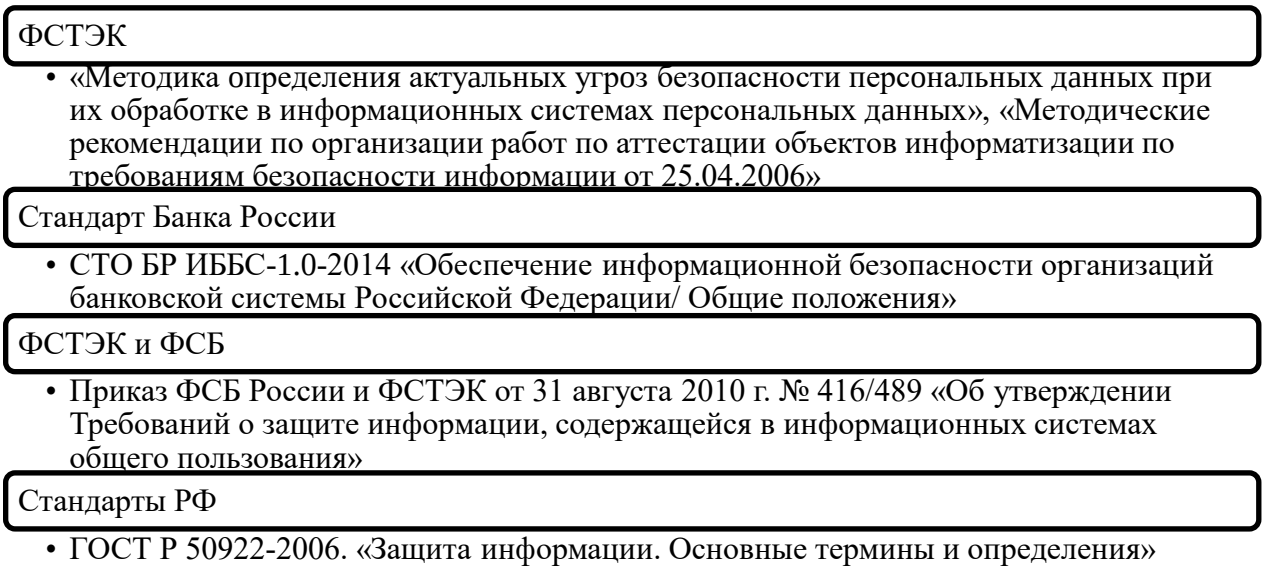


Рис. 5. Основные регулирующие документы в области защиты информации.

Следует также упомянуть в этой области РД по защите информации от НСД, утвержденные Гостехкомиссией России в 1997-1998 гг. (Нормативно-методические документы и порядок проведения работ по защите информации

при обработке ее на средствах ЭВТ (1997 г.), Сборник руководящих документов по защите информации от НСД (1998 г.)), но действующие до сих пор.

В 2006 году законодатели стали формировать нормативы по защите персональных данных. Был введен в действие Федеральный закон №152-ФЗ «О персональных данных» [22], после чего Правительством РФ и регуляторами в области защиты информации приняты основные требования к защите персональных данных (ПДн) при их обработке в ИСПДн [38] (рисунок 6).

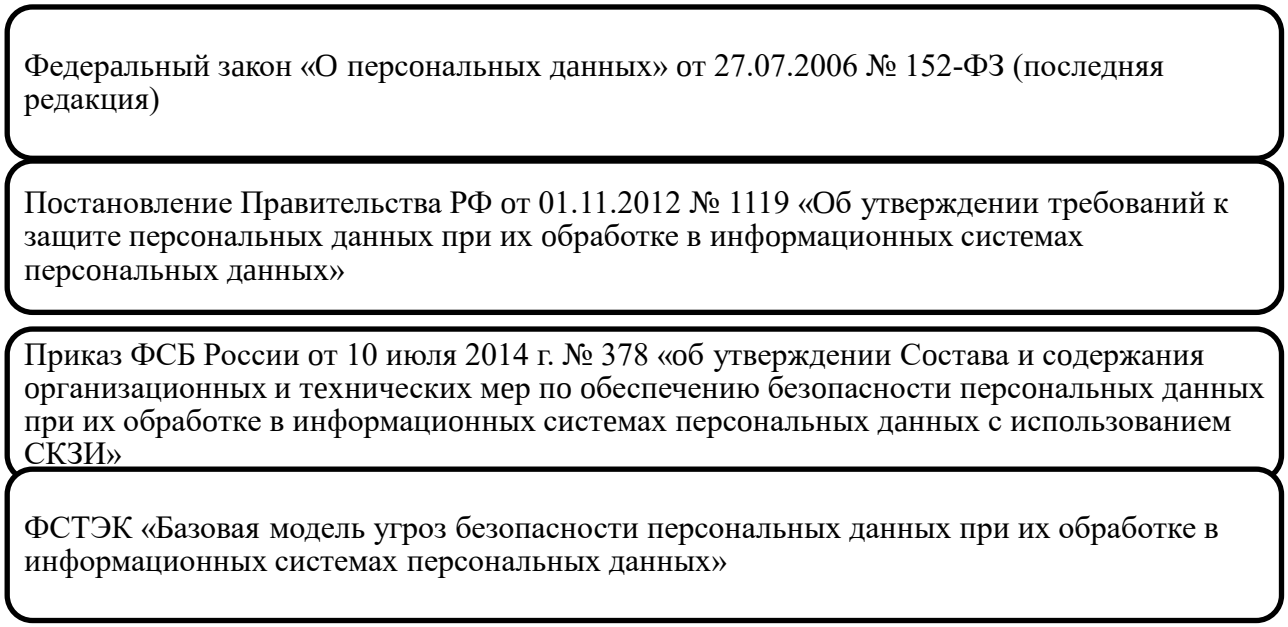


Рис. 6. Базовые регулирующие документы в области защиты персональных данных [22, 38, 40].

Законодателем установлено, что безопасность ПДн при обработке должен обеспечивать оператор, или лицо, которому оператор поручил обработку персональных данных. При этом вся ответственность за обеспечение безопасности и защиты персональных данных ложится на оператора (или лица, обрабатывающего ПДн по поручению оператора). Таким образом, указанные лица должны принимать все правовые, организационные и технические меры для обеспечения информационной безопасности при обработке ПДн в ИСПДн. Нарушение установленных требований в области защиты информации

предусматривает различные виды ответственности юридических и физических лиц, в соответствии с действующим законодательством.

Защита информации ограниченного доступа осуществляется на основании требований федеральных законов и подзаконных актов, а также других нормативно-правовых документов Российской Федерации (рисунок 7).

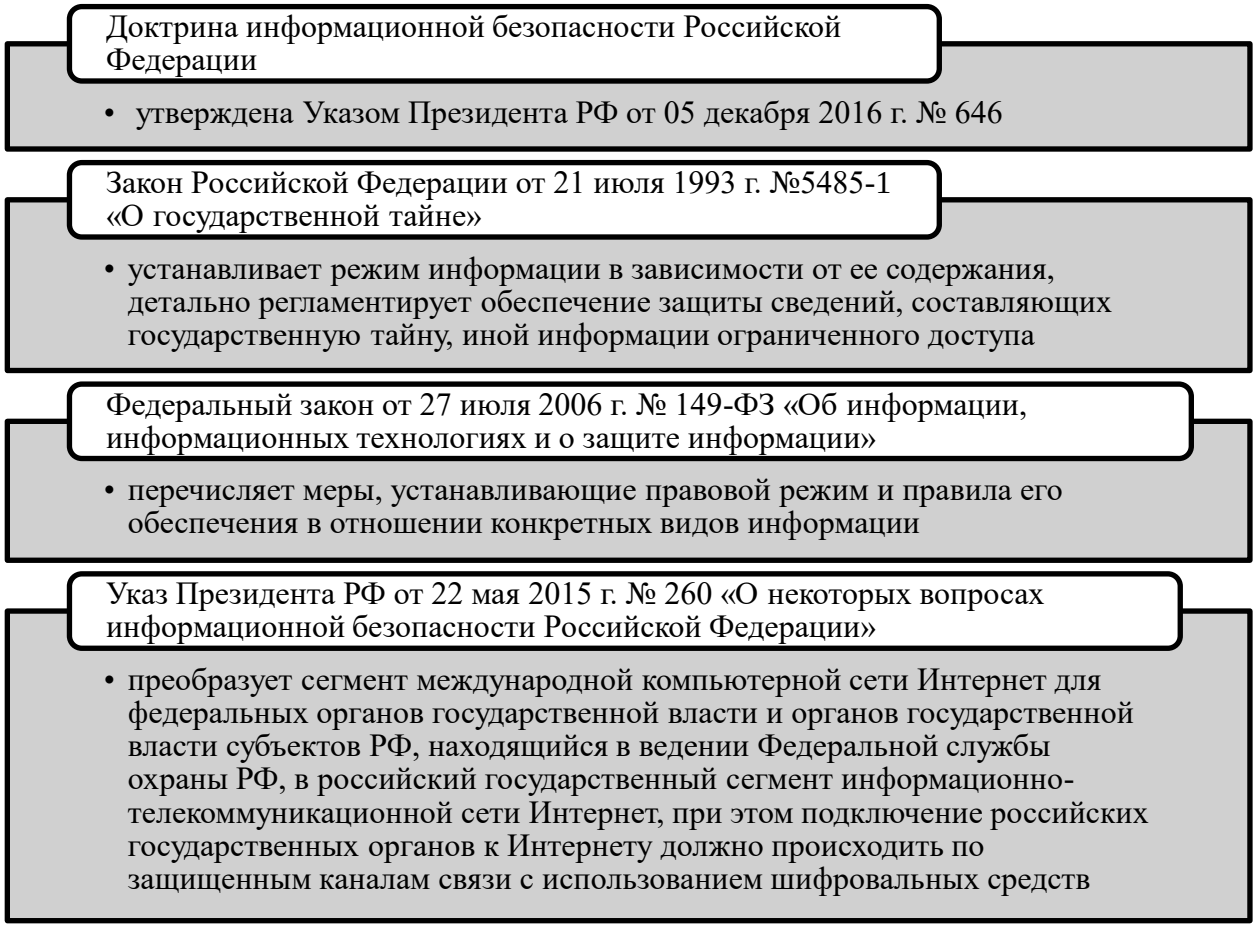


Рис. 7. Основные законодательные документы, устанавливающие и регламентирующие правила защиты информации ограниченного доступа [10, 23, 25, 37].

Основополагающим документом в этой области является Доктрина информационной безопасности Российской Федерации [25]. Прочие законодательные акты уточняют и детализируют виды информации, подлежащей защите, а также те необходимые меры, которые должны приниматься для обеспечения информационной безопасности, а также распределение ответственности и регламентацию правоотношений в этой

области. Применительно к информации, обращающейся в области государственного управления, принятие мер по ее защите возлагается на органы исполнительной власти, как на операторов государственных информационных систем (ГИС). Помимо этого, в случаях, если иные меры не могут обеспечить информационную безопасность, законодательно устанавливаются ограничения в доступе к информации, находящейся у органов исполнительной власти.

Таким образом, можно сделать следующие выводы.

Под информационной безопасностью понимается степень защищенности свойств информации, то есть конфиденциальности, целостности и доступности данных. При этом комплекс мер, обеспечивающий сохранение всех этих свойств информации, называется защитой информации. Тем не менее, существует еще и «широкая» трактовка данного понятия, при котором под информационной безопасностью понимается состояние защищенности национальных интересов страны в информационной сфере.

На современном этапе информационная безопасность является одной из важнейших составляющих национальной безопасности. Это связано с широчайшим распространением цифровой составляющей в экономике, социальной жизни и других сферах человеческой деятельности в современном мире, что делает обеспечение защиты информации одним из важнейших и актуальнейших вопросов на всех уровнях жизни не только в нашей стране, но и в мире.

В Российской Федерации принят целый ряд федеральных законов и подзаконных актов, определяющих и регламентирующих необходимые меры, которые должны приниматься для обеспечения информационной безопасности, а также регламентирующих распределение ответственности и правоотношения в этой области.

Законодательство в сфере информационной безопасности образует два блока, первый из которых включает нормы, устанавливающие правовой режим информации, права, обязанности, ответственность субъектов информационных

отношений, меры по созданию и обеспечению состояния информационной защищенности тех или иных объектов, а второй – нормы, устанавливающие требования к техническим средствам, сетям связи, условия передачи информации и т.п., что формирует их свойство обеспечивать защищенность информации и, в конечном счете, защищенность самих объектов.

1.2. ФУНКЦИИ И ПОЛНОМОЧИЯ ОРГАНОВ ВЛАСТИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Обеспечение информационной безопасности достигается разработкой и реализацией комплекса мероприятий (организационных, технических и правовых мер), направленных на поддержание состояния защищенности объектов безопасности (информации и информационной инфраструктуры), а также средств и субъектов этой деятельности.

Основными субъектами, осуществляющими деятельность по обеспечению информационной безопасности в Российской Федерации,

Президент РФ

- разрабатывает основу государственной политики в сфере информационной безопасности, определяет ключевые исполнительные органы в этой сфере (ФСБ, ФСТЭК)

Правительство РФ

- определяет концептуальную нормативную основу ключевых направлений государственной политики в сфере информационной безопасности, закрепляет правовое положение основных субъектов информационной безопасности, их права, обязанности и ответственность

Федеральная служба безопасности России (ФСБ)

- обеспечивает непосредственно сам процесс защиты значимых объектов информационной безопасности и ликвидации компьютерных атак

Федеральная служба по техническому и экспортному контролю (ФСТЭК)

- разрабатывает стратегию и основные нормативные требования в области защиты информации и обеспечения информационной безопасности

Министерство цифрового развития, связи и массовых коммуникаций (Минцифры)

- осуществляет функции по выработке государственной политики и нормативно-правовому регулированию в сфере информационных технологий (включая использование информационных технологий при формировании государственных информационных ресурсов и обеспечение доступа к ним), электросвязи и почтовой связи, массовых коммуникаций и средств массовой информации, в том числе электронных (включая развитие сети Интернет, систем телевизионного и цифрового вещания и радиовещания и новых технологий в этих областях), печати, издательской и полиграфической деятельности, обработки персональных данных

являются федеральные органы государственной власти, обладающие специальными полномочиями в указанной сфере (рисунок 8).

Рис. 8. Основные субъекты, осуществляющие деятельность по обеспечению информационной безопасности в России.

До 1993 г. в РФ все работы по защите информации были направлены, в основном, на противодействие иностранным техническим разведкам. Понятия «информация ограниченного доступа» по отношению к информации, не содержащей сведения несекретного характера, не существовало. Указанное обстоятельство было обусловлено тем, что рыночной экономики, как таковой, в современном ее понимании, просто еще не было. Поэтому, в основном, вся работа по защите информации была направлена на защиту информации, содержащей секретные сведения.

Вместе с тем, активное развитие новых технологий и не менее бурное развитие информационных технологий (ИТ) остро поставило проблему защиты информации ограниченного доступа, не содержащей секретных сведений. Поэтому под руководством Государственной технической комиссии при Президенте Российской Федерации специализированными НИИ РФ проблематика защиты информации активно развивалась, благодаря чему увидели свет ряд руководящих документов (РД ГТК), действующих и в настоящее время.

Выход указанных документов был обусловлен развитием всемирной паутины-Интернет, в связи с чем остро встал вопрос о переходе от идеологии защиты отдельных автоматизированных рабочих мест (АРМ) на основе ПК к идеологии защиты автоматизированных систем (АС) при межсетевом взаимодействии от несанкционированного доступа (НСД).

Развитие проблематики защиты информации обусловило централизацию указанных вопросов в масштабе страны, в связи с чем с 1993 г. в Российской Федерации была создана функционирующая Государственная система защиты информации (ГСЗИ). При этом основными методами по защите информации

определяются правовые, организационные, технические и экономические методы, которые должны применять в своей деятельности не только государственные организации, но и предприятия с различной формой собственности. Функции головной организации-регулятора в сфере обеспечения защиты информации в стране продолжала выполнять ГТК при Президенте РФ.

Безусловно, что создание ГСЗИ дало новый импульс в решении не только практических, но и нормативных и нормативно-методических вопросов защиты информации. Дальнейшее стремительное развитие информационно-коммуникационных технологий (ИКТ) привело к необходимости осуществления организационной перестройки руководящих органов ГТК, в соответствии с которой функции обеспечения технической защиты информации в процессе хранения, обработки и передачи были возложены на Федеральную службу технического и экспортного контроля (ФСТЭК) – регулятора проблематики в области защиты информации и ее головной организации по нормативно-методическому обеспечению в стране (Государственный научно-исследовательский испытательный институт проблем технической защиты информации (ГНИИИ ПТЗИ)).

После реорганизации ГТК при президенте РФ и появлением новых угроз в процессе межсетевого взаимодействия возникла необходимость совершенствования правовой базы, в связи с чем появился новый базовый

Федеральный закон №184 от 27 декабря 2002 г. «О техническом регулировании».
Федеральный закон от 07.07.2003 г. №126-ФЗ «О связи».
Федеральный закон от 29.07.2004г. «О коммерческой тайне»
Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»
Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных»
Федеральный закон №390 от 28 декабря 2010 г. «О безопасности».
Федеральный закон №99 от 4 мая 2011 г. ««О лицензировании отдельных видов деятельности»
Указ Президента РФ от 06 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера»
ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения. Дата введения 2008-02-01.
ГОСТ Р 51275-06. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. - М., 2006 г.

перечень документов, являющихся основополагающими при принятии решений по технической защите информации (рисунок 9).

Рис. 9. Базовый перечень документов для принятия решений о ТЗИ.

При этом существенным образом возросла и значимость ФСТЭК как регулятора деятельности по защите информации в стране.

В настоящее время в число основных субъектов, осуществляющих государственное регулирование в области информационной безопасности в России, входит Минцифры, в функции которого входит, в том числе, разработка и реализация федеральных целевых программ, государственных проектов и программ, направленных на обеспечение информационной безопасности для населения. Последней новеллой в законодательно-правовом поле по отношению к полномочиям Минцифры может стать передача этому министерству функций по обеспечению информационной безопасности детей от информации, причиняющей вред их здоровью и развитию. На данный момент этот проект находится на рассмотрении в Государственной думе.

Функции и полномочия ФСТЭК и ФСБ определяются Указами Президента РФ [35, 36]. В настоящее время функции этих органов в области информационной безопасности значительно расширились в связи с переходом на следующий этап в соответствии со Стратегией национальной безопасности и Доктриной информационной безопасности России [25].

В 2018 году вступил в силу Федеральный закон № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» [10]. Указанный Федеральный закон предусматривает создание единого центра мониторинга и управления информационной безопасностью для информационных систем, важных для национальной безопасности страны (объекты критической информационной инфраструктуры – КИИ). Под термином КИИ подразумеваются информационные системы, критически важные для обеспечения национальной безопасности страны. Подпадающие под принадлежность к КИИ информационные системы используются

государственными органами либо учреждениями в 12 областях экономики и промышленности, определенных в законе, как имеющие важнейшее значение для обеспечения нацбезопасности (ракетно-космическая промышленность, транспорт, финансовый сектор, здравоохранение, наука и т.д.).

С целью обеспечения информационной безопасности КИИ вводятся такие системы и структуры, как ГосСОПКА (государственная система обнаружения, предотвращения и ликвидации компьютерных атак) и НКЦКИ (Национальный координационный центр по компьютерным инцидентам), за создание и функционирование которых отвечает ФСБ [41, 42]. В функции ФСТЭК включается обеспечение безопасности КИИ на территории страны.

Таким образом, можно сделать следующие выводы.

Информационная безопасность государства в современном мире приобретает наивысший статус, поскольку именно она в настоящее время является залогом национальной безопасности страны. Широчайшее распространение цифровых технологий во всех областях жизнедеятельности привело к тому, что вопросы защиты информации становятся одними из важнейших и актуальнейших вопросов современности, особенно на общегосударственном уровне.

Безопасность информации, как составляющая информационной безопасности, включает в себя защиту информации и информационных ресурсов от несанкционированного доступа, искажения, уничтожения, установление режима информации в зависимости от ее содержания, обеспечение защиты сведений, составляющих государственную тайну, иной информации ограниченного доступа.

Дальнейшее развитие информационной безопасности в России в настоящее время рассматривается с точки зрения интеграции всех субъектов информационных отношений и создания единого центра мониторинга и управления информационной безопасностью для объектов критических информационных инфраструктур (КИИ).

ГЛАВА 2. РЕГУЛИРОВАНИЕ ОБОРОТА И ЗАЩИТЫ ОТДЕЛЬНЫХ ВИДОВ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМОЙ ОРГАНАМИ ГОСУДАРСТВЕННОЙ ВЛАСТИ И ОГРАНИЧЕННОЙ В ДОСТУПЕ

2.1. ИНФОРМАЦИЯ, ПРЕДНАЗНАЧЕННАЯ ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ И ГОСУДАРСТВЕННАЯ ТАЙНА

Существует много типов юридически защищенной законом информации. Однако, определенные документы представляют для государства особую важность, а другие – нет. Рассмотрим более детально, в чем же их специфика.

Действующее законодательство выделяет две общие категории информации – это общедоступная информация, находящаяся в свободном доступе и которую может использовать любой за нас, а также информация, ограниченная в доступе. Доступ к такой информации есть только у уполномоченных органов. Вторая группа информации вызывает у нас наибольший интерес, исходя из темы нашей работы.

Первоначально следует обращать внимание на категорию, к которой относится определенная информация, в зависимости от ее секретности. Современное законодательство имеет множество пробелов в регулировании вопроса отнесения информации к конкретному виду тайн. Нормативная база позволяет нам только определить порядок классификации информации, однако раздел «иные виды тайн» всё еще остается неурегулированным.

Федеральный закон №5485-1 от 21.07.1993 г. «О государственной тайне» ввел в практику применения информации, которая составляет государственную тайну, новую конструкцию – гриф секретности. Каждому документу, содержание которого составляет государственную или коммерческую тайну, теперь присваивается определённая законом степень секретности. Исходя из этого, незаконное использование информации, отмеченное грифом секретности, предопределяет степень ущерба, причиненного государству.

Так, законодательно выделяется три категории секретности, называемые «гриф секретности» - это «секретно», «совершенно секретно» и гриф «особой

важности». Если к работе с документами, отмеченными грифом «секретно» могут допускаться сотрудники, к которым предъявляются одни требования, то к «особо важным» сотрудникам требования абсолютно другие.

Существование такой категории, как «гриф секретности» позволяет систематизировать все документы, содержащие информацию, относящуюся к государственной тайне. К сотрудникам государственных структур, имеющим доступ к засекреченным документам, предъявляются определенные требования, которые устанавливаются с целью предотвращения возможного распространения информации. Например, по ФЗ «О полиции» сотрудники, имеющие доступ к категории документов «особой важности» не имеют права выезда за границу.

В настоящее время различные государственные и местные органы власти продолжают использовать государственную или официальную секретную информацию, которая все еще недостаточно регулируется.

Действующее законодательство предусматривает такое понятие как «служебная тайна». Мы можем его встретить в текстах нормативных актов, а также в установленных документах и научных статьях. Тем не менее, служебную тайну учёные относят к категории объектов, обладающих самостоятельностью.

Второй по степени важности правовой акт, регламентирующий основание и порядок отнесения информации к охраняемой государством тайне, - это ФЗ «Об информации» №149 от 27.07.2009 г. В его тексте можно встретить государственную, коммерческую, служебную тайну, а также иную. Кроме того, он содержит указание на то, что за несоблюдение порядка конфиденциальности ограниченной в доступе информации лицо подлежит юридической ответственности.

К документам, отмеченным грифом секретности, могут относиться также акты Президента и Правительства РФ. Например, текст Постановления Правительства №1233 от 03.11.1994 доступен только для работы федеральных органов исполнительной власти. Человек, обладающий правом доступа к

такому роду информации, должен изначально приниматься на работу с указанием его степени доступа к государственной тайне. Нормативные акты, регламентирующие деятельность других органов, могут содержать разъяснения относительно их доступа к текстам документов, составляющих государственную тайну.

Если органу, имеющему доступ к секретным документам, понадобится в его деятельности секретный документ другого органа или организации, то ему необходимо направить запрос на его получение.

Секретное делопроизводство ведется с особым учётом, установленным законом. Он подразумевает фиксацию каждого факта использования секретной документации с указанием фамилии и даты. Это позволяет упростить поиск источника незаконного распространения информации.

Кроме трех категорий секретной информации, которые мы уже рассмотрели, выделяют также такой гриф секретности, как «для служебного пользования». К нему относится любая информация, составляющая служебную тайну, но не относящаяся к государственной тайне. Доступ к такой категории информации предоставляется каждому сотруднику данного органа, либо организации, вне зависимости от его служебной категории.

Указ Президента РФ №188 от 06.03.1997 года утверждает перечень конфиденциальных сведений. В нем служебная тайна значится как «служебные сведения, доступ к которым ограничен органами государственной власти».

Если проанализировать практику применения неразглашаемых сведений, можно сделать вывод об отсутствии единой классификации секретных данных. Современные условия жизнедеятельности общества обозначают такие виды тайн, как:

1. Тайна частной жизни, на которую каждый человек имеет право по Конституции Российской Федерации. Любые сведения, составляющие личную жизнь человека (например, семейная тайна).

2. Коммерческая тайна, используемая в предпринимательской деятельности. Эта информация может содержать финансовые риски компаний,

политику доходов и расходов, перспективы развития компании и др. Раскрытие информации, относящейся к коммерческой, приведет к нарушению экономической безопасности и значительным убыткам субъекта предпринимательской деятельности.

3. Профессиональная тайна, которую также часто называют служебной. К ней может относиться адвокатская тайна, налоговая тайна, тайна следствия и др. Однако, в настоящее время законодатель предпринимает попытки конкретизации и разделения этих двух видов тайн.

Если говорить о разнице этих понятий, то следует обратить внимание на узкую специфику понятия «служебная тайна». Доступом к такой информации обладают только государственные и муниципальные служащие, в то время как профессиональной тайной могут пользоваться в своей деятельности любые органы.

Следует также отметить, что состав профессиональной тайны по своему объёму меньше состава служебной, в который входит нормативно-правовое обеспечение органа власти, должностные регламенты и порядок функционирования.

Однако, следует отметить существование более широкого подхода к пониманию понятия «профессиональная тайна». Многие относят к ней тайну, применяемую в любой профессии (тайна следствия, тайна исповеди, медицинская тайна). Данный подход создает барьер для самостоятельного существования профессиональной и служебной тайны.

Кроме того, некоторая категория информации вызывает дискуссии по поводу ее отнесения к разнличной категории охраняемой законом тайны. Различные органы и организации ежедневно используют личные данные человека. Содержание этих данных может служить профессиональной тайной для одних и служебной – для других. Например, судья – это государственный служащий и любая информация, используемая им в его деятельности – это служебная тайна. В то же время, частные сведения о лице могут использоваться при трудоустройстве специалистами отдела кадров коммерческих организаций.

Для данной категории лиц используемые ими сведения составляют профессиональную тайну.

Выделяется несколько видов служебной тайны. В зависимости от субъекта, использующего информацию, выделяется:

– служебная тайна государственных законодательных и исполнительных органов власти. Это информация, которая используется, прежде всего, для обеспечения интересов государства;

– служебная тайна органов дознания, предварительного следствия, а также судов, в т.ч. присяжных заседателей;

– служебная тайна, используемая в деятельности иных государственных служащих, к которой могут относиться любые конфиденциальные данные;

Кроме уже рассмотренной нами классификации служебной тайны по субъектам ее использования, выделяют также классификацию служебной тайны, в зависимости от ее объекта (налоговая тайна, тайна следствия, судебная тайна, банковская тайна и др.). Отсутствие установленной законом классификации видов служебной конфиденциальной информации позволяет трактовать эту классификацию по своему, в связи с чем ученые к служебной тайне также относят врачебную тайну.

В настоящее время человек постоянно сталкивается с необходимостью предоставления другим доступа к конфиденциальной информации. Многие даже не подозревают об отнесении той или иной информации к различным категориям секретности. Рассмотрим некоторые случаи.

1. Налоговая тайна. Каждый человек – налогоплательщик. Однако, не каждый знает о том, что информация, предоставляемая в налоговые органы, не вся относится к служебной тайне. Например, к ней относятся паспортные данные и место регистрации лица, однако приговоры суда по статьям о налоговых преступлениях, содержащие сведения о лицах, их совершивших, – это данные, которые размещаются в сети интернет для общего использования.

Налоговая тайна включает в себя несколько категорий информации, обладающей разной степенью служебной секретности. Например:

– данные об отчислениях в бюджет РФ или субъектов РФ;

– сведения о налогах и сборах физических лиц и организаций, которые являются налогоплательщиками;

– налоговые учёты и декларации;

– данные о начислениях и уплатах налогов.

2. Конфиденциальность реестра гражданских актов. К ним относится как тайна усыновления, так и любые сведения, составляющие частную информацию (акт рождения, смерти, установления отцовства и т.д.). Это та категория информации, которая вызывает множество споров при ее отнесении к определенному виду. Это информация, которая не подлежит разглашению сотрудниками органов ЗАГС, а также информация, составляющая личные конфиденциальные данные о жизни человека. Служебные данные, которыми располагают органы ЗАГС, возможно получить только по запросу правоохранительных органов, либо суда.

3. Медицинская тайна. Эта категория включает информацию о случаях использования медицинской помощи и информацию, полученную в результате. Эта информация включает: диагноз, текущее состояние здоровья, лечение назначенное врачом.(состояние здоровья человека, диагноз, назначенное лечение). Вопрос об отнесении таких данных к категории «служебная тайна» всё еще остается спорным.

Классификации служебной тайны по объектам и субъектам – наиболее применимые. Однако, существуют еще и другие. Так, служебную тайну делят на две большие категории:

1. Конфиденциальная информация, доступом к которой обладают органы государственной власти и которая используется в интересах

государства;

2. Конфиденциальная информация, не составляющая интереса для безопасности РФ, но которой располагают госслужащие в силу осуществления своих полномочий.

Однако, проводя параллель между профессиональной и служебной тайной, следует отметить позицию некоторых учёных о том, что служебная тайна доступна только органам, деятельность которых сама по себе является конфиденциальной. Это создано для того, чтобы обеспечить безопасность использования таких данных, что свидетельствует о грамотной работе органов власти. Конфиденциальной также является информация, касающаяся проведения служебных и иных проверок органов прокуратуры, МВД РФ и др.

Профессиональную тайну составляет информация, не подлежащая такой усиленной охране. В случае разглашения служебной тайны – под угрозу попадают интересы государства, а при разглашении профессиональной тайны – интересы организации, либо граждан.

На данный момент в России на уровне законодательства определены многие виды конфиденциальной информации. (рисунок 10).

I. Сведения, составляющие государственную тайну

Государственная тайна

•Закон РФ "О государственной тайне". Закон РФ "Об информации, информационных технологиях и защите информации". Уголовный кодекс РФ.

II. Сведения конфиденциального характера

Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации (СМИ) в установленных федеральными законами случаях

•Закон РФ "Об информации, информационных технологиях и защите информации". Закон РФ "О персональных данных". Уголовный кодекс РФ. Гражданский кодекс РФ. Семейный кодекс РФ. Трудовой кодекс РФ. Кодекс РФ об административных правонарушениях

Сведения, составляющие тайну следствия и судопроизводства

•Уголовно-процессуальный Кодекс РФ. Уголовный кодекс РФ. Кодекс РФ об административных правонарушениях

Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна)

•Закон РФ "О государственной гражданской службе в РФ". Уголовный кодекс РФ. Гражданский кодекс РФ. Трудовой кодекс РФ. "Перечень сведений конфиденциального характера". "Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти"

III. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами

1. Банковская тайна. 2. Тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений. 3. Сведения о мерах безопасности, применяемых в отношении судей, участников уголовного процесса, должностных лиц правоохранительных и контролирующих органов, а также их близких. 4. Тайна государственной охранной деятельности. 5. Тайна голосования. 6. Нотариальная тайна. 7. Тайна страхования. 8. Врачебная тайна. 9. Музейная тайна (сведения о музейных предметах негосударственного фонда РФ). 10. Геологическая и иная информация о недрах. 11. Редакционная и журналистская тайны. 12. Сведения, связанные с коммерческой деятельнотью. 13. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

•1. Закон РСФСР "О банках и банковской деятельности". Уголовный кодекс РФ. Гражданский кодекс РФ. 2. Закон РФ "О связи". Закон РФ "О почтовой связи". Закон РФ "О частной детективной и охранной деятельности в РФ". Уголовный Кодекс РФ. 3. Закон РФ "О государственной защите судей, должностных лиц правоохранительных и контролирующих органов". Уголовный Кодекс РФ. 4. Закон РФ "О государственной охране". Гражданский Кодекс РФ. 5. Уголовный Кодекс РФ. Кодекс РФ об административных правонарушениях. 6. Основы законодательства РФ о нотариате. Гражданский Кодекс РФ. 7. Гражданский Кодекс РФ. Закон РФ "О страховании". Закон РФ "Об индивидуальном учете в системе государственного пенсионного страхования". 8. Основы законодательства РФ об охране здоровья граждан. 9. Закон РФ "О музейном фонде РФ и музеях в РФ". 10. Закон РФ "О недрах". 11. Закон РФ "О средствах массовой информации". 12. Закон РФ "О коммерческой тайне". Уголовный Кодекс РФ. Гражданский Кодекс РФ. Трудовой кодекс РФ. 13. Патентный Закон РФ. Уголовный Кодекс РФ. Гражданский кодекс РФ. Кодекс РФ об административных правонарушениях.

Рис. 10. Основные виды конфиденциальной информации в РФ.

Остановимся подробнее на понятии «государственная тайна».

Понятие «секретные данные» предполагают выделение данной категории документации в отдельную группу и установление на нее особого режима использования.

К основным и важным принципам классификации и отнесения информации к государственной тайне относятся:

- принцип своевременности,

- принцип достоверности (обоснованности), - принцип законности.

Законность отнесения и сокрытия информации к государственной тайне основана на том, что секретная информация соответствует статьям 5 и 7 Закона РФ «О государственной тайне».

Обоснованность классификации и информации как государственной тайны заключается в определении с помощью экспертной оценки возможности классификации конкретной информации.

Режим тайны также построен на принципе своевременности. Он подразумевает получение доступа к информации только в случае его необходимости и использовании ее «здесь и сейчас». Длительное использование документа «особой важности» не допускается. Здесь еще следует учесть принцип разумного срока.

Секретные материалы закон РФ «О государственной тайне» классифицирует, опираясь на их целевой, ведомственной и отраслевой принадлежности.

Стоит отметить, что в самом законе не изложены аргументы для отнесения информации к той или иной категории. Данную задачу выполняют и применяют в своей работе, как органы, так и организации.

Отнесение сведений к государственной тайне осуществляется руководителями органов государственной власти в соответствии с «Перечнем сведений, составляющих государственную тайну», в «Перечне должностных лиц, имеющих право отнести сведения к государственной тайне».

В структуре "Перечня сведений, составляющих государственную тайну" существуют такие разделы:

- сведения в военной области;

- сведения в области экономики, науки и техники;

- сведения в области внешней политики и экономики;

- сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности.

В ранее действовавшей редакции Гражданского кодекса РФ существовала отдельная статья, регулирующая режим служебной и коммерческой тайны. Ст.139 ГК РФ (утратившая силу), устанавливала критерии каждого вида информации, позволяющие относить ее к объектам гражданских прав. В практике применения данной статьи всё чаще приходилось отождествлять понятия служебной и коммерческой тайны, что подвергалось критике со стороны многих учёных и практикующих юристов.

В настоящее время, особенно с развитием информационных технологий, всё большую актуальность набирает секрет производства (ноу-хау). В связи с этим возникает необходимость усиления правовой охраны таких разработок. Первое, что может этому способствовать, это установление режима секретности для таких объектов гражданских прав.

Использование ноу-хау в коммерческой деятельности дает серьезные преимущества компаниям, а возможность установления охраны без раскрытия технологии, в отличие от патента, приводит к тому, что коммерческие структуры все чаще используют режим коммерческой тайны.

С одной стороны, под ноу-хау понимается что-то не столь комплектное, технологичное, с другой стороны, ноу-хау - это не просто информация, идентичная коммерческой тайне. Объем сбыта ноу-хау составляет около 400 млрд долларов в год, причем около 60% этого объема - это оборот внутри транснациональных корпораций.

В современной юридической литературе достаточно работ, посвященных секрету производства (ноу-хау), однако, данная тема до сих пор остается актуальной и спорной.

Раскрывая понятие секрета производства (нау-хау), следует уделить внимание такого составляющего элемента, как коммерческая информация, относящаяся к организации деятельности какой-либо организации. В тоже время основное понятие секрета производства заключается прежде всего в сведениях, которые используются в технологическом процессе и обладают режимом защиты коммерческой тайны.

Конфиденциальность информации, составляющей секрет производства имеет большую ценность, заключающуюся в получении выгоды ее правообладателем до того времени, пока она не утратит свою конфиденциальность и не станет общеизвестной.

Исходя из определения секрета производства, приводимого в ГК РФ, можно выделить следующие характерные признаки: во-первых, неизвестность третьим лицам, во-вторых, особый правовой режим охраны конфиденциальности.

Представляя секрету производства режим охраны коммерческой тайны, законодатель тем самым устанавливает основное условие для возникновения права на ноу-хау и условий охраны данного права у правообладателя.

Характеризуя правовую охрану секрета производства, стоит отметить, что в российском законодательстве она представляется в соответствии с двумя видами правового регулирования: во-первых, законодательством о коммерческой тайне, во-вторых, законодательством о защите конкуренции, что не является взаимоисключающими. Так, например, ответственность за недобросовестную конкуренцию преследуется государством, в том случае, если будет обращение по данному поводу заинтересованного лица в соответствующий антимономольный орган, то режим охраны коммерческой тайны уже относится к обязанности правообладателя обеспечить секрету производства режим секретности коммерческой тайны.

В тоже время при наличии общих свойств в охране, коммерческая тайна и секрет производства имеют различия в правовой природе, общими у них является только такой признак, как: неизвестность иным лицам. В свою

очередь, у коммерческой тайны нет признаков собственности, т.к. она представляет собой не сам объект собственности, а лишь секретную информацию о данном объекте собственности, имеющего законного правообладателя.

Информация о новом способе производства как объект гражданского права представляет собой гражданско-правовую категорию секрета производства. [Пучков, с.135].

Право на секрет производства охраняется исходя из режима секретности, неизвестности третьим лицам, несмотря на то, что распоряжаться им вправе одновременно несколько правообладателей, имеющих на это соответствующее право.

Таким образом, секрет производства следует отличать от производственной тайны по критерию ее правового регулирования и оборотоспособности в коммерческой деятельности правообладателя секрета производства.

На основании изложенного, следует сделать вывод, что сведения, составляющие предмет секрета производства обладают конфиденциальностью и охраняются как коммерческая тайна ее правообладателя. Ценность такой информации заключается в установлении режима секретности, действующего до того времени, как с указанного ноу-хау в установленном законом порядке не будет проведено освобождение от установленного режима конфиденциальности, т.е. неизвестности третьим лицам.

Особенно это актуально сейчас, когда в современном мире и в частности, в предпринимательских отношениях разрабатываются новые технологии, внедряются различные средства и способы повышения конкурентоспособности отдельных организаций, для чего разрабатываются различные информационные ресурсы, в отношении которых организация-правообладатель ноу-хау заинтересована в установлении режима секретности. Право на секрет производства может быть более удобно в каких-то случаях, так как оно не

требует для закрепления определенных формальностей, при этом универсально, поскольку распространяется на широкий круг сведений. [72].

Таким образом, право доступа к секрету производства является юридическим выражением режима конфиденциальности, в том числе режима коммерческой тайны. Устанавливая данный режим, устанавливается и повышенная охрана конфиденциальности секрета производства, что несомненно важно в экономическом развитии. Устанавливая указанные режимы, секрету производства придается тем самым, большая значимость и повышенная правовая охрана в соответствии с нормами права.

В тоже время секрет производства и режим коммерческой тайны, несмотря на то, что оба обладают признаком неизвестности третьим лицам и защитой от разглашения, имеют отличительные черты, подчеркивающие их правовую природу как объектов интеллектуальных прав.

Следующим критерием предоставления охраны секрету производства является то, что должна иметь место конфиденциальность информации, составляющей объект охраны ноу-хау, т.е. данная информация не подлежит разглашению третьим лицам. Как уже отмечалось, в отношении секрета производства, правообладатель вправе установить режим коммерческой тайны, т.е. секретности, со всеми вытекающими из этого последствиями. В содержание режима коммерческой тайны входят различные правовые, технологические и иные меры, с помощью которых достигается обеспечение неразглашения данной информации третьим лицам, что придает секрету производства повышенную значимость в гражданском обороте. В связи с этим, лицо, которому на законных основаниях принадлежит право пользования секретом производства, наделяется также в отношении такого секрета производства исключительным правом, что представляет ему соответствующие правомочия и гарантии.

Секрет производства и коммерческая тайна могут различаться по своим целям, так секрет производства своей целью содержит коммерческую

оборотоспособность, в то время как коммерческая тайна таким свойством не обладает и не преследует такой цели.

По своей правовой природе коммерческая тайна представляет собой информацию, обладатель которой не разглашает ее третьим лицам и в связи с этим она не участвует в гражданском обороте и защищается от потери секретности правообладателем. В настоящее время единственным схожим признаком секрета производства и коммерческой тайны является признак секретности. Вместе с тем федерального закона, регулирующего вопросы служебной тайны, в отличие от многих других видов тайн (налоговой, коммерческой, врачебной и т.д.), до настоящего времени не принято.

Согласно постановлению Правительства России №1233 пункт 1.5 [29] руководители могут определять:

– круг лиц, обладающие правом сводного использования служебной информации в силу специфики своей деятельности;

– возможность осуществления обмена информацией, отмеченной грифом секретности, с другими органами;

– правовое значение отметки «Для служебного пользования», которая позволяет ограничивать круг лиц, имеющий доступ к данному виду документов;

– порядок охраны конфиденциальной информации, пресечение ее неправомерного использования;

Регулирование вышеупомянутых сфер осуществляется путём принятия специальных Федеральных законов, либо иных актов, которые определяют порядок использования каждого вида конфиденциальной информации в отдельности. В настоящее время неполноценное законодательное регулирование всех аспектов служебной тайны ставит вопрос о необходимости систематизации и дополнении существующих правовых норм, ее регулирующих. Когда рассматривался проект ФЗ № 124871-4 «О служебной тайне» [33], Комитет Государственной Думы по безопасности отметил, что отметка «Для служебного пользования» для государственных документов

должна регулироваться на уровне ФЗ и за ее разглашения должна быть установлена ответственность. (Заметка от 20.10.2011 № 202/4). Данный законопроект был отклонен. В силу части 1 статьи 17 Закона об информации, пункта 1.8 Правила обращения со служебной информацией и разглашения служебной тайны могут повлечь дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Важно отметить, что распространение тайны, находящейся под охраной законов (информации, отмеченной грифом секретности) может привести к существенным нарушениям безопасности государства. Учитывая различные обстоятельства, этому правонарушению способствующие, за разглашение государственной тайны может наступать уголовная ответственность.

Как уже отмечалось ранее, субъекты, использующие служебную информацию в своей деятельности – это органы и организации, в деятельности которых главный вид юридической ответственности за нарушение секретности – это дисциплинарная ответственность. За неправомерное использование информации, составляющей служебную тайну, лицо подлежит увольнению.

2.2. ОРГАНИЗАЦИОННО-ПРАВОВОЙ МЕХАНИЗМ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В настоящее время организационно-правовой механизм защиты конфиденциальной информации является достаточно разработанным в целом, но имеющий некоторые пробелы в отношении отдельных видов тайн.

Основную проблему завладения информацией, составляющей конфиденциальность, для владельца такой информации составляет то, что им причиняются убытки в результате того, что данная информация утрачивает признак секретности и становится доступной для третьих лиц.

В первую очередь, правообладатели информацией, составляющей тайну, будь то государственная, коммерческая, служебная и др. должны создать все необходимые условия для эффективной защиты информации, составляющей тайну от доступности третьим лицам. Рассмотрим основные методы защиты секретной информации.

Сам по себе гриф секретности – это не просто установленная законом структура. Он предполагает существование конкретных, установленных законом, реквизитов, которые наносятся на документ.

Существуют такие документы, информация в которых может относиться к разным категориям секретности. В таком случае, разные части указанного документа отмечаются соответствующими им грифами секретности, а весь документ принято относить к наивысшему по правовой охране грифу, указанному в нем.

Прежде всего, это главная цель защиты такого рода информации – это препятствование разглашению тайны, т.е. лишение возможности правонарушителям иметь доступ к охраняемой законом тайне, в результате противоправных действий которого информация, составляющая, тайну может быть похищена или уничтожена (изменена).

Следующим средством механизма защиты информации, составляющую тайну, является управление доступом, т.е. правообладателем осуществляется контроль за использованием данной информации, а также функционированием носителя информации (электронный базы данных и т.д.).

Контроль доступа имеет множество мер безопасности: распознавание пользователей, сотрудников и ресурсов системы (каждый объект имеет персональный код); аутентификация объекта или субъекта по предъявленному им идентификационному коду и др.

Еще одним средством, используемым для охраны информации, составляющую тайну, является маскировка, что представляет собой использование шифровки информации и таким образом, без использования специальной методики изменения шифра, она станет доступной только

правообладателю и ограничит доступ третьим лицам. Способ маскировки на наш взгляд представляет собой наиболее эффективный способ защиты секретной информации от притязаний третьих лиц.

Еще один способ составляет регламентирование – один из самых основных методов защиты информации и носителей информации, в результате применения которого устанавливаются специальные нормы, в связи с которыми осуществляются все действия с защищаемой информацией. Применение данного средства защиты информации минимизирует противоправный доступ к ней.

Использование в качестве средства защиты информации принуждения заключается в том, что например, в организации, где установлен режим охраны коммерческой тайны устанавливаются строгие регламенты, в соответствии с которыми работники должны осуществлять свою деятельность в целях недопущения разглашения информации, составляющей тайну.

Методом защиты информации, который побуждает пользователя и сотрудников не нарушать установленные правила, придерживаясь установленных моральных и этических стандартов называется побуждением.

[Урсул, с.125].

Согласно ст. 9 закона № 149 ФЗ определяется, что законодатель указывает на наличие информационных режимов. Это режимы:

– профессиональной тайны,
– режим служебной тайны;
– коммерческой тайны,
– государственной тайны,
– режим персональных данных.

Согласно пункту 2 статьи 3 Федерального закона от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне» [21] сведения о роли изобретения, промышленного образца, как правило, попадают под режим коммерческой тайны.

Так, В.Н. Лопатин учитывает судебную тайну и сведения предварительного следствия среди служебной тайной информации.

И напротив, К. М. Конджакулян указывает на необходимость разделения профессиональных секретов на государственные, служебные, медицинские, следственные, банковские, адвокатские и секретарские.

М.С. Братановская выделяет другие профессиональные секреты:

медицинскую, судебную защиту и представительство, признание, предварительное следствие, нотариальное действие.

Например, в соответствии со ст. 23 Конституции РФ [2] по нашему мнению, тайны по информационной передаче данных (телефон, почта) следует признавать правом каждого, а не только отдельной группы людей, занимающихся на профессиональном уровне отдельной профессиональной деятельностью. В связи с этим, она должна быть в Перечне включена в раздел, который относится к личности человека.

В настоящее время теория конституционного и административного права, впрочем и других юридических наук не достигла единства в понимании того, что же относится к видам конфиденциальной информации, в связи с чем, данный вопрос продолжает оставаться актуальным и дискуссионным.

Так, например, Коломиец полагает небезосновательно, что можно насчитать чуть менее пятидесяти различных видов секретной информации, для которых применяются различные термины. Необходимо обратить внимание на то, что применяемые термины по мнению данного автора перечисляются в различных правовых актах и не поддаются какой-либо систематизации и унификации.

Некоторыми авторами, напр., Михайловым В. считается, что все известные тайны следует соотносить на следующие виды: государственная тайна, коммерческая тайна и частная тайна, т.е. тайна, относящаяся к частной жизни человека.

Другие авторы в свою очередь дифференцируют тайны, существующие в обществе и государстве на современном этапе на следующие виды: профессиональная тайна, коммерческая тайна, банковская тайна, служебная

тайна, а также тайна персональных данных. Мы видим, что в этом перечне отсутствует государственная тайна.

Таким образом, можно предположить, что либо государственной тайне по мнению данных ученых придается отдельный правовой режим охраны, либо она, по их мнению включена в понятие профессиональной тайны, что на наш взгляд, не совсем оправдано.

Если рассматривать классификацию существующих тайн по такому критерию, как субъект, являющийся владельцем тайны на законных основаниях, то тайны можно классифицировать на следующие виды: государственная, банковская, служебная, коммерческая (владельцем которой является государство и сформированные им органы); коммерческая, налоговая, служебная, адвокатская и др (принадлежит юридическим лицам, как коммерческим, так и некоммерческим); личная, врачебная, семейная тайна и др. (принадлежит гражданам). Таким образом, классификация по данному критерию основана на классификации субъектов гражданского права.

Существуют три степени секретности информации [23]:

- Особое значение конфиденциальности;
- Совершенно секретная информация;
- Является самим способом работы с такими сведениями.

Если такую информацию расценивать как тайна, она обозначается как частная, военная и др., затрагивает отдельную сферу регулирования.

Анализируя подходы авторов к диффернцированию сведений, составляющих какую-либо тайну, стоит обратить внимание на мнение Е.К. Волчинской, которая среди всех видов тайн выделяла тайну естественную (первичную) и тайну вторичную (производную).

К первому виду она относила тайны, непосредственно связанные с владельцем данной тайны (личная, служебная, государственная и коммерческая), а ко второму виду относила тайны, которые были доверены субъекту, к которым относятся по мнению автора, профессиональные тайны.

Наиболее популярной является классификация тайн, исходя из субъектного состава, владельцам которых тайна принадлежит в соответствии с родом их профессиональной деятельности.

Что является адвокатской тайной? Под такой тайной понимаются любая информация по оказанию юридических услуг. [11].

Под банковской тайной подразумевается конфиденциальная информация о счетах и операциях клиентов. [15].

Врачебная тайна относится к информации о болезни, лечении и др. пациента. [34].

Журналистская тайна подразумевает информацию, полученную от гражданина, которую нельзя разглашать (Закон «О средствах массовой информации», статья 41).

По правому режиму коммерческой тайны, в ее основе находится целевая установка данной тайны, т.е. она представляет собой секретные от третьих лиц сведения, которые способствуют правообладателю такой информации получить какую-либо финансовую выгоду, укрепить и приумножить доходность.

На основании вышеизложенного, следует сказать, что как в законодательных актах, регулирующих охрану разных видов тайн, так и в современной доктрине существует значительное число критериев для деления тайны на виды и зачастую смешивая их. Например, один вид тайн, коммерческий может быть отнесен к разным групповым видам тайн.

На наш взгляд, в качестве основной классификации тайн, следует применять целевой критерий защиты информации, составляющей секретную информацию, потому что главным образом целевой критерий служит основанием для установления режима охраны какого-либо вида тайн.

Что касается иных критериев, то по нашему мнению, субъективный и объективный критерий деления тайн на виды может осуществлять не основную, а вспомогательную роль и разделять виды тайн, классифицированных по цели на уже различные подгруппы.

Если рассмотреть деление тайн по специальному правовому режиму, то можно выделить частную тайну, т.е. тайну о частной жизни ее правообладателя и тайну. Охраняемую публичный интерес ее правообладателя.

В первом случае в состав частной тайны включаются персональные сведения о лице и коммерческая тайна, а во втором случае, к тайне, основанной на публичном интересе, следует отнести государственную тайну, а также профессиональную тайну.

Что касается служебной тайны, касающейся также публичного интереса, то в данной классификации, на наш взгляд, ее следует считать разновидностью профессиональной тайны, на которую распространяется соответствующий режим конфиденциальности.

Таким образом, как уже было изложено выше, существует достаточно много оснований для классификации различных тайн на виды. Для обеспечения единства классификации и решения проблем в правоприменительной деятельности, следует на федеральном уровне принять закон, которым урегулировать специальные режимы информации, составляющую какой-либо вид тайны, определить содержание такой информации, порядок установления в отношении ее режима охраны тайны и условия и основания его прекращения, сроки действия режима охраны, условия допуска к данной тайне, а также виды нарушений и условия привлечения к различным видам ответственности. Перечень сведений, которые должны быть включены в новый законодательный акт не является исчерпывающим и должен максимально регулировать вопросы правового режима охраны тайн.

Государственной тайне уделяется особое внимание со стороны государства, т.к. в случае неправомерного ее распространения, под угрозу попадает безопасность как государства в целом, так и его граждан.

ФЗ «О государственной тайне» полностью раскрывает информацию о сведениях, которые составляют гос. тайну.

Важно сказать, что законодательство о конфиденциальной информации, относящейся к государственной тайне, в настоящее время довольно

несовершенно. Следует доработать еще множество неурегулированных аспектов. Например, необходимо соотнести критерии различных видов информации с грифами секретности и установить ответственность за распространение, исходя из степени важности информации для безопасности государства.

Приведем список государственной тайной информации [23]:

1. сведения в военной области (о содержании стратегических и оперативных планов, о планах строительства Вооруженных Сил РФ, о разработке, производстве, утилизации ядерных боеприпасов, о дислокации, степени готовности, защищенности режимных и особо важных объектов и т.д.);

2. сведения в области экономики, науки и техники (о содержании планов подготовки России и ее отдельных регионов к возможным военным действиям, о силах и средствах гражданской обороны, об объемах и планах государственного оборонного заказа, о достижениях науки и техники, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства, и т.д.);

3. сведения в области внешней политики и экономики (о внешнеполитической, внешнеэкономической деятельности РФ, о финансовой политике в отношении иностранных государств);

4. сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности (о силах, средствах и результатах разведывательной и оперативно-розыскной деятельности, о методах и средствах защити секретной информации, об организации и о фактическом состоянии защиты государственной тайны, о защите Государственной границы России и т.д.).

Данный список регулярно увеличивается в связи объемным понятием гос. тайны. Есть случаи в судебном праве, когда обычный гражданин мог разглашать тайную информацию, полученную из свободно доступных интернет-источников. На наш взгляд, это является недопустимым, нарушающим права данного гражданина.

На основании вышеизложенного, гражданин может быть привлечен к ответственности за разглашение сведений, составляющих государственную тайну, только в том случае, если этот гражданин понимает, что он или она раскрывает информацию, составляющую государственную тайну, а также имеет официальный доступ к зарегистрированным государственным секретам со всеми вытекающими отсюда последствиями.

К примеру, Верховный Суд РФ принял достаточно справедливую позицию, [76] о том, что приказ Министра обороны Российской Федерации от 01.01.2001 г. № 055 «Об утверждении Перечня сведений, подлежащих засекречиванию исключительно в Вооруженных Силах Российской Федерации, является засекреченным документом. При этом не относится к нормативно-правовым актам.

Суд привел довод, что спорный правовой акт не содержал модель поведения граждан с секретной информацией, устанавливал только правила определения секретности каких-либо отдельных актов и по кругу субъектов распространял свое действие исключительно на тех должностных лиц, кто во исполнении своих полномочий имел доступ к секретной информации. Таким образом, в отношении простых граждан, не являющихся должностными лицами и не имеющими доступа к информации, составляющей тайну, данный приказ не мог действовать.

Неконфиденциальная информация включает данные о ЧС, демографии, льготах, социальных гарантий и др.

Помимо этого, можно выделить отдельную группу документов, содержащих секретную информацию, но не являющихся государственной тайной, несмотря на то, что тоже ограничены в обороте. Такие документы имеют статус и гриф «Для служебного пользования» и распространяются на очерченный круг субъектов. В качестве примера можно привести справочник телефонов предприятий, входщих в состав военной промышленности.

Любое государство обеспечивает сохранность сведений, являющихся секретными для третьих лиц, в т.ч. других государств. В государстве для

обеспечения сохранности таких сведений формируются государственные органы, занимающиеся выработкой регламентов работы с информацией. Являющейся секретной и не подлежащей распространению, а также порядок доступа и требования к лицам, которые допускаются в установленном законом порядке к работе с такой информацией.

На территории Российской Федерации функционирует специальная межведомственная комиссия [28], которая занимается деятельностью служб, имеющих доступ к секретной информации.

Как уже было отмечено выше, защита сведений, являющихся для государства секретными, составляет одну из внутренних функций государства, но достаточно сложную в правовом регулировании, что соответственно вызывает трудности в правоприменении.

В целях решения проблем правоприменения, связанных с недостаточностью в правовом регулировании информации, составляющей тайну, следует внести изменения в Закон «О государственной тайне» и дать в нем список всей информации относящейся к гос. тайне и к которой может быть доступ должностных лиц. Установление данного перечня необходимо в целях исключения судебных споров в процессе использования таких сведений.

Существует множество факторов, формирующих информацию, которая относится к государственной тайне. Это сведения, касающиеся внутренней и внешней политики государства, экономической безопасности и обороноспособности.

На современном этапе развития, наибольший интерес вызывает деятельность наукоемких предприятий, большая часть которых относится к коммерческим организациям, т.е. имеют цель извлечение прибыли. Несмотря на это, к таким наукоемким организациям, пусть в своем меньшинстве, но могут относиться и общественные организации, не имеющие цели извлечения прибыли. Что касается коммерческих организациях, то для достижения своей цели извлечения прибыли, ими формируются новые партнерские отношения, расширяется рынок сбыта, заключаются новые контракты, зачастую

международные, что также может иметь правовой режим секретности от распространения третьим лицам, в результате чего может быть нанесен урон деловой репутации предприятия и его прибыльности. Также для достижения целей деятельности и создания прочных связей. Данные предприятия вкладывают немалую часть прибыли в развитие информационных технологий, а также технологических процессов, что в свою очередь также составляют коммерческую тайну.

Указанная деятельность, как уже указывалось выше, осуществляется с целью привлечения новых контрагентов, которых нужно не только привлечь и наладить с ними деловые отношения, но у удержать и упрочить с ними деловые связи, что непременно принесет свой положительный результат при дальнейшем стабильном сотрудничестве.

С развитием виртуального пространства экономика нуждается в улучшении способов ее защиты. Современные проблемы требуют современных решений. В настоящее время становится невозможно уследить за первоначальным источником информации в сети Интернет. В результате, в сеть проникает информация, которая автоматически становится общедоступной.

В целях завоевания рынка сбыта и своего потенциального покупателя, коммерческие организации, продающие товары или оказывающие услуги, должны представить на рынок сбыта не только товары, имеющие высокое качество, но и уникальные товары, т.е. такие товары, которые потребитель не сможет приобрести у другого продавца. В данном случае налицо развитие конкуренции, т.е. каждый стремиться показать товар лучшего качества, чем у конкурента, имеющий свою оригинальность и соответствующую, устраивающую потребителя цену.

Важно учитывать, что организации, занимающиеся предпринимательской деятельностью, а, в частности, продажей товаров, не заинтересованы раскрывать секреты производства своим конкурентам. Это приведет к большим убыткам, а в конечном итоге к банкротству.

Практически каждая фирма, будь ее целью продажа товаров, осуществление работ или оказание услуг, не заинтересована в раскрытии секретов своего производства. Таким образом, необходимо применение режима конфиденциальной информации.

Кроме того, к такой информации следует относить еще экономическое состояние той или иной фирмы. Полное движение денежных средств, распределение и соотношение доходов и расходов, ежемесячная прибыль, спонсорство и т.д. В настоящее время, важную роль приобретает правовая охрана секрета производства (ноу-хау), которая тоже составляет коммерческую тайну. Тем не менее, невозможно деятельность всех фирм сделать абсолютно секретной, так не представится возможным осуществлять их взаимодействие между собой.

Эта информация включает учредительные документы организации и данные в государственных архивах; факторы окружающей среды, негативно влияющие на безопасную работу объектов производства. А также безопасность всего населения.

Закон устанавливает определенные категории допуска сотрудников к информации, в зависимости от ее грифа секретности. Деятельность таких сотрудников подразумевает возможность использования информации только в служебной деятельности. Они несут ответственность (в том числе уголовную) за незаконное ее распространение. Перечень документов, содержание которых охраняется законом, должен быть зафиксирован во внутреннем приказе организации, имеющей доступ к конфиденциальной информации.

На самом тексте документа, содержащего государственную тайну, стоит отметка «секретно», либо «особо секретно», в зависимости от ее содержания. Каждый сотрудник имеет разную степень доступа к таким документам. Это осуществляется с целью защиты охраняемой законом информации от неправомерного использования.

Гриф секретности подразумевает не только невозможность распространения информации в ее первоначальном виде, но также

устанавливает запрет на копирование и использование отдельных ее фрагментов. В организациях, имеющих доступ к конфиденциальной информации, обязательно ведение журналов сотрудников, обладающих доступом к ней с указанием степени доступа.

Очень сложно доказать когда, кем и где произошло распространение государственной тайны, т.к. в силу ее специфики мы, к сожалению, сможем только увидеть результат ее незаконного использования, выражающийся в подрыве безопасности экономики, обороны, либо иных сфер деятельности государства.

Регулирование семейных правоотношений отражены в конституции РФ [2] и семейной кодексе РФ [7].

В рамки семейной тайны включаются следующие категории:

- тайна, связанная с усыновлением;

- тайна, связанная с частной жизнью самих супругов;

- отношения, складывающиеся из личных имущественных и личных неимущественных связей между супругами.

В качестве предмета семейной тайны могут быть рассмотрены следующие сведения:

- сведения о жизни лица;

- факты о состоянии физического здоровья лица;

- информация о его благосостоянии;

- сведения о том, какие занятия предпочитает лицо и какие поступки оно совершает;

- факты о том, каких убеждений и взглядов придерживается лицо при совершении поступков;

- информация о том, какие отношения складываются между членами семьи и с другими лицами, которые таковыми не являются. [Карапетян, с.34].

Если сравнивать понятие личной и семейной тайны, то можно сказать, что они имеют много общих характеристик и признаков, что позволяет их отождествлять друг с другом в некоторых случаях. Но имеются и определенные

различия, которые заключаются в том, что личная тайна присуще одному лицу, а семейная тайна касается нескольких лиц, которые выступают членами одной семьи и регулируются семейным законодательством РФ.

Одной из самых распространенных семейных и одновременно личных тайн является тайна усыновления, которая обычно обеспечивается, установленными законодательством, способами охраны и защиты.

Если тайна завещания была нарушена, то завещатель может выступить с требованием о компенсации морального вреда, а также использовать другие методы защиты прав населения.

Банковская тайна представляет собой одну из основополагающих элементов особых отношений, складывающихся между кредитными организациями и их клиентами, а равно между кредитными организациями и лицами, желающими получить какие-либо сведения. Банковская тайна может быть определена нормами права, которые устанавливают:

1) совокупность прав и обязанностей, которые устанавливаются для участников отношений, образовавшихся в теме использования, предоставления и охраны сведений, которыми обладает организация, предоставляющая кредиты и оказывающая иные услуги;

2) сущность сведений, на которые может быть распространен рассматриваемый режим защиты;

3) обстоятельства и порядок предоставления и применения сведений, которыми обладает организация, предоставляющая кредиты и оказывающая иные услуги;

4) порядок осуществления правовой защиты сведений, которыми владеет указанная организация, вбирая в себя так же основания ответственности за разглашение указанных сведений.[76].

В любой кредитной организации все сотрудники обязаны сохранять конфиденциальность операций, счетов и депозитов своих клиентов и корреспондентов, а также другой информации, созданной кредитной организацией, если это не противоречит положениям федерального закона. [44].

В случае разглашения такой информации кредитные организации Банка России, аудиторские и иные организации, а также их должностные лица и сотрудники несут предусмотренную законодательством юридическую ответственность, в том числе возмещение причиненного ущерба.

Правовое определение понятие «налоговая тайна» закреплено в п. 1 ст. 102 Налогового кодекса РФ [6], согласно которому под ней следует понимать информацию любого типа, которая касается налогоплательщика РФ, полученные налоговым органом, органами внутренних дел, органом государственного внебюджетного фонда и таможенным органом

В случае обращения лица за получением медицинской помощи и в случае её оказания, пациент обладает правом на врачебную тайну.

Итак, под врачебной тайной понимают следующее:

- информация о лице, находящимся на лечении, а также полученная медицинским персоналом от такого лица в процессе осуществления лечения и не которая не может быть оглашена в рамках общества;

- информация о лице, которое находится на лечении, но которую нельзя сообщать данному лицу из определенных соображений. [Бурмемейстер, с.15].

Врачебную тайну составляют также:

- сведения о самом обращении лица за медицинской помощью;

- сведения о физическом и психическом здоровье лица;

- сведения о том, какой диагноз был поставлен лицу;

- другая информация, которая может быть получена при осуществлении обследования или лечения лица. [Бурмемейстер, с.20].

Закон запрещает разглашение информации, составляющей медицинскую тайну, лицам, которые узнали об этом в ходе обучения, профессиональных, служебных и других обязанностей, за исключением случаев, прямо предусмотренных законом.

Законом разрешается передача информации, которая образует врачебную тайну другим лицам только с согласия самого пациента.

Законодатель определяет группу случаев, когда допускается передача информации, составляющую врачебную тайну, без получения согласия гражданина или его законного представителя.

Можно перечислить следующие такие случаи:

1) если само лицо, в отношении которого были произведены мероприятия по обследованию и лечению, не может в силу своего состояния здоровья выразить свою волю по данному вопросу;

2) если существует опасность того, что будет распространено инфекционное заболевание, приведет к массовому отравлению и поражению большого количества граждан;

3) если поступил запрос по данным сведениям от органов по судебным разбирательствам;

4) если медицинская помощь оказывается лицу, которому еще не исполнилось пятнадцать лет, а оповещение родителей или его законных представителей в этом случае обязательно;

5) если у медицинского персонала имеется информация о том, что вред здоровью лица был причинен в результате совершения противоправного поступка.

Данный список не подлежит расширительному толкованию. [46].

Итак, рассмотрев различные виды личных и семейных тайн можно сказать о том, что данные категории выступают в качестве объектов гражданских правоотношений. При этом, можно заметить и то, что в любых гражданских правоотношениях можно выделить элементы указанных тайн. Если даже взять заключение договора купли-продажи определенного предмета. В договоре обязательно должны быть зафиксированы персональные данные как продавца, так и покупателя. Персональные данные же выступают одним из составляющих категорий личной тайны гражданина.

Действительно, каждый день человек вступает в различные гражданские правоотношения, в рамках которых осуществляется возникновение элементов личной и семейной тайны.

2.3. РЕГУЛИРОВАНИЕ ИНФОРМАЦИИ, ОГРАНИЧЕННОЙ В ДОСТУПЕ В СИЛУ ЕЕ ПОТЕНЦИАЛЬНОЙ ОПАСНОСТИ ДЛЯ ОБЩЕСТВА

Введение в оборот конструкции «гриф секретности» произошло с целью дальнейшего предупреждения распространения такой информации, разглашение которой может поставить под угрозу безопасность государства в целом, либо его граждан.

Некоторые учёные, говоря об ограничениях распространения секретной информации, употребляют понятие «цензура». Отождествление этих понятий - ошибочно. В настоящее время Конституция РФ устанавливает запрет на введение цензуры, однако следует помнить о существовании ограничений на распространение секретных документов и понимать, что это не одно и то же.

Действующая Конституция РФ устанавливает возможность ограничения прав и свобод человека [2]. Свобода и права человека могут ограничиваться

только Федеральным законом и только с целью защиты основ конституционного строя, а также обеспечения безопасности государства и его граждан.

Нам следует рассматривать только ту часть данной статьи, которая касается ограничением права человека на информацию и ее распространение. Какая именно информация представляет угрозу безопасности государства в случае ее разглашения?

Действующее законодательство не дает нам ответ на этот вопрос.

Частичная легализация понятия «вредная информация» произошла в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию». Из него следует, что детям распространение конфиденциальной информации может нанести существенный вред.

В Федеральном законе «Об информации, информационных технологиях и о защите информации» нет понятия «вредная информация». Взамен этого, используется определение «информация, а используется термин «информация, распространение которой ограничивается или запрещается» [14]. Стоит отметить, что в данном законе нет информации о причинах и цели таких запретов.

В Законе об информации отсутствует общий перечень видов вредной информации. Так, вся информация, на распространение которой установлен запрет, делится на две большие группы: 1) информация, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, и 2) иная информация, за распространение которой предусмотрена уголовная или административная ответственность (ч. 6 ст. 10).

В настоящее время СМИ очень сильно влияют на общественное мнение.

Гарантируется свобода средств массовой информации и запрещена цензура. [23].

Однако получение информации может привести к созданию идеалов или норм поведения, которые позволяют людям влиять на умы людей и манипулировать их публичным поведением через СМИ. Таким образом, в дополнение к правам и свободам СМИ, закрепленным в Конституции, та же

статья 29 запрещает «разжигание ненависти и вражды» со стороны СМИ на основе социальной, расовой, национальной или религиозной ненависти.

Под запретом находится пропаганда социального, расового, национального, религиозного или языкового превосходства.

Кроме Конституции РФ, порядок ограничения прав и свобод человека, а в частности права на конфиденциальность, установлен в статье 10 «Конвенции о защите прав человека и основных свобод».

Там содержится указание на то, что человек имеет полную свободу на получение информации и на ее дальнейшее распространение, однако конкретизируется, что содержание информации, полученной человеком, может налагать на него определенные обязанности и ограничения.

Распространение информации, которую принято относить к охраняемой законом тайне, может привести к нарушению общепризнанных принципов и норм права, поставить под угрозу национальную безопасность страны, либо подорвать репутацию человека.

Также существует запрет на экстремистскую информацию путем СМИ. [12]. В статье 11 данного закона определяется ответственность СМИ за «распространение экстремистских материалов и осуществление экстремистской деятельности» до тех пор, пока они не прекратят свое существование. Ответственность за использование СМИ для разжигания ненависти и вражды также определяется административным и уголовным законодательством Российской Федерации.

Согласно Кодексу об административных нарушениях есть штрафы и конфискация такого рода материалов (статьи 20.3, 20.29).

Также ответственность за использование СМИ с целью развития войны, вражды закреплена в уголовном законодательстве [9]. Наказывается также штрафами либо лишение свободы, либо принудительные работы с лишением права на определенные должности.

В целом анализ законодательства РФ показал, что в целях исполнения требований ч. 2 ст. 29, ч. 3 ст. 55 Конституции РФ, а также п. 2 ст. 10

Европейской Конвенции о защите прав человека и основных свобод (ратифицирована РФ в 1998 году) в части установления ограничения свободы слова, приняты ряд законодательных актов устанавливающих определенные запреты на распространение информации в средствах массовой информации, направленные на обеспечение «защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства», а также ответственность за нарушение данных запретов. [Туманская, № 9].

Напомним, что в апреле 2018 года Таганский районный суд Москвы вынес решение о блокировке Telegram. Роскомнадзор требовал передать ключи ФСБ для дешифровки переписки пользователей. При этом юристы Telegram уведомили Роскомнадзор, что предоставить ключи технически невозможно. Роскомнадзор приступил к масштабным блокировкам IP-адресов (такие блокировки получили название «ковровых»), которые, возможно, использует Telegram для обхода блокировок.

Ведомство отдало указание о блокировке почти 20 миллионов IP-адресов, многие из которых принадлежат международным интернет-компаниям, таким как Google, Amazo№ и Microsoft. В разных городах России прошла «акция в поддержку свободного Интернета». Жители России запускали бумажные самолетики – символ Telegram· [Танимов, Кудашкин].

«Роскомсвобода» и Центр цифровых прав стали пионерами в области защиты прав интернет-пользователей. Эксперты проводят ежемесячные мониторинги и составляют индекс свободы Интернета, запускают онлайн-кампании. К защите прав подключаются юристы и правозащитники, например, правозащитная организация «Агора» тоже отстаивает права пользователей. «Гражданское общество начинает понимать: зарождается новый сектор прав человека, который нуждается в поддержке. Уже в ООН обсуждаются права на анонимность и шифрование», – отметил Артем Козлюк.

Как отмечает Екатерина Абашина «Блокировки в той форме, в которой они осуществляются сейчас, нарушают права пользователей на свободный

доступ к информации, потому что фактически российские блокировки выходят за пределы ограничений свободы распространения и получения информации, допустимых по закону». [Танимов, Кудашкин].

С экспертом согласилась юрист Центра защиты прав СМИ Светлана Кузеванова. Она отметила: «Любые ограничения права на свободу слова и свободу распространения информации должны соответствовать установленным законом ограничениям, которые налагаются, например, в интересах национальной безопасности, территориальной целостности или общественного порядка, для охраны здоровья и нравственности, защиты репутации или прав других лиц, а также для защиты иных значимых интересов». Она также озвучила, что Конституция РФ дает полную свободу искать и озвучивать информацию (статья 29).

Именно поэтому любые ограничения, налагаемые на деятельность интернет-ресурсов, по мнению Светланы Кузевановой, должны быть соразмерны и пропорциональны допущенному с помощью этого ресурса нарушению. «Если и производится ограничение доступа к информации в Интернете, то оно должно быть точечным, поскольку «ковровое» блокирование ресурса (по IP-адресу) лишает аудиторию права на доступ ко всему контенту ресурса самой разнообразной тематики. С учетом того, что необоснованное блокирование ресурса неизбежно влечет нарушение прав граждан на доступ к информации, ограничение права распространять информацию допускается в исключительных случаях, а процедура ограничения каждый раз должна проходить тщательный тест на соразмерность и необходимость» (Светлана Кузеванова).

Напротив, заместитель председателя Законодательного собрания Санкт-Петербурга, член фракции «Единая Россия» Сергей Соловьев уверен, что блокировки ни в коем случае не нарушают права граждан на доступ к информации. «Блокировки нужны для того, чтобы пресечь терроризм, экстремизм, активность движений религиозного толка. Для оперативности решения этих вопросов такие решения власти оправданы. Да и нормальным

людям нечего скрывать в переписках в социальных сетях. А тех, кто использует интернет-каналы для террористической деятельности, правоохранительные органы должны отслеживать», – отметил С.Соловьев.

Не существует такого законодательного акта, принятие которого смогло бы полностью решить проблему охраны прав и свобод человека в сети интернет. Интернет по-прежнему остается предметом множества споров и правонарушений. Действующее законодательство не успевает адаптироваться под развитие современных технологий, поэтому множество аспектов по распространению информации в сети интернет так и остаются неурегулированными.

Особую роль в защите прав и свобод человека в сфере информации в сети интернет играет Федеральный Закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации». [14]. Он содержит различные критерии информации, которые позволяют разделить ее на несколько групп:

1. Информация, запрет на которую устанавливается решениями государственных органов (рецепты наркотических и психотропных веществ, порнографические материалы и т.д.);

2. Информация, которая находится под защитой авторских и смежных прав (произведения науки, литературы, искусства, полезные модели, аудио, видео произведения и т.д.);

3. Информация, распространение которой составляет диспозиции статей уголовного кодекса (призывы к убийству или самоубийству, совершение террористических и экстремистских действий и т.д.);

4. Информация, которая составляет судебную тайну. Данная категория не ограничивается законом «Об информации, информационных технологиях и о защите информации», т.к. сфера ее деятельности довольно широкая. Следует учитывать существование баз данных, а также руководствоваться ФЗ №4791-1 «О статусе судей в РФ». Распространение

данной информации ставит под угрозу порядок осуществления правосудия на территории РФ.

Факты распространения информации в сети интернет обладают рядом специфических признаков, например, наличием дополнительных субъектов ответственности. За нарушение законодательства в сфере защиты информации, к ответственности в рамках сети интернет могут привлекаться также лица, которые являются организаторами распространения незаконно полученной информации.

Национальное законодательство нашей страны по вопросам распространения информации – несовершенно. Развитие современных технологий позволяет правонарушителям изобретать более сложные способы распространения секретной информации, законодательство не успевает обеспечить полную охрану. Рассмотрим особенности регулирования сферы информации в других странах. Такие страны как Германия и США, например, делают акцент на защите авторских и смежных прав, а также на борьбу с терроризмом, предпочитая не вмешиваться в информационный поток.

Граждане имеют полное право распоряжаться информацией, полученной законным путём.

Полной свободе Соединенных Штатов следует противопоставить жесткую охрану информации в Китае. «Золотой щит» данной страны – это комплекс радикальных мер, направленных на борьбу с распространением информации, особенно - секретной. Китай устанавливает цензуру, а также фильтр информации, полученной через сеть интернет. Китай установил запрет на пользование некоторыми мессенджерами и социальными сетями (WhatsApp, Viber, Youtube, Telegram). Кроме того, под запретом многие зарубежные новостные сайты.

Действующее законодательство РФ не устанавливает строгих запретов на получение и распространение информации, выбирая американскую модель поведения. Мы стараемся устанавливать ограничения путём принятия дополнительных Федеральных законов, а также по решениям Суда. Главная

цель неразглашения информации – это защита прав и свобод человека и гражданина.

Несмотря на то, что режим использование информации предоставляет гражданам полную свободу в ее получении и использовании, Закон Яровой пошел вразрез данному принципу. Он предоставил правоохранительным органам возможность блокировать сайты, содержащие запрещенный контент, без решения суда. Это установило серьезный контроль за пользователями в сети интернет, созданием сайтов. Кроме того, под контроль попали даже операторы связи, т.к. появилась возможность отслеживать телефонные переговоры. За последнее время применение данного закона привело к закрытию множества сайтов, что способствовало возникновению множества жалоб и судебных споров, в которых обсуждался критерий обоснованности данного решения.

По мнению органов власти, интернет платформы могут привести к массовым беспорядкам. Например, под такое ограничение попал популярный среди молодёжи мессенджер – Телеграмм.

В первую очередь необходимо усовершенствовать действующее законодательство, установив комплекс мер, направленных на пресечение распространения охраняемой информации. Я считаю, что Закон «Об информации, информационных технологиях и защите информации» нужно дополнить такими определениями: модерация, премодерация, фильтрация, модератор веб-сайта. А также необходимо создание законодательной возможности для органов исполнительной власти Российской Федерации для обеспечения соблюдения своих требований на крупных веб-сайтах. выполнение модерации, премодерации или фильтрации информации, опубликованной или отображаемой в поиске. Поиск, который имеет большую аудиторию и пользователей, относящихся к определенной группе риска.

Каждому создателю сайта в интернете следует устанавливать цензуру страниц, исходя из его целевой аудитории. Нужно устанавливать возможность просмотра информации, но не ее написание. Блокировка сайта – крайняя мера.

Необходимо предпринимать попытки по улучшению функционирования интернет-систем с целью отсутствия дальнейшего преследования сайта.

Следует отметить, что человеку необходимо 2 минуты, чтобы найти любую интересующую его информацию в сети Интернет. Правоохранительные органы не успевают блокировать запрещенные для несовершеннолетних детей сайты, т.к. их огромное количество. Существенный минус в том, что практически невозможно отследить создателя сайта и источника распространения информации.

Кроме того, следует установить множество ограничений на пользование информацией в сети интернет. Например, сайты, доступ на которые разрешен только по достижении 18 летнего возраста, не проверяют фактический возраст человека, посещающего сайт с экрана компьютера. Содержание некоторого интернет-контента может оказать неблагоприятное влияние на психику ребенка.

Каждый день в сети Интернет создается множество сайтов. Правоохранительные органы, в рамках защиты сферы информации, должны привлекать больше ресурсов, чтобы успевать за постоянным обновлением системы, ибо на смену заблокированным сайтам ежесекундно приходят новые.

Это очень сложно.

Государство устанавливает общий перечень форм защиты нарушенных прав, который также распространяется и на сферу информации.

Под формой защиты понимается комплекс внутренне согласованных организационных мероприятий по защите субъективных прав и охраняемых законом интересов. Различают две основные формы защиты – юрисдикционную и неюрисдикционную. [Грудцын, с.99].

Юрисдикционная форма выделяет специальный и общий порядок по защите прав, которые были нарушены. В судебном порядке происходит защита всех прав, которые были нарушены.

Специальный порядок защиты гражданских прав и охраняемых законом интересов, в соответствии со ст. 11 ГК РФ [76], следует признавать

административный порядок их защиты. Он применяется в виде исключения из общего правила, т.е. только в прямо указанных в законе случаях.

В соответствие с законодательством применяется смешанный, т.е. административно-судебный порядок защиты нарушенных гражданских прав. В этом случае потерпевший, прежде чем предъявить иск в суд, должен обратиться с жалобой в государственный орган управления.

Неюрисдикционная форма защиты охватывает собой действия гражданин организаций по защите гражданских прав и охраняемых законом интересов, которые совершаются ими самостоятельно, без обращения за помощью к государственным и иным компетентным органам. [Грудцын, с. 100].

Самозащита гражданских прав: защита прав разрешена в такой форме, когда жертва имеет возможность юридически влиять на преступника без обращения в судебные или другие правоохранительные органы.

В рамках этой формы защиты правообладатель нарушенного или оспариваемого права может использовать различные средства самозащиты, которые должны быть соразмерны нарушению и не могут выходить за рамки того, что необходимо для его преодоления. [3].

Самозащита подразумевает возможность осуществлять охрану своих прав любыми не запрещенными способами. Это базовый механизм защиты своих прав.

Он обеспечивает свободу защитных действий в условиях нарушения прав человека на информацию и не только.

Комплекс способов, позволяющих осуществить защиту своих прав самостоятельно, либо обратиться в уполномоченные органы является механизмом защиты свободы и права каждого гражданина.

Конституция РФ устанавливает ограниченный круг способов защиты своих прав и свобод (международно-правовая защита, конституционная, судебная, административная и самозащита своих прав)..

Первые два механизма схожи между собой по реализации, отличия состоят лишь в том, что первый осуществляется конституционными судами, а второй – всеми остальными судебными органами.

Сущность данного механизма заключается в том, что лицо обращается в судебные органы с заявлением или жалобой в том порядке, который установлен законодателем.

Международно-правовой механизм защиты прав и свобод человека предполагает его обращение в международные органы, которые действуют и функционируют в рассматриваемой деятельности, но только в том случае, если все меры внутригосударственной защиты были использованы.

Главный фактор, который позволяет ограничивать право на неприкосновенность частной жизни – это личная инициатива лица, чье право подлежит ограничению. [Кибальник, с.49]. Очень сложно сформулировать в законе право на ограничение частной жизни так, чтобы оно не противоречило Конституции РФ.

Таким образом, меры и способы защиты прав и свобод, независимо от их содержания, является первоочередной функцией государства, которое реализуют её посредством использования определенного механизма, в котором принимают участие различные органы государственной власти и их должностные лица.

Совершенствование действующего законодательства ставит необходимость установления определенных обязанностей в сфере информации для крупных интернет сайтов. Следует установить блокировку поиска информации, которая охраняется законом, а также контроль за интернет публикациями. Ответственность за распространение секретной информации следует установить как для пользователя-распространителя, так и для модератора сайта.

ГЛАВА 3. ЗАЩИТА ИНФОРМАЦИИ, ОГРАНИЧЕННОЙ В ДОСТУПЕ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ ЯМАЛО-НЕНЕЦКОГО АВТОНОМНОГО ОКРУГА

3.1. МЕРОПРИЯТИЯ И ИНСТРУМЕНТЫ ЗАЩИТЫ ИНФОРМАЦИИ, ОГРАНИЧЕННОЙ В ДОСТУПЕ В ОРГАНИЗАЦИЯХ

Ограниченная в доступе информация любого вида обладает обоснованием, в том числе и нормативным, для непосредственной защиты прав и законных интересов субъектов права на тайну.

Каждый вид информации с ограниченным доступом имеет нормативное определение с целью защиты прав и законных интересов субъектов права на тайну.

Правовую основу защиты информации, ограниченной в доступе в деятельности органов государственной власти Ямало-Ненецкого автономного округа ооставляют Конституция Российской Федерации, Указ Президента Российской Федерации от 12 мая 2009 года № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года», Указ Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Рооссийской Федерации от 09 сентября 2000 года № Пр-1895, Федеральный закон от 28 декабря 2010 года № 390-ФЗ «О безопасности», Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 27 июля 2006 года № 152-ФЗ «о персональных данных», Федеральный закон от 10 января 2002 года № 1-ФЗ «об электронной цифровой подписи», Федеральный закон от 06 апреля 2011 года № 63-ФЗ «об электронной подписи» и иные правовые акты.

Отношения, связанные с защитой ин формации, ограниченной в доступе в деятельности органов государственной власти Ямало-Ненецкого автономного округа регулируются Федеральным законом № 8- ФЗ от 09.02.2009 «Об обеспечении доступа к ин формации о деятельности государственных органов и органов местного самоуправления» (далее Федеральный за кон № 8-ФЗ).

В реестре государственных полномочий, такого региона как Ямал, за всеми государственными структурами – органами власти закреплено полномочие по обеспечению в пределах своей компетенции режима секретности и защиты сведений, составляющих государственную тайну, и иной охраняемой законом тайны. Нормативным обоснованием обозначенной выше функции являются Концепция технической защиты информации региона и Положение о системе технической защиты информации, содержащей сведения, составляющие государственную тайну в округе. Данные документы утверждены под грифом для служебного пользования.

Кроме того, непосредственно в самих органах закреплены ответственные сотрудники, а в многочисленных структурах и целые подразделения, по информационной защите.

Правительством региона утвержден Сводный перечень служебной информации ограниченного доступа (постановление Правительства ЯНАО от 31.05.2017 года № 513-П). Специальный орган или сотрудник в региональных

органах власти, ответственный за информационную безопасность ограниченного доступа, на основании вышеупомянутого Перечня, разрабатывает свой местный перечень сведений служебной информации ограниченного доступа, который утверждается в установленном порядке.

В автономном округе расположены два центра обработки данных Правительства округа, на которых размещены около 200 веб-ресурсов, среди них – государственные информационные системы, сайты органов власти, местного самоуправления и муниципальных учреждений. Самый уязвимый компонент сетевого периметра организаций – это веб-ресурсы: несанкционированный доступ злоумышленников к приложению возможен на

39% сайтов, а угроза утечки важных данных присутствует в 68% веб-приложений.

Меры по защите служебной информации ограниченного доступа, которая реализуется (хранится, обрабатывается и используется) на объектах информатизации региональных государственных органов, также осуществляют специальные подразделения или наиболее подготовленные специалисты, назначаемые нормативным правовым актом в пределах компетенции. А также к этой области могут привлекаться определенные организации, имеющие допуск и лицензии на право проведения соответствующих работ, соответственно на договорной основе.

Во исполнение требований соответствующего постановления непосредственное руководит мероприятиями по защите ограниченной информации в государственных органах Ямала руководитель, либо назначенный приказом соответствующего органа власти заместитель руководителя органа государственной власти.

Как во многих государственных органах и властных структурах Российской Федерации, основные угрозы характерные для документов конфиденциального типа в органах исполнительной власти ЯНАО зависят как от технических моментов, так и от человеческого фактора.

Для предотвращения технических факторов применяются программно-аппаратные средства защиты информации, также используется метод построения инженерно-технической системы защиты информации. В тоже время, обязательно нужно отслеживать состояние оборудования и контролировать соответствующие исполняемые программы. В чем недостаток обозначенного метода – это постоянное совершенствование злоумышленников, в связи с чем программно-аппаратные системы и механизмы не всегда могут справиться с новыми угрозами и требуют постоянной актуализации.

В любом виде деятельности, в том числе и в информационной безопасности человеческий фактор особенно значим. Здесь, в целях предотвращения негативных последствий, необходимо проведение

действительно качественных инструктажей и своевременного обучения специалистов по информационной безопасности, назначение ответственных, из числа наиболее подготовленных, за работу с документами, информацией ограниченного доступа. Минусы данного метода - быстрое развитие социальной инженерии, а также пренебрежение людей элементарными правилами и техникой безопасности при информационной защите. В данном случае эффективным средством будет являться ужесточение наказания за проступки в этой области.

Каковы же основные принципы защиты ограниченной информации, в том числе и в органах власти Ямало-Ненецкого автономного округа.

1. Совершенствование руководящих документов для четкого регулирования сферы информационной защиты. Правительством региона периодически (раз в 2 года) актуализируется Концепция технической защиты информации Ямало-Ненецкого автономного округа.

2. В целях безопасности документов властные структуры определяют круг ответственных должностей и перечень лиц, допускаемых и имеющих доступ к информации ограниченного доступа. Данные мероприятия закрепляются соответствующими правовыми актами, приказами.

3. Определение перечня сведений, подлежащих защите. Положение о системе технической защиты информации, содержащей сведения, составляющие государственную тайну в Ямало-Ненецком автономном округе, совершенствуется по мере поступления соответствующих признаков.

4. Систематизация информационной безопасности для защиты документов ограниченной в доступе. Служебное делопроизводство систематически совершенствуется, в том числе путем внесения актуальных изменений в соответствующие инструкции.

5. Применение и использование программно-аппаратных сил и средств для защиты носителей информации. Следует понимать, что здесь органы власти Ямало-Ненецкого автономного округа исполняют общую для

всех функцию по созданию информационных систем в установленной сфере деятельности.

6. Ну и соответственно непосредственная профилактическая работа с сотрудниками в целях информационной безопасности (инструктажи, правила техники безопасности и т.д.).

В процессе служебной деятельности, для обеспечения защищенности служебной информации, информации ограниченного доступа в стадии использования и обработки ее на автоматизированном рабочем месте государственного органа региона, непосредственный исполнитель обязан осуществить стирание остаточной информации на несъемных носителях (жестких дисках) и в оперативной памяти посредством перезагрузки. Также устройства отображения и вывода информации (дисплей, принтер и т.д.) должны устанавливаться с учетом исключения несанкционированного доступа к выводимой информации посторонних лиц, не имеющих к ней непосредственного отношения.

Должностные лица органа государственной власти Ямальского региона при обработке служебной информации ограниченного доступа руководствуются требованиями Инструкции о порядке обращения со служебной информацией ограниченного доступа в исполнительных органах государственной власти, а также разработанными непосредственно в органе власти внутренними документами:

- Положением по организации и проведению работ по защите служебной информации ограниченного доступа в органе государственной власти;

- Инструкцией пользователя по эксплуатации технических и программных средств защиты конфиденциальной информации в органе государственной власти.

Кроме того, организационные (организационно-юридические) меры, подготовка организационно-распорядительной документации по вопросам защиты информации: инструкции, регламенты, приказы, методические указания, преследуют цель – упорядочивание процессов и соответствие

требованиям внутреннего и внешнего регулирования (так называемый «комплаенс», «бумажная безопасность»).

В связи с тем, что исполнительные органы государственной власти автономного округа осуществляют полномочия в различных сферах государственного управления, перечень необходимых документов может меняться в зависимости от специфики объектов информатизации, на которых планируется обрабатывать защищаемую информацию. Изначально определяются объекты, подлежащие защите, устанавливаются ответственные лица за организацию защиты информации, определяется степень угрозы безопасности защищаемой информации и готовится техническое задание на создание защищённого объекта информатизации и т.д.

Организационная структура обеспечения информационной безопасности в органах власти Ямало-Ненецкого автономного округа выглядит так – директора департаментов, служб региона и их подразделения по защите информации (штатные специалисты по защите информации); руководители и подразделения по защите информации организаций и предприятий, подведомственные этим департаментам и службам, выполняющих работы со сведениями, составляющими тайну страны и (или) допущенных к работе с информационными ресурсами округа (входят в структуру системы по согласованию). Подразделения по технической защите информации (штатные и нештатные специалисты по защите информации) организаций, имеющих ключевые системы информационной инфраструктуры (автоматизированные системы, участвующие в управлении экологически опасными объектами, а также комплексами жизнеобеспечения региона).

3.2. СОВОКУПНОСТЬ СРЕДСТВ И СИСТЕМА МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ ЯМАЛО-НЕНЕЦКОГО АВТОНОМНОГО ОКРУГА

Защита информации считается важной составной частью основной деятельности региональных органов власти, которая достигается посредством проведения комплекса правовых, организационных, технических, а также

методических мероприятий, которые направлены на предотвращение, нейтрализацию угроз безопасности информации в зависимости от условий деятельности и решаемых задач по обеспечению безопасности информации.

Проведение приведенного комплекса мероприятий по защите информации базируется на определении:

1. угроз безопасности информации на определенных объектах информатизации;
2. перечней объектов защиты и сведений, которые защищаются;
3. средств, а также методов защиты информации.

Цели защиты информации на территории северного региона можно увидеть на рисунке 12.

Рис. 12. Цели защиты информации в ЯНАО.

Главными задачами защиты информации на территории Ямало-Ненецкого автономного округа считаются:

1. проведение единой государственной политики по защите информации;

2. создание и организация работы органов по защите информации;

3. определение и учет информационных ресурсов, систем и средств формирования, передачи, хранения, обработки и распространения данных, подлежащей защите;

4. исключение либо большое затруднение добывания информации средствами технической разведки посредством предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию для того, чтобы ее уничтожить, исказить и блокировать;

5. подготовка предложений по совершенствованию правового, нормативного, методического, научно-технического и организационного обеспечения защиты информации на объектах Ямало-Ненецкого автономного округа;

6. проведение анализа состояния и прогнозирование источников угроз безопасности информации;

7. введение в областные государственные программы мероприятий по защите информационных ресурсов и средств информатизации;

8. выявление ключевых проблем и определение приоритетных направлений развития системы защиты информации на территории региона;

9. проведение практических мероприятий по формированию и развитию системы защиты информации на территории округа;

10. методическое и информационное обеспечение работ по защите информации;

11. контроль и проведение анализа состояния защиты информации в органах государственной власти;

12. совершенствование и развитие системы подготовки специалистов по защите информации.

Главные объекты обеспечения защиты информации на территории Ямала показаны на рисунке 11.

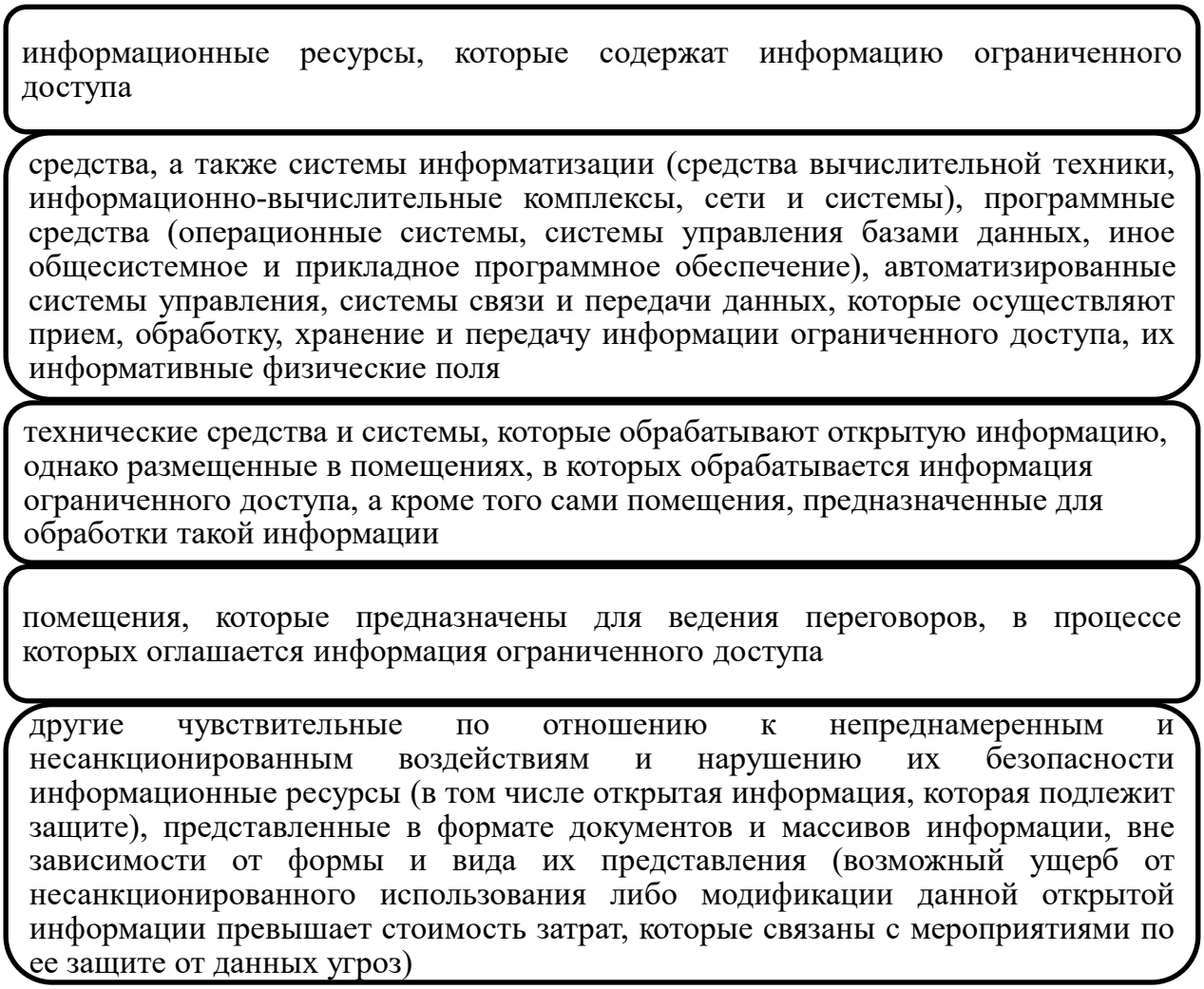


Рис. 11. Объекты обеспечения защиты информации на территории ЯНАО.

Некорректное моделирование угроз следует отнести к одной из главных проблем защиты информации государственной власти Ямало-Ненецкого автономного округа, потому что упущение из рассмотрения того либо другого фактора может привести к осуществлению угроз безопасности, которые могут привести к ухудшению всех финансово-экономических показателей работы государственной власти вплоть до прекращения ее деятельности.

Еще одной проблемой является приобретение готовых продуктов, а также решений, с низкой стоимостью, которые не прошли установленные процедуры сертификации уполномоченных органов, не соответствуют требуемым

качествам, которые предъявляются к данным системам, и не включают в поставляемый пакет технической поддержки. Не совершенствующиеся системы, которые уже есть, снижают качество их работы и степень надежности.

Итак, проблемы с которыми сталкиваются государственные органы власти при организации защиты информации, такие:

1. большой объем информации различных категорий, которая поступает в обработку;
2. большой объем нормативных документов, которые подлежат к доработке в рамках формировании системы защиты информации;
3. низкая степень автоматизации процессов обработки информации из-за не развитой информационной инфраструктуры.
4. недостаточное финансирование расходов, которые связаны с технической защитой государственных информационных систем.

Кроме того, проблемой в сфере информационной безопасности в государственных органах региона, как и в федеральных органах власти, является отсутствие закрепленного на законодательном уровне нормативного акта о служебной тайне. Предложение по пути решения данного вопроса – это разработка на региональном уровне и инициирование в думе Ямала закона о служебной тайне, что не противоречит законодательству Российской Федерации.

Еще, необходимо отметить, что при анализе деятельности информационной безопасности на Ямале, выявлена такая проблема как отсутствие единого подхода именно к обеспечению защиты информации ограниченного доступа. Дело в том, что органы государственной власти строят эту защиту на своем уровне, как говорится «кто во что горазд», хотя руководящие документы в этой сфере разработаны и действуют. Решение – определение регионального органа власти уполномоченного координировать работу в сфере информационной защиты.

В данный момент на рынке средств защиты информации существует множество различных решений по защите информации, создано огромное

многообразие таких средств, выбрать одно из которых довольно сложно. Но требования регуляторов, таких как ФСТЭК или ФСБ, заставляют госорганы использовать лишь ограниченный круг СЗИ. В связи с этим не всегда учитывается специфика региона.

Совершенствование способов и средств технической разведки, повышение опасности угроз несанкционированного доступа к информации и специальных воздействий на нее в системах и средствах информатизации и связи которые происходят с течением времени изменения условий и приоритетов защиты объектов обусловливают надобность развития системы защиты информации на территории региона.

Ямальские властные структуры используют аппаратные и технические средства защиты информации. Программные средства защиты информации создаются в результате разработки специального программного обеспечения, которое бы не позволяло постороннему человеку, незнакомому с этим видом защиты, получать информацию из системы. К основным программным средствам защиты информации, которые используются, относятся:

- программы идентификации и аутентификации пользователей компьютерных систем;

- программы разграничения доступа пользователей к ресурсам компьютерных систем;

- программы шифрования информации;

- программы защиты информационных ресурсов.

Программные средства включают в себя:

- парольный доступ-задание полномочий пользователя;

- блокировка экрана и клавиатуры, например с помощью комбинации клавиш в утилите Diskreet из пакета Norton Utilites;

- использование средств парольной защиты BIOS на сам BIOS и на ПК в целом и т.д.

В технических средствах защиты информации используются электронные и электронно-механические устройства, включаемые в состав технических

средств компьютерных систем и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к техническим, а не к инженерно-техническим средствам защиты является обязательное включение в состав технических средств компьютерных систем. К основным техническим средствам защиты информации относятся:

- устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т.п.);
- устройства для шифрования информации;
- устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы).

Также есть и вспомогательные технические средства защиты информации;

- устройства уничтожения информации на магнитных носителях;
- устройства сигнализации о попытках несанкционированных действий пользователей компьютерных систем и др.

Совершенствование деятельности по защите информации в органах власти ЯНАО должна предполагать собой оптимизацию совокупной системы защиты информации, что даст возможность ввести и использовать методы и средства защиты информации, защищенные информационные ресурсы, с помощью которых повысится мощность информационной безопасности органов государственной власти Ямало-Ненецкого автономного округа.

Также надо усовершенствовать организационные мероприятия по защите информации, которые основаны на сокращении затрат на создание совокупной системы защиты информации, повышении уровня защищенности, который обеспечивает ГСЗИ, выборе лучшего оптимального решения по формированию комплексной системы защиты информации.

Необходимо отметить, что совокупность средств и система мероприятий по защите информации в органах государственной власти регионального уровня максимально отражена в Концепции информационной безопасности,

утвержденной Правительством ЯНАО от 24 ноября 2011 года № 847-П. Уполномоченным органом власти, ответственным за обеспечение информационной безопасности в государственных органах Ямала является департамент информационных технологий и связи. Этот департамент является центральным органом, проводящим государственную политику и осуществляющим исполнительно-распорядительную деятельность в сфере цифрового развития, информационных технологий, в том числе в области использования информационных технологий при формировании государственных информационных ресурсов и обеспечения доступа к ним.

Кроме того, в вышеуказанной концепции в сфере обеспечения информационной безопасности, кроме общих положений, четко прописаны:

- цели и задачи обеспечения информационной безопасности;

- объекты информационной безопасности;

- основные угрозы информационной безопасности;

- основные направления деятельности по обеспечению информационной безопасности;

- принципы формирования системы информационной безопасности;

- структура подразделений, обеспечивающих ин формационную безопасность в органах власти автономного округа;

- модель взаимодействия участников информационной системы;

- меры, методы и средства обеспечения безопасности информационных систем;

- по рядок организации работ при разработке и эксплуатации информационных систем и системы обеспечения информационной безопасности;

- порядок управления системой обеспечения информационной безопасности;

- и контроль состояния информационной безопасности.

Технические средства привлекают все большее внимание специалистов не только потому, что их легче защитить от повреждений и других случайных

или злоумышленных воздействий, но еще и потому, что техническая реализация функций выше по быстродействию, чем программная, а стоимость их неуклонно снижается.

В заключении рассмотрения вопроса по защите информации ограниченной в доступе в органах власти Ямало-Ненецкого автономного округа хотелось бы заметить, что на основе проделанного мной анализа современного состояния, целей, задач и ключевых проблем обеспечения информационной безопасности, а также очевидно объектов, угроз информационной безопасности, методов и средств предотвращения, нейтрализации угроз информационной безопасности, а также специфики и особенностей обеспечения информационной безопасности в различных сферах деятельности государственных органов региона необходимо, на мой взгляд, кроме прочих, две основные меры. Это обеспечение единого понимания всеми участниками процесса информатизации автономного округа проблем информационной безопасности и разработка единых подходов к построению программно-технических систем защиты объектов информатизации автономного округа.

Еще одним из немаловажных аспектов, хочу отметить, что аттестацию автоматизированных рабочих мест во властных органах Ямала осуществляют так называемые «сторонние» организации. В связи с чем, в целях экономии бюджетных средств, одним из предложений является создание специализированного государственного учреждения подведомственного органу власти, которая в дальнейшем смогла получить лицензию по технической защите конфиденцильной информации и обслуживать государственные структуры в установленном порядке абсолютно бесплатно.

Комплексная система информационной безопасности округа должна в полной мере обеспечивать безопасное использование информационных ресурсов автономного округа и получение информационных услуг.

ЗАКЛЮЧЕНИЕ

При рассмотрении тайны личной жизни, принято рассматривать конкретные её виды (семейная тайна; тайна завещания; банковская тайна и другие).

Особенностью их всех является то, что они получили свое закрепление в нормах права, что позволяет применять к ним конкретные способы и меры защиты. Так, законодатель устанавливает определенный механизм осуществления правозащитных мер, в котором используются не только нормы закона, но и принимают активное участие органы государственной власти.

Проведенный анализ норм правовых актов, дает возможность сделать вывод, что в настоящее время вопрос о защите личных сведений гражданина является наиболее актуальным, так как информационные технологии достигли высокого уровня развития, что приводит к частым нарушениям указанных прав лица. Следовательно, необходимо приводить законодательство РФ в строгое соответствие с уровнем развития общественных отношений.

С моей точки зрения заслуживает особого внимания вопрос, касающийся возможности правового и обоснованного ограничения представленных правомочий и строго определять обстоятельства, которые будут выступать причиной нарушения данных свобод. Можно предложить некоторые усовершенствования законодательства, а конкретно:

- четко прописать случаи, когда ограничение таких прав будет рассматриваться как правомерное и обоснованное;
- объяснить порядок производства такого ограничения;
- расписать порядок восстановления права при необоснованном ограничении;
- определить ответственность должностных лиц за необоснованное ограничение и нарушение указанных правомочий;
- и в конце концов, необходимо на федеральном уровне выделить и узаконить такое понятие как «служебная тайна», хотя бы и с разбивкой по

видам существующих тайн. Ведь я не нашел ни в одном источнике понятие «служебная информация».

Важно иметь ввиду, что основным условием ограничения или нарушения данных прав является факт того, что это необходимо в силу законодательных требований в силу обеспечения прав и свобод иных лиц, что данная свобода лица противоречит законодательным положениям.

Информация, которая причиняет вред, в настоящее время, имеет существенное значение, так как её воздействие настолько велико, что возникают многие ситуации, свидетельствующие об её влиянии и имеющие негативный характер.

По итогам исследования можно сказать, информация, которая причиняет вред передается различными способами и может принимать различную форму. Она может содержаться в обычных средствах массовой информации, таких, как газеты, журналы, телевидение, телефоны, сеть Интернет. Но, в настоящий момент, появляются новые формы и способы передачи указанных сведений. Поэтому можно говорить, что информация может быть в письменной, наглядной и электронной форме.

Юридическая ответственность представляет собой определенную меру негативных последствий для того субъекта, который нарушил положения закона. В рамках общественных отношений, связанных с распространением информации, которая причиняет вред, также устанавливается юридическая ответственность, которая, главным образом, представлена административной ответственностью. Судебная практика указывает на большое количество дел, связанных с указанной проблематикой, что свидетельствует о необходимости разработки новейших способов борьбы с такой информацией.

В настоящий момент времени для того чтобы решить задачи информационной безопасности необходимо объединить в систему, в комплекс, на базе существующих актуальных норм и правил, действующего законодательства все имеющиеся формы, методы и способы информационной защиты, то есть принять значительные меры организационного характера.

Стремление руководителя, и это вполне объяснимое стремление, создать, развивать и поддерживать на актуальной, необходимой ступени действенную систему информационной защиты, именно такую, которая может и должна разбираться в каждом конкретном случае, с учетом специфики деятельности, и определять наиболее эффективные силы и средства, мероприятия и способы решения задач по защите информации.

Вместе с тем, организаторские способности руководителя предприятия имеют огромное значение, играют важную роль в достижении основных целей деятельности этого самого предприятия. Для выбора управленческого решения нужно, пожалуй, системно опираться на нормативно-методические документы, наработанные опытом предприятия, в нашем случае, в области информационной безопасности. И вот тогда решение руководителя будет эффективным.

Организационно-правовые формы и многообразность полномочий, осуществляемых в различных сферах государственными органами в решении задач и исполнении функций, призывает регулярного повышения качества системы защиты информации, совершенствования соответствующего законодательства на всех уровнях управления, актуализации инструкций и руководств для сотрудников и работников органов власти.

Сконцентрировать, систематизировать до конца имеющийся материал по информационной защите, найти все векторы защиты информации, поставить в самый подходящий момент приоритеты в необходимости использования сил и средств, способов, приемов и методов информационной защиты – главнейшая цель организационной составляющей всего механизма, системы защиты информации.

Отталкиваясь от того, что информационная безопасность стоит на первом месте в системе государственной безопасности, создание, а также проведение единой государственной политики в данной области требует первостепенного рассмотрения.

Выполненные в работе исследования, а также разработанные теоретические положения дают возможность найти решение научной проблеме, которая имеет важное значение, введение которой вносит большой вклад в развитие защиты информации, ограниченной в доступе, в органах государственной власти Российской Федерации. В рамках решения данной проблемы предложены методы защиты информации, которые отличаются тем, что позволят использовать новые методы защиты, тем самым увеличивая мощность всей системы безопасности.

Выполненные в работе научные исследования представлены такими результатами как -

1. выявлены проблемы, которые основаны на некорректном моделировании угроз и приобретении дешевых продуктов, что снижало безопасность информационной системы;
2. предложен подход к обеспечению защиты информации, который использует комплексную систему безопасности округа
3. предложен критерий, который обеспечит единое понимание всеми участниками процесса информатизации автономного округа проблем информационной безопасности и разработка единых подходов к построению программно-технических систем защиты объектов информатизации автономного округа.
4. проведен анализ работы информационной безопасности округа, который показал, что защита информации считается важной составной частью основной деятельности органов государственной власти Ямало-Ненецкого автономного округа.

Для эффективной защиты информации в региональных структурах власти предлагаю следующие рекомендации, которые на мой взгляд позволят усовершенствовать систему информационной безопасности властных органов региона:

- централизовать полномочия по защите информации ограниченного доступа в едином органе власти для всех региональных государственных структур в целях проведения единой политики в данной сфере;

- актуализировать региональную концепцию информационной защиты с учетом требований сегодняшнего дня, в целях практической реализации государственных функций по информационной безопасности (разложить досконально по полочкам);

- центральному органу власти по информационной безопасности разработать детальные методические рекомендации именно для руководителей департаментов и служб округа (практическая значимость заключается в том, что зачастую руководители не понимают, чем занимаются специалисты по ИБ);

- в случае закрепления информационных специалистов в каждом органе власти ЯНАО, запретить возлагать на них иные обязанности кроме полномочий по защите информации;

- установить квалификационные требования при приеме на работу специалистов указанной сферы – высшее образование в сфере информационной безопасности, технической защите информации);

- регулярная переподготовка, повышение квалификации специалистов в рассматриваемой сфере деятельности

Ну и нельзя не сказать о финансовой составляющей для бюджета региона, я уже упоминал об этом ранее. В целях экономии бюджетных средств, а так же оптимизации деятельности в сфере ИБ, рекомендация по созданию собственного регионального подразделения (соответственно получившего в дальнейшем лицензию ФСБ и ФСТЭК), подведомственного властным органам, которое будет проводить аттестацию рабочих мест во всех органах власти ЯНАО (конечно же на безвозмездной основе) без привлечения сторонних организаций.

Практическая значимость результатов будет подтверждена их применением в органах государственной власти округа.

Практическую ценность представляют: методы совершенствования, программные продукты для проведения анализа, а также синтеза систем защиты информации.

Представленные в работе подходы и предложения к защите информации считаются перспективными для осуществления параметров информационной безопасности. Особое внимание представляет развитие исследований и разработок, которые могли бы быть применены в целях защиты информации в органах государственной власти.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативно-правовые акты

1. «Конвенция о защите прав человека и основных свобод» (Заключена в г. Риме 04.11.1950) (с изм. от 13.05.2004) (вместе с «Протоколом [№ 1]» (Подписан в г. Париже 20.03.1952), «Протоколом № 4 об обеспечении некоторых прав и свобод помимо тех, которые уже включены в Конвенцию и первый Протокол к ней» (Подписан в г. Страсбурге 16.09.1963), «Протоколом № 7» (Подписан в г. Страсбурге 22.11.1984)) // «Собрание законодательства РФ», 08.01.2001, № 2, ст. 163

2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 14.03.2020 № 1-ФКЗ // Российская газета. – 04.07.2020. – № 144.

3. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 31.01.2016)// «Российская газета», № 238-239, 08.12.1994.

4. Гражданский кодекс Российской Федерации (часть третья) от 26.11.2001 № 146-ФЗ (ред. от 03.07.2016) (с изм. и доп., вступ. в силу с 01.09.2016)// «Российская газета», № 233, 28.11.2001.

5. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ (ред. от 03.07.2019) (с изм. и доп., вступ. в силу с 14.07.2019) // «Российская газета», № 256, 31.12.2001

6. Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ (ред. от 28.12.2016)// «Российская газета», № 148-149, 06.08.1998.

7. Семейный кодекс Российской Федерации от 29.12.1995 № 223-ФЗ (ред. от 30.12.2015)// «Российская газета», № 17, 27.01.1996.

8. «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ (ред. от 01.04.2019) // «Российская газета», № 256, 31.12.2001

9. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 17.06.2019) (с изм. и доп., вступ. в силу с 01.07.2019) // «Собрание законодательства РФ», 17.06.1996, № 25, ст. 2954

10. Федеральный закон № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» (в ред. от 13.07.2015) // Собрание законодательства РФ. 31.07.2006. № 31 (1 ч.). Ст. 3448; 20.07.2015. № 29 (часть I). Ст. 4390.

11. Федеральный закон от 31.05.2002 № 63-ФЗ (ред. от 29.07.2017) «Об адвокатской деятельности и адвокатуре в Российской Федерации» // «Российская газета», № 100, 05.06.2002

12. Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 23.11.2015) «О противодействии экстремистской деятельности» // «Собрание законодательства РФ», 29.07.2002, № 30, ст. 3031

13. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 01.05.2019) «О защите детей от информации, причиняющей вред их здоровью и развитию» // «Российская газета», № 297, 31.12.2010

14. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации» // «Российская газета», № 165, 29.07.2006

15. Федеральный закон от 02.12.1990 № 395-1 (ред. от 06.06.2019) «О банках и банковской деятельности» // «Собрание законодательства РФ», 05.02.1996, № 6, ст. 492

16. Федеральный закон № 147-ФЗ от 17 августа 1995 года «О естественных монополиях» (в ред. от 05.10.2015) // Собрание законодательства РФ. 21.08.1995. № 34. Ст. 3426; 12.10.2015. № 41 (часть I). Ст. 5629.

17. Федеральный закон от 26.07.2006 г. № 135-ФЗ «О защите конкуренции» (ред. от 05.10.2015) // Собрание законодательства РФ. 31.07.2006. № 31 (1 ч.). Ст. 3434; 12.10.2015. № 41 (часть I). Ст. 5629.

18. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ, 31.07.2017, № 31 (Часть I), ст. 4736 // Российская газета, № 167, 31.07.2017.

19. Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ, 31.07.2017, № 31 (Часть I), ст. 4743 // Российская газета, № 167, 31.07.2017.

20. Федеральный закон «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» от 20.08.2004 № 119-ФЗ // Собрание законодательства РФ, 23.08.2004, № 34, ст. 3534// Российская газета, № 182, 25.08.2004.

21. Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 18.04.2018) «О коммерческой тайне» //«Российская газет», № 166, 05.08.2004

22. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017) «О персональных данных» // Российская газета, № 165, 29.07.2006

23. Закон РФ от 21.07.1993 № 5485-1 (ред. от 29.07.2018) «О государственной тайне» // Собрание законодательства РФ, 13.10.1997, № 41, стр. 8220-8235

24. Указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера» // Собрание законодательства РФ, 10.03.1997, № 10, ст. 1127// Российская газета, № 51, 14.03.1997.

25. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ, 12.12.2016, № 50, ст. 7074.

26. Указ Президента РФ от 30.11.1995 № 1203 (ред. от 14.01.2019) «Об утверждении Перечня сведений, отнесенных к государственной тайне» //

Собрание законодательства РФ, 04.12.1995, № 49, ст. 4775// Российская газета, № 246, 27.12.1995.

27. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 05.12.2016 г. № 646. – [Электронный ресурс] – Режим доступа. –URL: http://kremli№.ru/acts/ba№k/41460 (дата обращения: 18.07.19).

28. Указ Президента РФ от 06.05.2011 № 590 (ред. от 25.07.2014) «Вопросы Совета Безопасности Российской Федерации» (вместе с «Положением о Совете Безопасности Российской Федерации», «Положением об аппарате Совета Безопасности Российской Федерации», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по безопасности в экономической и социальной сфере», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по военной безопасности», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по общественной безопасности», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по п... // «Собрание законодательства РФ», 09.05.2011, № 19, ст. 2721.

29. Постановление Правительства РФ от 03.11.1994 № 1233 (ред. от 18.03.2016) «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» // Собрание законодательства РФ, 25.07.2005, № 30 (ч. II), ст. 3165.

30. Постановление Правительства РФ от 26.06.1995 г. № 608 «О сертификации средств защиты информации» (ред. от 21.04.2010) // Собрание законодательства РФ. 1995. № 27. Ст. 2579; 2010. № 18. Ст. 2238.

31. Распоряжение Правительства РФ от 08.12.2011 № 2227-р (ред. от 18.10.2018) «Об утверждении Стратегии инновационного развития Российской

Федерации на период до 2020 года» // Собрание законодательства РФ, 02.01.2012, № 1, ст. 216.

32. Приказ ФСТЭК России от 10.04.2015 г. № 33 «Об утверждении Правил выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации, иной информации ограниченного доступа и продукции (работ, услуг), сведения о которой составляют государственную тайну, в установленной ФСТЭК России сфере деятельности» // Бюллетень нормативных актов федеральных органов исполнительной власти. № 39. 28.09.2015.

33. Проект Федерального закона № 124871-4 «О служебной тайне» (ред., внесенная в ГД ФС РФ, текст по состоянию на 24.12.2004) // СПС КонсультантПлюс

34. «Основы законодательства Российской Федерации об охране здоровья граждан» (утв. ВС РФ 22.07.1993 № 5487-1) (ред. от 07.12.2011) // «Российские вести», № 174, 09.09.1993. (утратил силу).

35. Указ Президента Российской Федерации № 960 от 11.08.2003 (ред. от 03.07.2018) «Вопросы Федеральной Службы Безопасности Российской Федерации» // Собрание законодательства РФ, № 161, 15.08.2003// Российская газета, № 51, 14.03.1997.

36. Указ Президента РФ от 16.08.2004 № 1085 (ред. от 31.08.2020) «Вопросы Федеральной службы по техническому и экспортному контролю» [Электронный ресурс] // Собрание законодательства РФ, 23.08.2004, № 34, ст. 3541.

37. Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с «Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети

«Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет») // Собрание законодательства РФ, 25.05.2015, № 21, ст. 3092// Российская газета, № 111, 26.05.2015.

38. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства РФ, 05.11.2012, № 45, ст. 6257// Российская газета, № 256, 07.11.2012.

39. Приказ ФСБ России и ФСТЭК от 31 августа 2010 г. № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования» // Российская газета, № 240, 22.10.2010// Бюллетень нормативных актов федеральных органов исполнительной власти, № 45, 08.11.2010.

40. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием СКЗИ» // Российская газета, № 211, 17.09.2014.

41. Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам» (вместе с «Положением о Национальном координационном центре по компьютерным инцидентам») // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 10.09.2018.

42. Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными

неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 10.09.2018.

Научная литература

43. Бурмейстер Ирина Александровна Медицинская (врачебная) тайна: теоретический аспект // Сибирский юридический вестник. 2015. №2 С.15-20.

44. Гражданское право / Под ред. А И. Калпина, А И. Масляева. — М.: Проспект, 2011. – 560 с.

45. Гатин А.М. Гражданское право/А.М. Гатин. — М.: Дашков и К, 2015. — 590 с.

46. Гражданское право: учеб. / С.С. Алексеев, Б. М. Гонгало, Д. В. Мурзин [и др.]; под общ. ред. чл.-корр. РАН С.С. Алексеева. — 2-е изд., перераб. и доп. — М.: Проспект; Екатеринбург; Институт частного права, 2015. — 550 с.

47. Грошева Екатерина Константиновна, Невмержицкий Павел Иванович Информационная безопасность: современные реалии // Бизнес-образование в экономике знаний. 2017. №3 (8). URL: https://cyberle№i№ka.ru/article/№/i№formatsio№№aya-bezopas№ost-sovreme№№ye-realii (дата обращения: 18.07.2019).

48. Грудцын Л.Ю. Гражданское право России: учеб/ Л.Ю. Грудцын, А.А. Спектор. — М.: ЗАО Юстицинформ, 2015. — 459 с.

49. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности, – СПб: СПбНИУИТМО, 2014. – 100 с.

50. Ефанова Е.А. Система информационной безопасности в Российской Федерации // Молодежный научный форум: Общественные и экономические науки: электр. сб. ст. по мат. XLVI междунар. студ. науч.-практ. конф. № 6(46).

URL: https://№auchforum.ru/archive/M№F_social/6(46).pdf (дата обращения: 18.07.2019)

51. Карапетян А. О частной, личной и семейной тайне в уголовном судопроизводстве // Бизнес в законе. 2013. №3 С.34-37.

52. Кибальник Алексей Григорьевич, Соломоненко Иван Геннадьевич Об ограничении Конституционного права на тайну личной (частной) жизни // Общество и право. 2015. №2 (20) С.49-52.

53. КОЛЕС 27001:2005. Информационные технологии. Методы обеспечения безопасности - Системы управления информационной безопасностью. Требования. - 2005. – 89 с.

54. Рыженков А.Я. Правовые формы противодействия монополистической деятельности в России // Современное право. 2015. № 7. С. 59-62.

55. Рыженков А.Я. Конституционный запрет монополизации и его отражение в отраслевом законодательстве // Юрист. 2016. № 1. С. 27-31.

56. Туманская В.А. Ограничение свободы массовой информации в соответствии с Конституцией РФ // Общественные и экономические науки. Студенческий научный форум: электр. сб. ст. по мат. IX междунар. студ. науч.-практ. конф. № 9(9). URL: https://№auchforum.ru/archive/S№F_social/9(9).pdf (дата обращения: 18.07.2019)

57. Танимов О.В., Кудашкин Я.В. О правовой природе и возможности правового регулирования в сети Интернет. [Электронный ресурс] СПС «КонсультантПлюс» (дата обращения: 18.07.2019).

58. Черепанова Ю.Е. Проблемы монополизации полномочий органами исполнительной власти в информационнойсфере // Вестник ННГУ. 2016. №3. URL: https://cyberle№i№ka.ru/article/№/problemy-mo№opolizatsii-pol№omochiy-orga№ami-ispol№itel№oy-vlasti-v-i№formatsio№№oysfere (дата обращения: 08.04.2019).

59. Эбзеев Б. С. Личность и государство в России : взаимная ответственность и конституционные обязанности. М. : Норма, 2017.- 98 с.

60. Бецков А.В. О некоторых аспектах правового понятия «информационная безопасность» / А.В. Бецков, И.В. Прохоров, А.Н. Митькин // Экстремальные ситуации, конфликты, социальное согласие. Сборник статей XIX Международной научно-практической конференции. Академия управления МВД России. 2018. С. 66-68.

61. Круликовский А.П. Анализ основных понятий информационной безопасности / А.П. Круликовский, П.В. Петроченко // Проблемы информационной безопасности. Труды VI Всероссийской с международным участием научно-практической конференции. 2020. С. 126-127.

62. Мохоров Д.А. Понятие информационной безопасности государства / Д.А. Мохоров, К.А. Семенова // Евразийский юридический журнал. 2020. № 2 (141). С. 391-392.

63. Нечай А.А. Кибербезопасность и информационная безопасность: сущность, содержание и отличие понятий / А.А. Нечай // XXIV Царскосельские чтения. 75-летие Победы в Великой Отечественной войне. Материалы международной научной конференции. 2020. С. 229-232.

64. Пелевина Е.С. Особенности системы информационной безопасности как элемента международной безопасности в современном мире / Е.С. Пелевина // Теории и проблемы политических исследований. 2017. Том 6. № 1А. С. 194-205.

65. Стейнджер Д. Разница между ИТ-безопасностью и кибербезопасностью [Электронный ресурс] / Режим доступа: https://igguru.net/2019/07/19/what-is-the-difference-between-it-security-and-cybersecurity/ (дата обращения 20.11.2020)

66. Танимов О.В., Федичев А.В. К вопросу об информационной безопасности современного государства // Правовая информатика. 2016. №2. С. 22-25.

67. Филиппова Н.В. Основные направления защиты информации в органах государственной власти / Н.В. Филиппова, О.И. Нестеровский, Н.Е. Тельнова // В сборнике: Профессиональные компетенции государственных

служащих: формирование и развитие. Материалы всероссийской научно-практической конференции. Редколлегия: Е.М. Лещенко [и др.]. 2019. С. 381-385.

68. Чикишева Н.А. Понятие и правовая основа информационной безопасности / Н.А. Чикишева // Современные проблемы и перспективные направления инновационного развития науки. Сборник материалов международной научно-практической конференции (январь 2020). 2020. С. 81-84.

69. Шободоева А.В. Развитие понятия «информационная безопасность» в научно-правовом поле России / А. В. Шободоева // Известия Байкальского государственного университета. — 2017. — Т. 27, № 1. — С. 73–78.

70. Ясенев В.Н. Информационная безопасность: Учебное пособие / В.Н. Ясенев, А.В. Дорожкин, А.Л. Сочков, О.В. Ясенев // Нижний Новгород: Нижегородский госуниверситет им.Н.И. Лобачевского, 2017. – 198 с.

71. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК) [Электронный ресурс]. Режим доступа: www.fstec.ru (дата обращения 20.11.2020).

72. Право интеллектуальной собственности: Учебник / под общ. ред. Л.А. Новоселовой. М., 2019. Т. 4: Патентное право. С. 311.

73. Пучков В.О. Информация - объект гражданского права? // Арбитражные споры. 2020. № 2. С. 135.

74. Урсул А. Д. Информатизация общества и переход к устойчивому развитию цивилизации / Вестник ВОИВТ, 2013, № 1-3. С. 12.

Архивные материалы и материалы практики

75. Определение Конституционного Суда Российской Федерации от 15 января 2003 г. № 45-О «Об отказе в принятии к рассмотрению запроса Арбитражного суда города Москвы о проверке конституционности статей 12 и 30 Федерального закона «О защите конкуренции на рынке финансовых услуг» // Вестник Конституционного Суда РФ. 2003. № 3.

76. Определение ВС РФ от 7 мая 2002 г. № КАС 02-132 // СПС КонсультантПлюс