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

Институт права
(наименование института полностью)

Кафедра «Конституционное и административное право»
(наименование)

40.05.01 Правовое обеспечение национальной безопасности
(код и наименование направления подготовки / специальности)

Государственно-правовая
(направленность (профиль)/специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (ДИПЛОМНАЯ РАБОТА)

на тему Правовая политика в сфере информационной безопасности

Обучающийся Л.О. Чмиль
(Инициалы Фамилия) (личная подпись)

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

Тольятти 2022

Аннотация

Вопросы обеспечения безопасности общества, личности и государства не теряют свою актуальность во всей ретроспективе существования человечества. И по мере того, как человечество достигает в своем развитии новых вершин, ему приходится открывать для себя все новые и новые аспекты обеспечения безопасности.

Так, в условиях становления и развития современного информационного общества, особую значимость приобретают вопросы информационной безопасности, чем посвящена тема дипломной работы.

Объект исследования - общественные отношения, возникающие в сфере регулирования информационного общества как определяющей тенденции современности, что ведет к серьезным трансформациям всех сфер общественных отношений.

Предмет исследования - нормы действующего законодательства, регулирующие вопросы обеспечения информационной безопасности в Российской Федерации и научно-теоретические исследования ученых, посвященные данной проблеме.

Цель работы – комплексный научно-правовой анализ правовой политики в сфере информационной безопасности.

Выпускная квалификационная работа структурно представляет собой совокупность следующих элементов: введение, три главы, шесть параграфов, заключение и список используемой литературы и используемых источников.

Оглавление

Введение

Актуальность темы исследования.

Вопросы обеспечения безопасности общества, личности и государства не теряют свою актуальность во всей ретроспективе существования человечества. И по мере того, как человечество достигает в своем развитии новых вершин, ему приходится открывать для себя все новые и новые аспекты обеспечения безопасности.

Так, в условиях становления и развития современного информационного общества, особую значимость приобретают вопросы информационной безопасности, чем посвящена тема настоящей выпускной квалификационной работы.

Понятие информационной безопасности было впервые упомянуто в российском законодательстве в 1992 году, в ст. 13 Закона РФ № 2446-1 от 05.03.1992 г. «О безопасности», где оно фигурировало в качестве обозначения одного из аспектов безопасности России. Это позволяет говорить, что, как правовая категория, информационная безопасность явление еще сравнительно молодое. И, даже несмотря на то, что за минувшие годы исследователи-правоведы посвятили немало времени и трудов его всестороннему изучению, в его правовом обеспечении по-прежнему остается немало неоднозначностей и пробелов.

Такое положение вещей объясняется тем, что и современное информационное законодательство, и современная юридическая наука просто не успевают за развитием информационного общества, высокие темпы которого практически не оставляют времени на тщательную проработку законопроектов и прогнозирование последствий их внедрения.

Ситуацию осложняет появление и развитие глобальных компьютерных сетей и формирование на их основе глобального информационного пространства, в котором развернулась борьба за достижение информационного превосходства. Наряду с этим развитие компьютерных

сетей повлекло за собой новый этап в развитии преступности: появились новые виды преступлений и возросли масштабы преступлений давно известных.

Кроме того, одним из приоритетных направлений российской государственной политики стало развитие информационного обеспечения деятельности органов государственной власти, один из компонентов, которого показывающего уровень прозрачности в государстве, является информационная открытость органов государственной власти.

Все это закономерно обусловило многократный рост числа информационных угроз и, соответственно, повысило актуальность вопросов обеспечения информационной безопасности. Что в свою очередь обуславливает и актуальность данного исследования.

Объект исследования - общественные отношения, возникающие в сфере регулирования информационного общества как определяющей тенденции современности, что ведет к серьезным трансформациям всех сфер общественных отношений.

Предмет исследования - нормы действующего законодательства, регулирующие вопросы обеспечения информационной безопасности в Российской Федерации и научно-теоретические исследования ученых, посвященные данной проблеме.

Цель выпускной квалификационной работы – комплексный научно-правовой анализ правовой политики в сфере информационной безопасности.

Для достижения поставленной цели необходимо решить следующие задачи:

- рассмотреть понятие и угрозы информационной безопасности;
- проанализировать источники правового регулирования информационной безопасности;
- исследовать организационно-правового обеспечение информационной безопасности органами государственной власти;

- выявить особенности обеспечения информационной безопасности субъектами коммерческой деятельности;
- обобщить практику противодействия приоритетным источникам угроз информационной безопасности;
- наметить пути совершенствования системы информационного обеспечения деятельности органов государственной власти.

Нормативно-правовая база исследования: Конституция Российской Федерации, Гражданский кодекс Российской Федерации, Уголовный кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, а также другие федеральные законы и нормативные правовые акты, нормы международного права, составляющие правовую основу правовой политики в сфере информационной безопасности Российской Федерации.

Теоретическая основа выпускной квалификационной работы представлена трудами ученых, посвященных актуальным проблемам правового обеспечения информационной безопасности в Российской Федерации и перспективах совершенствования правового регулирования информационной сферы. В работе использованы исследования следующих ученых: А.И. Алексенцева, И.В. Блиновой, М.М. Васильевой, С.В. Голубчикова, И.А. Добровольской, А.М. Карминского, Д.А. Ларченко, Н.С. Левшина, О.В. Мотовилова, С.П. Расторгуева, М. Б. Смоленского, А.А. Снытникова, А.А. Стрельцова ии др.

Выпускная квалификационная работа структурно представляет собой совокупность следующих элементов: введение, три главы, шесть параграфов, заключение и список используемой литературы и используемых источников.

Глава 1 Теоретико-правовой анализ информационной безопасности как угрозы национальной безопасности

1.1 Понятие и угрозы информационной безопасности

Понятие информационной безопасности было впервые упомянуто в российском законодательстве в 1992 году, в ст. 13 Закона РФ № 2446-1 от 05.03.1992 г. «О безопасности» [14], где оно фигурировало в качестве обозначения одного из аспектов безопасности России, находящихся в компетенции Совета безопасности РФ. Легальное определение информационной безопасности появилось в законодательстве гораздо позднее, в 2000 году, с утверждением Доктрины информационной безопасности Российской Федерации [13].

Примерно в то же время понятие информационной безопасности получило первое упоминание в международных правовых документах. В частности, в 1998 году, оно было упомянуто в резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» [24], принятой по инициативе РФ.

Переходя к непосредственному исследования понятия «информационная безопасность», необходимо отметить, что само слово «информация» происходит от латинского слова «informatio», что означает «разъяснение, высказывания, осведомленность» [4].

В ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» [74] понятие информации определяется как «сведения (сообщения, данные) независимо от формы их представления».

Несмотря на наличие легального определения информации, в доктрине предпринимаются попытки сформулировать его научно-теоретические понятие.

К примеру, А.А. Снытникова, «информация как благо нематериальное имеет множество разнообразных оттенков. В зависимости от тех или иных обстоятельств в повседневной жизни информация может быть актуальной и устаревшей, объективной и субъективной, основательной и безосновательной, многоплановой и однобокой, укрепляющей и компрометирующей и т.д.» [47, с. 20].

Ученые выделяют следующие свойства информации: объективность и субъективность, полнота, достоверность, адекватность, доступность, актуальность, репрезентативность [50].

О.В. Мотовилова отмечает, что «получение, обработка, передача и хранение различного рода информации - непременное условие работы любой управляющей системы» [23, с. 36]. Это означает, то процессы, происходящие в любой управляющей системе, будут основаны на движении информации, обмене ею между элементами и звеньями.

Наличие положительных характеристик информации, которой обмениваются элементы системы (достоверность, полнота, адекватность, актуальность и т.д.), а также процессов, посредством которых происходит движение и передача информации (скорость, наличие связи между всеми уровнями и элементами системы, отсутствие пробелов), определяет эффективность функционирования всей системы, правильность постановки целей и задач, передачи управляющих импульсов и получения ответа.

В современном обществе реализация управленческих процессов в сфере управления обществом и государством основывается на применении информационных технологий, которые кардинально изменили картину производства, движения и потребления информации.

Информационные технологии, также, как и промышленная революция XVIII-XIX веков преобразовали структурные связи в обществе, задав новый вектор и динамику развития человеческого сообщества. Значение информационных технологий заключается не только в многократном увеличении скорости и объема обработки массивов информации, но и в

возможности перевести реальную жизнь в цифровое пространство, соединить в цифровом поле объекты, которые в реальной жизни несоединимы, смоделировать новые умозрительные конструкции и связи. В практической деятельности информационные технологии значительно облегчили жизнь человека, освободив его от рутинной и сложной работы, а также создав платформу для объединения и конструирования новых связей.

В настоящее время нельзя назвать ни одной сферы жизнедеятельности, где не использовались бы цифровые технологии. Информационные технологии стали жизненно важной и неотъемлемой частью каждого общества, вне зависимости от сферы их применения. Общественные, публичные, коммерческие отношения опираются на информационные технологии. Начиная от многонациональных корпораций, которые поддерживают мэйнфреймовые системы и базы данных и малых предприятий, которые владеют одним компьютером, до систем обеспечения государственной деятельности, информационные технологии играют определяющую роль.

Логика развития современного общества и государства нуждается не только в совершенствовании государственного управления посредством его информатизации, но и новой стратегии государственного управления в период становления и развития информационного общества [6].

Преимущества использования информации и информационных технологий были оценены публичным сектором управления, поскольку новые технологии обеспечивали возможность работы с информацией (сбор, хранение, обработка, обмен), это повышало эффективность работы органов государственной власти.

В целом, с каждым годом происходит формирование и успешное развитие информационных технологий не только в мире, но и в России. Это связано в первую очередь с тем, что количество информационных возможностей возрастает. Увеличивается число пользователей в сети Интернет и число информационной и электронной техники. Однако с такой

положительной тенденцией можно заметить, что существует и выявляется преступная деятельность в информационной сфере. Сфера информационных технологий охватывает достаточно большой объем информации, сведений и иных данных, которые находятся как в закрытом доступе, так и в открытом [46, с. 47].

Рассматривая сферу информационных технологий необходимо отметить, что даже в ней совершаются преступления. Уголовный кодекс Российской Федерации (далее – УК РФ) [53] в главе 28 прописывает определенный перечень преступлений, которые совершаются в сфере компьютерной информатизации. Так же в некоторых других главах указываются преступления, которые посягают на информационную безопасность.

Все обуславливает необходимым проведение на государственном уровне правовой политики, направленной на обеспечение информационной безопасности.

В пп. 1 п. 5 Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [56] раскрывается понятие национальной безопасности Российской Федерации: «национальная безопасность Российской Федерации – это состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны».

Из определения национальной безопасности РФ непосредственно можно выделить следующие основные направления обеспечения безопасности:

– безопасность личности;

– безопасность общества;

– безопасность государства.

В п. 26 Стратегии национальной безопасности указано среди стратегических национальных приоритетов, направленных на защиту национальных интересов РФ информационная безопасность.

Как можно заметить, Стратегия национальной безопасности определяет информационную безопасность в качестве одного из стратегических национальных приоритетов России.

Согласно п. 56 Стратегии, целью обеспечения информационной безопасности является укрепление суверенитета Российской Федерации в информационном пространстве. Само понятие «информационное пространство» не имеет нормативного определения ни в тексте Стратегии, ни в других нормативных правовых актах. Вместе с тем, данное понятие достаточно полно раскрывается в различных научных трудах.

Например, И.А. Добровольская выделяет два основных подхода к определению понятия «информационное пространство» - технический и гуманитарный [12, с. 36]. Согласно техническому подходу, информационное пространство – это совокупность систем, осуществляющих обработку, хранение и передачу информации с применением различных технических средств и ресурсов. В то же время, гуманитарный подход определяет информационное пространство как совокупность знаний и информации, формирующейся и постоянно изменяющейся в процессе эволюции общества. Объединяя указанные подходы, можно сделать вывод о том, что информационное пространство представляет собой интегрированную среду хранения, передачи и распространения информации обо всех сферах жизнедеятельности человеческого общества. Опираясь на такое определение, в контексте заявленных в Стратегии целей обеспечения информационной безопасности, можно констатировать, что степень обеспечения информационной безопасности может оказывать влияние на широкий спектр различных общественных отношений, так или иначе использующих в своей

деятельности информационные технологии. Данное утверждение находит свое подтверждение при анализе п. 57 Стратегии, где заявлены задачи, решение которых должно позволить достигнуть целей обеспечения ИБ. Фактически, перечисленные в Стратегии задачи информационной безопасности, так или иначе, охватывают все основные направления обеспечения безопасности, перечисленные выше.

Далее необходимо с понятием «информационная безопасность».

В действующей Доктрине информационной безопасности Российской Федерации [58] ключевое ее понятие, т.е. «информационная безопасность понимается как защищенность личности, общества и государства от информационных угроз извне и изнутри, обеспечивающее реализацию конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое социально-экономическое развитие Российской Федерации, оборону и безопасность государства.

В целом, информационная безопасность представляет собой две составляющие:

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

Однако, среди ученых не сложилось единообразного понимания информационной безопасности, которая приобретает тот или иной смысл в зависимости от объекта безопасности. К примеру, если объектом защиты выступает информация, то такие понятия, как «информационная безопасность» и «безопасность информации» выступают синонимамичными

категориями. Если же объектом является другой объект, например, участник информационных отношений, то в понятие «информационная безопасность» слово «информационная» указывает на направление деятельности, в таком случае трактуется как состояние защищенности данного объекта от угроз информационного характера.

А.И. Алексенцев информационную безопасность определяет как «состояние информационной среды, обеспечивающее удовлетворение информационных потребностей субъектов информационных отношений, безопасность информации и защиты субъектов от негативного информационного воздействия» [1, с. 44]. Приведенное определение включает все необходимые признаки для характеристики информационной безопасности.

В последнее время под информационной безопасностью понимается защита от информации. Например, С.П. Расторгуев, считает, что «в результате проблема защиты информации, которая ранее была как никогда актуальна, перевернулась подобно монете, что вызвало к жизни ее противоположность. Теперь уже саму информационную систему и, в первую очередь человека - необходимо защищать от поступающей «на вход» информации, потому что любая поступающая на вход самообучающейся системы информация неизбежно изменяет систему. Целенаправленное же деструктивное информационное воздействие может привести систему к необратимым изменениям и, при определенных условиях, к самоуничтожению» [42, с. 47].

Понятие «информационная безопасность» достаточно тесно взаимосвязано с понятием «безопасность информации» или «защита информации», они достаточно синонимичны. Но «безопасность» не может существовать сама по себе, безотносительно к объекту, «без внутреннего смысла» [49, с. 55].

Таким образом, информационная безопасность представляет собой широкое понятие, включающее в себя все, что взаимодействует с информацией.

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

- принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

- создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
- неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации; дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;

– девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
– снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;
– манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

– монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
– блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
– низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться:

- противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;
- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

- противоправные сбор и использование информации; нарушения технологии обработки информации; внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности; уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;

– стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
– обострение международной конкуренции за обладание информационными технологиями и ресурсами;
– деятельность международных террористических организаций;
– увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий; деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
– разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

– критическое состояние отечественных отраслей промышленности;
– неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
– недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой

государственной политики в области обеспечения информационной безопасности Российской Федерации;

- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России; недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации; недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

Таким образом, информационная безопасность является составной частью системы национальной безопасности Российской Федерации, имеющая собственное содержание и представляющая собой сложную, многоаспектную категорию. Под информационной безопасностью

понимается состояние определенного объекта и деятельность, направленная на организацию обеспечения состояния защищенности данного объекта.

1.2 Источники правового регулирования информационной безопасности

Правовая основа информационной безопасности обозначена в п. 4 Доктрины информационной безопасности. При этом, определяющее значение имеет Конституция Российской Федерации [19], основные права и обязанности в сфере информации, среди которых можно назвать следующие:

- право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23 Конституции РФ);
- запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия (ст. 24 Конституции РФ);
- право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29 Конституции РФ);
- перечень сведений, составляющих государственную тайну, определяется федеральным законом (ст. 29 Конституции РФ).

При рассмотрении правовых механизмов, регулирующих те или иные сферы общественных отношений, как правило, затрагиваются также и нормы международного права, являющиеся составной частью правовой системы Российской Федерации (ч. 4 ст. 15 Конституции РФ).

Нормами международного права установлены стандарты защиты информации, однако без учета индивидуальных особенностей национальных правовых систем. В связи с чем, в сфере информационной безопасности приоритет принадлежит национальному законодательству, что также обусловлено высокой степенью анонимности при реализации угроз

информационной безопасности, а также значительным влиянием политических и конъюнктурных факторов и что делает невозможным эффективное применение международно-правовых механизмов.

В целом, отношения в сфере обеспечения информационной безопасности регулируются не только Конституцией РФ, но и федеральным законодательством Российской Федерации, включающее:

- федеральные законы;
- указы Президента РФ;
- постановления Правительства РФ;
- нормативные акты федеральных органов исполнительной власти.

Кроме того, в систему правового обеспечения информационной безопасности входят нормативные правовые акты регионального значения, муниципального уровня и локальные нормативные акты организаций и предприятий. При этом, важно отметить, что любые нормативные акты федерального уровня имеют большую юридическую силу, чем акты регионального или муниципального уровня, что имеет объективные предпосылки, заложенные в п. «м ст. 71 и ч. 1 ст. 76 Конституции РФ. Названные положения в полной мере относится к ситуации, когда в федеральных законах содержатся бланкетные нормы, отсылающие к различным подзаконным актам федерального уровня. Из этого следует, что любые подзаконные нормативные правовые акты федерального уровня в сфере информационной безопасности, принятые в соответствии с федеральными законами и не противоречащие им, также имеют приоритет над нормативными актами субъектов РФ.

Итак, основополагающим правовым актом в сфере информационной безопасности федерального значения является Федеральный закон «Об информации, информационных технологиях и о защите информации» [74], отражающий и конкретизирующий основные положения Конституции РФ в сфере информационной безопасности. Так, в соответствии со ст. 1

указанного нормативного акта, «настоящий Закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации».

Федеральный закон «Об информации, информационных технологиях и о защите информации» является центральным нормативным правовым актом информационного права, дает определение ряду категорий информационного права, а также задает базовые принципы механизмов правового регулирования данной отрасли права. На основе изложенных в законе принципов выстраивается, в числе прочего, и система нормативных правовых актов в области информационной безопасности.

Важную роль имеет Федеральный закон «О безопасности» [77]. В нем определяются основные принципы, содержание и направленность государственной политики по обеспечению безопасности государства во всех сферах, включая и сферу информационной безопасности. Данным нормативным актом осуществляется наиболее общее распределение полномочий в сфере обеспечения безопасности между органами власти.

В Законе РФ «О средствах массовой информации» [16] отображаются основные понятия СМИ, организация их деятельности, а также порядок распространения информации и ответственность за нарушение законодательства о средствах массовой информации. Данным законом охраняется право на неприемлемость цензуры и четко прописаны моменты, когда не допускается массовое использование информации.

Безусловно, любая информация может иметь определенную ценность, однако, некоторая является настолько важной, что получение несанкционированного доступа к ней может привести к угрозам безопасности государства различной степени тяжести и в различных сферах. Из-за этого общество вынуждено создавать разнообразные системы и

механизмы защиты информации, технические, организационные и правовые, регулирующие порядок оборота информации с ограниченным доступом (конфиденциальной информации) в Российской Федерации.

Проблема защиты конфиденциальной информации, как для организаций любой формы собственности, так и органов власти, в настоящее время стоит достаточно остро, поскольку, последняя является важнейшей составляющей любых информационных отношений. Вопросы правового регулирования использования и распространения информации в последнее время занимают одно из значительных мест в юридической литературе. Это обусловлено, прежде всего, тем, что содержание юридически значимой тайны заключается в том, что ее предмет образует информация, не предназначенная для широкого круга лиц, а ее разглашение может повлечь нежелательные последствия для владельцев и обладателей тайны.

Рассматривая организацию защиты отдельных видов конфиденциальной информации, можно констатировать, что для каждого вида конфиденциальной информации, государством разработан отдельный правовой механизм ее защиты, например, персональные данные защищаются Федеральным законом «О персональных данных» [75], целью которого является «обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну» (ст. 6). или определяемому физическому лицу (субъекту персональных данных)». Тема организации защиты персональных данных и регулирования их обработки обладает высокой общественной значимостью и высоким уровнем потенциального вреда от неправомерной обработки персональных данных. В этой связи, можно заметить, что механизмы правового регулирования обработки персональных данных постоянно развиваются, а законодательными органами власти России предпринимаются оперативные меры по реагированию на вновь возникающие угрозы.

Помимо правового регулирования обработки персональных данных, к обеспечению информационной безопасности также имеют прямое отношение механизмы регулирования работы с иными видами конфиденциальной информации.

К примеру, тайна следствия и судопроизводства осуществляется в соответствии с требованиями ст. 161 Уголовно-процессуального кодекса Российской федерации (далее – УПК РФ) [52].

Что касается профессиональной тайны, то, как указывает С.В. Голубчиков, «предметом профессиональной тайны являются отношения, которые возникают между субъектами, участвующими в обработке и защите профессиональной тайны» [7, с. 5]. К таким субъектам относятся владельцы (доверители) – физические лица, доверившие сведения другому лицу, держатели и пользователи – физические, юридические и иные лица, которым в силу их профессиональных обязанностей, были доверены в пользование сведения, составляющие профессиональную тайну.

Защита профессиональной тайны установлена рядом норм федеральных законов, среди которых можно назвать следующие:

- Гражданский кодекс Российской Федерации (далее – ГК РФ) [10];
- Федеральный закон «Об адвокатской деятельности и адвокатуре в Российской Федерации» [79];
- Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации» [72];
- Основы законодательства Российской Федерации о нотариате [25] и др.

Федеральный закон «О коммерческой тайне» [78] устанавливает виды информации, которая является или не является коммерческой тайной. Так, «информация, составляющая коммерческую тайну, определяется как научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, в том числе ноу-

хау, которая обладает действительной или потенциальной коммерческой ценностью в силу ее неизвестности третьи лицам, которые могли бы получить выгоду от ее разглашения или использования, к которой нет свободного доступа на законном основании и по отношению к которой принимаются адекватные ее ценности правовые, организационные, технические и иные меры охраны». Законом определены права обладателя сведений, составляющих коммерческую тайну, которые возникают с момента установления им режима коммерческой тайны.

Охрана тайны интеллектуальной осуществляется в соответствии с нормами части четвертой ГК РФ [11], направленных на защиту автора интеллектуальных произведений.

ФЗ «Об информации, информационных технологиях и о защите информации» определено, что информация, составляющая государственную тайну, так же относится к конфиденциальной, однако, защита данного рода информации осуществляется в соответствии с Законом «О государственной тайне» [15]. Государственная тайна особо охраняется государством и представляет собой «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации».

Рассматривая вопросы правового регулирования информационной безопасности нельзя не отметить, что вся система обеспечения информационной безопасности не в состоянии эффективно работать в ситуации, когда отсутствуют механизмы привлечения к ответственности за нарушение установленных норм и правил, либо за различные деструктивные воздействия на механизмы системы. Ответственность за нарушения в сфере обеспечения информационной безопасности определяются положениями ГК ГК РФ [9] в части возмещения вреда, УК РФ и Кодекса РФ об административных правонарушениях (далее – КоАП РФ) [18].

Следует обратить внимание на то, что большинство норм федерального значения в части регулирования информационной безопасности содержат положения, нуждающиеся в конкретизации посредством подзаконного нормотворчества. При этом, количество подзаконных нормативных актов в сфере информационной безопасности достигает несколько сотен.

Так, важное значение для информационной безопасности имеют Указы Президента РФ, представляющих собой документы стратегического планирования. Среди таких указов следует назвать указы, утвердившие Стратегию национальной безопасности РФ и Доктрину информационной безопасности РФ.

К примеру, Доктрина информационной безопасности РФ является документом стратегического планирования в сфере обеспечения национальной безопасности РФ, в котором развиваются положения Стратегии национальной безопасности РФ, а также других документов стратегического планирования в указанной сфере. Существенным отличием ныне действующей Доктрины является то, что в ней закрепляются и значительно расширяются основные понятия и термины, недостаточно интерпретируемые в предыдущем документе, а выделение терминологии в отдельный раздел Доктрины, осуществляет постановку более четких границ правового регулирования документа.

Действующая Доктрина информационной безопасности формирует основные положения Стратегии национальной безопасности, касающиеся:

- тенденции усиления конфронтации среди мировых лидеров в области глобального информационного пространства;
- возможных угроз безопасности и устойчивости функционирования российской критической информационной инфраструктуры;
- вопросов деятельности, связанной с использованием информационных и коммуникационных технологий в сфере преступлений террористической и экстремистской направленности;

– возможности импортозамещения с целью уменьшения критической зависимости от иностранных технологий и промышленной продукции.

Можно отметить тот факт, что курс на импортозамещение прослеживается в обоих документах. Данная задача выделяется как основная для нашей страны. Меж тем, в Доктрине информационной безопасности экономическая сфера обеспечения информационной безопасности сосредоточена именно на необходимости формирования национальной отрасли информационных технологий и информационной безопасности, следствием которого должна послужить ликвидация какой-либо зависимости от зарубежных информационных технологий.

Кроме того, в сфере информационной безопасности важное значение имеют указы Президента РФ, отражающие оперативную реакцию государства на вновь возникающие угрозы. В числе таких документов следует назвать Указ Президента РФ «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [55]. Указанный нормативный акт стал шагом к перераспределению полномочий государственных органов в сторону создания единой системы органов, ответственных за выработку и реализацию мер по обеспечению информационной безопасности. тдельное внимание в документе уделяется также необходимости качественного локального регулирования вопросов, касающихся информационной безопасности на объектах КИИ и иных стратегически важных объектах.

Помимо общих вопросов, затрагивающих систему информационной безопасности в целом, Указами Президента также регулируются отдельные направления, связанные с защитой отдельных видов информации [59; 57].

Нормативными актами Правительства РФ регулируются конкретные направления информационной безопасности. Так, например, Постановление Правительства РФ «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных

информационных систем и дальнейшего хранения содержащейся в их базах данных информации» [30] играет важную роль в цифровизации деятельности государственных органов. Названное постановление определяет наиболее общие и важные положения, касающиеся разработки программного обеспечения для автоматизации деятельности государственных органов и подведомственных им предприятий.

Следует подчеркнуть, что Правительство РФ осуществляет оперативное реагирование на вновь возникающие угрозы в сфере информационной безопасности. Это выражается, в числе прочего, в выработке конкретных мер, направленных на преодоление угроз. Так, Постановлением Правительства РФ «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)» [33] исполняются Указа Президента РФ от 01.05.2022 № 250. В частности, конкретизируются требования к организациям, имеющим стратегическое значение или обслуживающим объекты КИИ РФ, в части обязанности создания и функционирования специализированных подразделений по ИБ и правового статуса заместителей руководителя по ИБ.

Кроме того, нормативными правовыми актами Правительства РФ унифицируются технологии, используемые для создания и эксплуатации ГИС. Согласно Постановлению Правительства РФ «О проведении эксперимента по созданию, переводу и развитию государственных информационных систем и их компонентов на единой цифровой платформе Российской Федерации «ГосТех» [31], в настоящий момент в ряде органов реализуется пилотный проект по использованию единой цифровой платформы Российской Федерации «ГосТех». Указанное обстоятельство можно считать шагом к обеспечению единого подхода к обеспечению информационной безопасности во всех государственных органах. Вместе с

тем, выбранный инструмент имеет неоднозначные оценки с точки зрения эффективности, что будет показано далее в ходе исследования.

Таким образом, на уровне подзаконного нормотворчества развиваются и конкретизируются отдельные направления регулирования информационной безопасности. Вместе с тем, данные документы носят достаточно общий характер. Дальнейшая конкретизация отдельных правовых механизмов, регулирующих отношения в сфере информационной безопасности, осуществляется на уровне приказов отдельных федеральных органов исполнительной власти.

Содержательный аспект информационного обеспечения деятельности региональных органов исполнительной власти отражен в программных и стратегических документах, направленных на развитие цифровой экономики и обеспечение информационной безопасности.

Программным документом цифровизации всех уровней управления является Государственная программа Российской Федерации «Информационное общество» [32], которая ставит целью снижение цифрового и информационного неравенства в регионах.

Основным документом информатизации и информационного обеспечения деятельности региональных органов власти является Распоряжение Правительства РФ «Об утверждении Концепции региональной информатизации» [41].

Изложенное в первой главе выпускной квалификационной работе, позволяет сделать следующие выводы.

Во-первых, информационная безопасность является составной частью системы национальной безопасности Российской Федерации, имеющая собственное содержание и представляющая собой сложную, многоаспектную категорию. Под информационной безопасностью понимается состояние определенного объекта и деятельность, направленная на организацию обеспечения состояния защищенности данного объекта. По своей общей направленности угрозы информационной безопасности Российской

Федерации подразделяются на угрозы конституционным правам и свободам человека и гражданина, информационному обеспечению государственной политики Российской Федерации и развитию отечественной индустрии информации.

Во-вторых, правовая основа информационной безопасности обозначена в п. 4 Доктрины информационной безопасности. При этом, определяющее значение имеет Конституция Российской Федерации. Нормами международного права установлены стандарты защиты информации, однако без учета индивидуальных особенностей национальных правовых систем. В целом, отношения в сфере обеспечения информационной безопасности регулируются не только Конституцией РФ, но и федеральным законодательством Российской Федерации, а также нормативными правовыми актами регионального значения, муниципального уровня и локальными нормативными актами организаций и предприятий.

Глава 2 Организационно-правовое обеспечение информационной безопасности

2.1 Организационно-правовое обеспечение информационной безопасности органами государственной власти

Каждая страна в современном мире правомочна защищать национальные интересы, в которых проявляется ее государственная независимость, рост экономического благополучия населения, модернизация межкультурных связей в обществе и качественное улучшение жизни граждан. В то же время методы и пути реализации заявленных целей при обеспечении возможности реализации национальных интересов у каждой страны, как правило, свой. И этот путь не может слепо копироваться, даже у стран с очень хорошими показателями, продемонстрированными ими при достижении перечисленных целей. Это вполне закономерный вывод, учитывая то обстоятельство, что условия формирования социумов различны и зачастую неповторимы. Поэтому цели и задачи, а так же методы их достижения должны уточняться и видоизменяться в соответствии с изменениями внутренних и внешних условий, в которых находится конкретное государство. В то же время, глобализация, бесспорно, принесла один очень хороший результат – сформированное мировое информационное пространство. И этим пространством необходимо уметь грамотно распорядиться. В этих условиях налаживание и развитие международных связей России становится приоритетной задачей, как государства, так и всего общества в целом [46]. И одной из актуальных проблем становится вопрос организационной основы обеспечения информационной безопасности.

Итак, организационные основы обеспечения информационной безопасности конкретизированы в пунктах 10-29 Доктрины информационной безопасности РФ, в которых обозначены основные сферы общественных отношений, включающие организация вооруженной защиты Российской

Федерации, борьбы с проявлениями терроризма и экстремизма, контрразведывательной деятельности, сведениями, составляющими государственную тайну, неприкосновенности частной жизни, защиты персональных данных физических лиц и др.

Исходя из перечисленных основных сфер общественной жизни, а также учитывая положения п.33 Доктрины информационной безопасности, можно выделить перечень органов, составляющих организационную основу информационной безопасности.

Так, на уровне федеральных органов государственной власти организационную основу информационной безопасности составляют: Президент РФ, органы исполнительной власти, органы законодательной и судебной власти, а также Центральный Банк РФ и органы власти субъектов Федерации и органы местного самоуправления.

Ключевым элементом, оказывающим влияние на информационную безопасность, безусловно, является Президент РФ. В соответствии с п.32 Доктрины информационной безопасности, он определяет состав системы обеспечения информационной безопасности. Одновременно с этим, в п. 31 Доктрины информационной безопасности подчеркнуто, что система обеспечения информационной безопасности строится на основе разграничения полномочий всех ее структурных элементов. Таким образом, именно Президенту РФ принадлежит одна из ведущих ролей в определении объема полномочий каждого государственного органа в сфере обеспечения информационной безопасности.

Одним из важнейших элементов структуры является ФСБ России, на которую согласно ст. 11.2 Федерального закона «О федеральной службе безопасности» [65], на службу возложены полномочия по формированию и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств.

Рассматривая ключевые элементы структуры, нельзя не упомянуть ФСТЭК России [64]. Данная служба играет важную роль в осуществлении технического регулирования в области информационной безопасности. В частности, именно приказами ФСТЭК осуществляется определение требований к информационным системам, применяющимся в государственных органах и подведомственных им государственных предприятиях, а также контроль над выполнением указанных требований в ходе различных аттестаций и сертификаций.

Значительная роль МВД России в структуре органов, оказывающих влияние на информационную безопасность, заключается в том, что предварительное расследование по большой части преступлений, которые посягают на отношения в сфере информационной безопасности, осуществляется именно МВД [54].

Федеральная служба охраны России [61] играет значительную роль в обеспечении информационной безопасности, поскольку является органом, обеспечивающим нормальное функционирование системы правительственной связи. Кроме того, ФСО является организатором системы межведомственного электронного документооборота, объединяющей между собой информационные системы различных органов власти всех уровней при обмене информацией, не содержащей сведений, составляющих государственную тайну.

Ключевую роль в обеспечении информационной безопасности в России играет Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) [29]. Именно в ведении указанного министерства находится реализация большей части государственных программ, направленных на построение цифрового общества, внедрение информационных технологий в различные сферы жизни. Его роль в обеспечении информационной безопасности заключается в том, что именно Роскомнадзор отвечает за выработку и практическое применение механизмов правового регулирования, направленных на

обеспечение защиты персональных данных, контроля и надзора за деятельностью операторов связи, СМИ, а также в информационно-телекоммуникационной сети «Интернет».

Важная роль в сфере обеспечения информационной безопасности принадлежит таможенным органам, деятельность которых направлена на защиту государственных экономических интересов и осуществление регулирования внешней торговли исходя из интересов поддержания необходимого уровня национальной безопасности страны. В то же время таможенная служба прилагает серьезные усилия по созданию благоприятных таможенных режимов с целью обеспечения высокого уровня развития внешней торговли отечественными производителями, что в свою очередь так же является фактором усиления уровня экономической безопасности и представляет собой часть осуществляемой государством экономической политики на современном этапе развития мировой экономики.

ФТС России [63], как уполномоченный орган исполнительной власти, осуществляет руководство таможенным делом в Российской Федерации и, в связи с этим, ставит перед собой определенные задачи, которые могут быть сформулированы следующим образом:

- разработка таможенной политики;
- поддержание достаточного уровня национальной безопасности путем защиты экономических интересов страны;
- обеспечение реального участия РФ в международных организациях по вопросам связанным с экономической безопасностью.

Таким образом, официально декларируется, что экономическая безопасность является важным структурным элементом национальной безопасности. Кроме того, важной задачей таможенных органов, по-прежнему, является снижение уровня экономических преград, затрудняющих ведение внешнеэкономической деятельности российским предприятиям и организациям. К внешним преградам относят серьезную зависимость экономики страны от импорта, особенно в сфере продовольствия и высоких

технологий, открытость нашей экономики и её часто бесконтрольное вовлечение в глобальную экономику или при отсутствии должного контроля, необходимого для обеспечения достаточных гарантий защиты государственного суверенитета. Исследования, проводимые различными подразделениями, как государственных, так и общественных организаций, показывают, что данные угрозы по-прежнему только нарастают. В то же время важность сбалансированной таможенной политики для обеспечения национальной безопасности страны не подвергается сомнениям. И развитие этой политики должно проходить по трем направлениям:

- постоянное совершенствование законодательства регулирующего деятельность таможенных органов;
- участие таможенных органов в разрабатываемых государственных программах обеспечения экономической безопасности;
- постоянный мониторинг экономической обстановки, с целью совершенствования механизма деятельности таможенных органов и таможенной политики [46, с. 23].

Таможенные органы по собственному административно-правовому статусу считаются военизированными и правоохранительными структурами, т.е. относятся к силам обеспечения государственной защищенности. И ФЗ «О безопасности» относит таможенные органы именно к таковым. В то же время зоны ответственности таможенных служб, их роль в обеспечении защищенности экономики государства с каждым годом только возрастает, что обусловлено политическими и финансовыми задачами как внутри страны, так и за еепределами. Можно выделить три уровня защищенности: интернациональный, государственный и личный. И таможенные службы принимают участие в процессах понижения рисков и опасностей на всех 3-х уровнях.

Так, в согласовании с п. 8 ст. 12 Федеральный закон «О таможенном регулировании в Российской Федерации» [76], таможенные органы оказывают помощь в борьбе с интернациональной преступностью. Основным

в данной деятельности является выявление каналов международной контрабанды, что является необходимым условием поддержки отечественного производства, а это в свою очередь усиливает экономический потенциал и ведет к экономическому росту и увеличению эффективности работы государства. В науке неоднократно указывали, что «для эффективного функционирования государства важнейшее значение имеет состояние экономической безопасности государства, а для ее поддержания нужен стабильный экономический рост и целевое использование национальных ресурсов» [45, с. 36].

Борьба с таможенными правонарушениями одна из самых важных функций таможенных служб по обеспечению финансовой защищенности страны. Криминализация внешнеэкономической деятельности участников ВЭД продолжает оставаться серьезной опасностью для экономической защищенности страны. Динамика таможенных преступлений служит важным подтверждением этого положения, что позволяет сделать вывод о том, что функции таможенных органов по обеспечению экономической безопасности становятся всеобъемлющими. Сегодня таможенные органы призваны оберегать, прежде всего, финансовые интересы страны и обеспечивать её экономическую безопасность. И поддержание экономической безопасности, в настоящее время, становится приоритетным направлением работы, в числе других задач, стоящих перед таможенными органами в целом.

При рассмотрении организационных основ обеспечения информационной безопасности, следует отдельное внимание уделить вопросу цифровизации деятельности органов государственной власти. Возникновение новых видов и форм общественных отношений вызывает к необходимости их правовую регламентацию с целью обеспечения прав участников самих отношений, а также интересов общества и государства. Цифровые технологии стали проникать на все уровни и во все типы экономических связей между хозяйствующими субъектами [20].

Прежние модели формирования системы правового регулирования общественных отношений перестают удовлетворять потребностям новой информационно-коммуникационной и технологической среды. На фоне перспективы автоматизации (технологизации, цифровизации) юридических процессов, которая стала рассматриваться как альтернатива традиционным законотворческим институтам, вопрос создания концептуальных правовых основ регулирования цифровых технологий становится еще более очевидным. При этом проблемы формирования правовой среды определяются не просто отсутствием того или иного закона. «Основные проблемы, определяющие негативные условия для трансформации правовой среды связаны с невозможностью эволюционного пути развития законодательства и права» [80, с. 145] на современном этапе.

Россия, также, как и многие другие цивилизованные страны стоит на пути широкого внедрения в управленческую деятельность информационных технологий и расширения качества информационного обеспечения деятельности государственных органов на всех уровнях.

Законодательство РФ, непосредственно связанное с внедрением и использованием технологий электронного управления, насчитывает несколько десятков нормативно-правовых актов. Причем, электронное управление рассматривается в основном не как отдельная сфера, как этого требует развитие современного общества, а как составляющая сферы информатизации. Целью создания электронной информационной системы Электронное правительство является обеспечение открытости деятельности органов государственной власти и реализации гражданами конституционных прав на участие в управлении государственными делами, повышения эффективности деятельности органов государственной власти всех уровней.

Электронное правительство представлено тремя составляющими: граждане, бизнес и государство. Все эти компоненты взаимодействуют между собой в рамках взаимно-обратной связи.

В России процесс построения электронного правительства, т.е. информационного обеспечения деятельности органов власти, начался с принятия «Стратегии развития информационного общества в России» в 2008 г. и целевой программы «Электронная Россия» [48]. В 2017 году принята новая Стратегия [62]. Также для реализации поставленных задач был утвержден ряд документов, имеющих прямое отношение к развитию информационного обеспечения органов власти:

- Концепция формирования электронного правительства в Российской Федерации [39];
- Концепция региональной информатизации [41];
- Концепция использования информационных технологий в органах государственной власти [40];
- Программа «Цифровая экономика» [26].

В 2010 г. распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-р утверждена государственная программа Российской федерации «Информационное общество» [32], целью которой является получение гражданами и организациями преимуществ от применения информационных и телекоммуникационных технологий за счет обеспечения равного доступа к информационным ресурсам, развития цифрового контента, применения инновационных технологий, радикального повышения эффективности государственного управления при обеспечении безопасности в информационном обществе. Первоначально планировалось, что Программа будет реализована до 2020 года, однако в 2017 году она была продлена до 2030 года.

Исполнителями Подпрограммы «Информационное государство» назначены Минкомсвязь, Минздравсоцразвития, Минобрнауки.

Согласно Федеральному закону «О федеральном бюджете на 2022 год и на плановый период 2023 и 2024 годов» [68] на реализацию Программы «Информационное общество» заложено в 2022 году 3 320 000 тыс. рублей.

В условиях перевода государственных услуг в цифровую среду, с 2012 года все регионы и муниципалитеты начали постепенный переход на электронное межведомственное взаимодействие. А с 2018 года в соответствии с Указом Президента РФ № 601 от 7 мая 2012 года 70% всех госуслуг оказываются в электронном виде [60].

Практически каждый орган государственной власти на федеральном и региональном уровне имеет официальный сайт, что значительно облегчает получение государственных услуг. Каждый желающий может с легкостью зайти на официальный сайт и ознакомиться с необходимой информацией, а также отправить личное обращение или запрос.

Нельзя сказать, что информатизация публичного управления в российской практике происходит абсолютно гладко. Так, например, обращения граждан и организаций принимаются государственными службами как на электронную почту, так и через специальную форму для регистрации обращений на сайте. Однако интерфейс публичных страниц для обращения граждан, созданный в рамках государственных закупок не всегда отвечает содержательным требованиям, например, не всегда удается с легкостью найти необходимую информацию на сайте, через избыточную нагроможденность сайта или отсутствие регулярного наполнения, не всегда проработан пользовательский интерфейс, например, отсутствуют необходимые фильтры для поиска необходимой информации. С обращениями тоже могут возникать трудности, так как не всегда легкодоступен перечень документов необходимых для рассмотрения вопроса, кроме того, формы для обращений бывают неудобными или непонятными обычному пользователю.

На более высоком уровне препятствиями на пути внедрения электронных государственных услуг являются:

– высокая цена и сложность реализации индивидуальных транзакционных услуг и регламентов;

– отсутствие юридической базы для полноценной работы государственных учреждений с информацией в электронной форме, которая обеспечивала бы законодательную основу для практического исключения проблемы медиа-разрыва;
– отсутствие большого количества высококлассных специалистов-государственных служащих в государственных учреждениях;
– недостаточный уровень заработной платы государственных служащих, который не обеспечивает мотивацию для совершенного владения компьютерными технологиями.

Таким образом, использование информационно-справочных и аналитических систем положительно влияет на сферу государственного управления и создает возможности для совершенствования и обогащения практики публичного управления.

В настоящее время в России происходит активное внедрение и развитие информационных технологий в сфере публичного управления, для чего создана нормативно-правовая база, обеспечены организационные и финансовые ресурсы для реализации данного процесса. Однако отдельные препятствия (недостаточность технического обеспечения всей территории страны, особенно удаленных регионов) исключают возможность качественного и быстрого информационного обеспечения, полномасштабного охвата населения государственными услугами в цифровом формате, привлечения граждан к участию в управлении государственными и муниципальными вопросами, активизации гражданской составляющей у жителей страны. В этом направлении государству предстоит принять еще ряд тактических решений, дабы процесс интеграции информационных технологий отвечал планам и задачам государственной политики цифровизации.

2.2 Обеспечение информационной безопасности субъектами коммерческой деятельности

Информационная безопасность обеспечивается и коммерческими структурами, что связано с необходимостью обеспечения конфиденциальной информации. Под конфиденциальностью понимают принцип неразглашения информации, не предназначенной для открытого доступа или пользования всеми желающими.

В основе конфиденциальности лежит идея о том, что конкретная информация не должна быть доступна тем, кто ее не должен видеть. Все виды деловой и личной информации создаются, хранятся и обмениваются. Информация может быть сведениями о продажах, личными и персональными данными, маркетингом, счетами или многими другими документами. Для большинства из этих типов информации нет завышенных требований к конфиденциальности или секретности. Например, существует информация, которая не является критически важным секретом, допустим, если бы общественности стала известна информация о том, сколько компания тратит на электричество или водоснабжение.

И, наоборот, для любого бизнеса, осуществляющего крупномасштабные операции с информацией о кредитных картах клиента в качестве платежа либо информация о персональных данных клиента чрезвычайно важно защитить [81, с. 52].

Существует несколько классификаций информации по степени ее секретности. Информация ограниченного доступа – к ней относятся государственная тайна, ноу-хау, коммерческая тайна, персональные данные и другие виды тайн. Публичная информация – информация, полученная или созданная в процессе выполнения публичных обязанностей, установленных законами или изданными на их основании правовыми актами. Предпочтительная информация – может включать в себя лицо или определенную группу лиц, которым доступна конфиденциальная

информация, разглашение данной информации влечет за собой юридическую ответственность.

Информация – это своего рода ресурс. Информационные ресурсы являются неистощимыми и предполагают существенно иные методы воспроизведения и обновления, нежели материальные ресурсы [5, с. 356].

В информационных технологиях используются следующие элементы: аутентификация, авторизация и контроль доступа.

Аутентификация должна быть в первую очередь. В жизни мы можем проверить удостоверение личности с фотографией или попросить предъявить банковскую карточку и ввести PIN-код. Компьютерные системы, как минимум, должны запрашивать идентификатор пользователя и пароль.

Управление доступом включает в себя то, что человек может или не может делать, основываясь на своей роли. Может ли они читать, записывать, изменять, добавлять или удалять информацию?

Как можно заметить существуют проблемы и последствия разглашения конфиденциальной информации, которые охватывают все аспекты современного бизнеса. Меры применяются независимо от того, является ли информация электронной, печатной или даже устной. Обучение сотрудников и клиентов, а также ясность в коммуникациях являются ключевыми.

Далее следует привести несколько способов эффективной защиты конфиденциальной информации.

Так, работодатель имеет полный доступ к информации на компьютерах работников и вправе требовать возмещения убытков в случае разглашения коммерческой тайны. Страх потерять высокооплачиваемую работу будет препятствовать сотрудникам разглашать коммерческую или юридическую тайну компании.

Иногда компании устраивают провокации: рассылают сотрудникам вирусные письма, запрашивают конфиденциальную информацию по телефону и т.д.

DLP-система (предотвращение утечки данных). Он отслеживает передачу и печать файлов, внезапные всплески в интернет-коммуникации, посещение атипичных веб-сайтов и т.д. Она также выполняет лингвистический анализ корреспонденции и документов, а также устанавливает опасность утечки по ключевым словам.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности и создаст условия для ее дальнейшего совершенствования.

Конфиденциальная информация сама по себе не является коммерческой тайной. Чтобы сведения признали коммерческой тайной, необходимо ввести режим коммерческой тайны. Сотрудники не обязаны догадываться, что для работодателя сведения конфиденциальные и он не желает их распространять.

Предыдущий тезис подтверждается следующим примером из правоприменительной практики: работодатель не доказал, что ввел режим коммерческой тайны в отношении чертежей, которые сотрудник выложил в интернет Организация не создала необходимых условий, чтобы работник выполнил режим коммерческой тайны. Суд указал: «сотрудник не подтверждал свое согласие на соблюдение режима коммерческой тайны для каких-либо документов ввиду того, что перечень информации, составляющей коммерческую тайну, сторонами договора... не определялся, порядок обращения с данной информацией и контроль за его соблюдением не устанавливался, учет лиц, получивших допуск к конфиденциальной информации, не осуществлялся, поскольку его текст и оригиналы чертежей не содержат грифа «Коммерческая тайна» с указанием обладателя такой информации» [35].

По общему правилу после того, как обладатель информации принял эти меры, режим коммерческой тайны считается установленным (п. 1 и 2 ст. 10 ФЗ «О коммерческой тайне»).

Исключением из приведенного алгоритма является механизм охраны такого объекта гражданских прав, как секрет производства (ноу-хау).

В действующей до 1 октября 2014 года редакции ст. 1465 ГК РФ под «секретом производства (ноу-хау) признаются сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны», что предполагало необходимость обязательного присвоения ноу-хау статуса коммерческой тайны. Ныне действующая редакция статьи 1465 ГК РФ смягчила требования к охране конфиденциальности ноу-хау. Сейчас обладателю информации достаточно принимать разумные меры, чтобы сохранить сведений в секрете. В качестве одной из таких мер, но не как обязательный признак ноу-хау, закон называет введение режима коммерческой тайны.

Если организация не введет режим коммерческой тайны, то не сможет привлечь к ответственности лицо, которое распространило информацию.

Комплексный анализ действующего законодательства позволяет выделить следующие виды ответственности.

Во-первых, дисциплинарная ответственность. Работодатель вправе расторгнуть трудовой договор по своей инициативе, если сотрудник разгласит в том числе коммерческую тайну. При этом, важно учесть тот факт что сотрудник, к которому применяется данный вид ответственности должен получить данные сведения в связи с исполнением трудовых обязанностей (подп. «в» п. 6 ст. 81 Трудового кодекса Российской федерации (далее - ТК РФ) [51]). Помимо увольнения, работодатель вправе применить дисциплинарное взыскание в виде замечания или выговора (ст. 192 ТК РФ).

Во-вторых, материальная ответственность. Следует обратить внимание на тот факт, что сотрудник, который выдал коммерческую тайну, несет материальную ответственность в полном размере причиненного ущерба (п. 7 ст. 243 ТК РФ). При этом следует помнить, что закон не запрещает за один проступок одновременно применять материальное и дисциплинарное взыскание.

В-третьих, административная ответственность. Лицо, которое получило доступ к информации, при исполнении служебных или профессиональных обязанностей, понесет ответственность, если разгласит такую информацию (ст. 13.14 КоАП РФ).

В-четвертых, уголовная ответственность. Максимальное наказание для сотрудника, который нарушил режим коммерческой тайны, составляет лишение свободы до семи лет (ст. 183 УК РФ).

Резюмируя сказанное, для установления режима охраны коммерческой тайны, видится целесообразным совершить следующие действия:

Во-первых, издать положение о коммерческой тайне. В положении о коммерческой тайне необходимо указать, какая конфиденциальная информация будет составлять коммерческую тайну. Организация вправе разработать несколько положений для разных подразделений, данная мера потребуется, если компания занимается разными видами деятельности или производственные и коммерческие процессы имеют специфику. Например, сотрудники производственных цехов и бухгалтеры владеют разной информацией. Поэтому лучше, помимо универсальных фраз про ответственность за разглашение, прописать детально виновные действия. Это будет понятнее сотруднику и позволит устранить неопределенность в суде.

Важно помнить, что нельзя включить в состав коммерческой тайны пять групп сведений:

- общедоступные сведения о регистрации организации или предпринимателя;

- сведения в документах на право вести предпринимательскую деятельность, например, в лицензиях;
- данные о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании бюджетных средств;
- информация об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
- сведения, которые обладатель информации обязан раскрыть или не должен скрывать.

Во-вторых, ознакомить сотрудников с положением о коммерческой тайне. Каждого сотрудника необходимо ознакомить с положением о коммерческой тайне. Чтобы упорядочить сбор подписей, ведут журнал. В нем каждый сотрудник подтверждает, что ознакомился с положением о коммерческой тайне, – ставит подпись и дату. Необходимо, чтобы сотрудник сам проставил дату, когда ознакомился с документом. Иначе в случае спора сотрудник может заявить, что подписал положение о коммерческой тайне позже, чем разгласил информацию.

В-третьих, утвердить перечень сведений, которые составляют коммерческую тайну. Перечень нужен, чтобы не утверждать новое положение каждый раз, когда появилась информация, которую решили отнести к коммерческой тайне.

В-четвертых, изменить трудовые и гражданско-правовые договоры. Условие об обязанности хранить коммерческую тайну стоит включить:

- в трудовые договоры – закон это прямо разрешает;
- гражданско-правовые договоры. Так, доступ к информации получают лица, которые не связаны с организацией трудовыми отношениями, например, консультанты, переводчики.

В-пятых, внести изменения в должностные инструкции. Стоит включить положения о коммерческой тайне в должностную инструкцию

сотрудника. Это позволит еще раз напомнить сотруднику о том, что он обязан соблюдать режим коммерческой тайны.

Все вышеописанные ситуации предполагают нарушение режима коммерческой тайны со стороны наемных лиц (по трудовому либо гражданско-правовому договору). Однако, не редко возникают ситуации, при которых сторонние организации могут нарушить режим конфиденциальности информации, полученной ими в ходе вступления в правоотношения со своими контрагентами.

Взаимодействие с контрагентом предусматривает, возможность предоставления ему доступа к информации, которую он бы не узнал при других обстоятельствах. Так, доступ к конфиденциальной информации компании получают:

- аудитор – к информации о хозяйственно-финансовых операциях организации;
- консалтинговая фирма – к информации об отношениях с контрагентами и клиентами;
- маркетинговая организация – к сведениям о порядке, способах и системе ценообразования в организации;
- рекрутинговая организация – к персональным сведениям будущих сотрудников;
- посредник, которому поручили продать или купить товар, – к информации о коммерческих планах.

Есть два документа, которые ограничат контрагента в желании распространить конфиденциальную информацию:

- соглашение о порядке ведения переговоров. Если договора еще нет, стороны могут заключить соглашение о порядке ведения переговоров (п. 5 ст. 434.1 ГК РФ);
- соглашение о неразглашении конфиденциальной информации – если стороны договорились заключить или уже заключили договор.

Сторона, которая получила конфиденциальную информацию в ходе переговоров о заключении договора, обязана:

- не раскрывать эту информацию;
- не использовать ее ненадлежащим образом для своих целей.

Обязанность не раскрывать информацию и не использовать ее не зависит от того, будет ли заключен договор.

Такое правило установила часть 4 статьи 434.1 ГК РФ. Оно также соответствует Принципам международных коммерческих договоров УНИДРУА (см. ст. 2.16) [38].

Виновная сторона должна возместить другой убытки, которые возникли из-за того, что она раскрыла конфиденциальную информацию или использовала для своих целей (п. 4 ст. 434.1 ГК РФ). Однако это правило не применяется к контрагентам-гражданам – их признают потребителями по Закону РФ «О защите прав потребителей» (п. 6 ст. 434.1 ГК РФ).

Стороны вправе установить неустойку за разглашение конфиденциальной информации, которую получили в ходе переговоров (п. 5 ст. 434.1 ГК РФ).

В ситуации, когда стороны договорились заключить или заключили договор, стороны вправе заключить Соглашение о неразглашении конфиденциальной информации и указать в нем, например, ответственность в виде штрафов. Соглашение заключают в простой письменной форме (ст. 161 ГК РФ).

Стороны вправе установить как двустороннее обязательство по неразглашению так и обязательство одной стороны. В таком соглашении раскрывающая сторона доверяет информацию другой. Обязательства берет на себя только одна сторона (принимающая).

Лицо, которое взяло на себя обязательство не разглашать чужие сведения, должно уведомить о заключенном соглашении своих сотрудников, которые имеют доступ к информации. Сотрудники возьмут на себя обязательство относиться к конфиденциальной информации контрагента как

к конфиденциальной информации организации, в которой они работают. Обычно в Положении о коммерческой тайне указано, что сотрудник обязуется не разглашать сведения, которые составляют коммерческую тайну контрагентов организации-работодателя.

Сегодня информация персонального характера все чаще рассматривается «как экономически выгодный товар и как источник власти» [27, с. 6]. Между тем, информационная сфера представляет собой одно из важнейших направлений реализации интересов личности. А интересы личности, в свою очередь, в совокупности с интересами государства и общества в информационной сфере составляют информационную безопасность Российской Федерации.

ФЗ «О персональных данных» представляет собой важную попытку создать основы межотраслевого регулирования отношений, возникающих в сфере оборота персональных данных. Однако, процесс формирования нормативной базы, регулирующей оборот персональных данных сегодня находится лишь на стадии становления, о чем свидетельствует.

Максимальный штраф за неправильную работу с персональными данными – 75 тыс. руб. (ст. 13.11 КоАП РФ). В рамках одной проверки Роскомнадзор может обнаружить несколько разных нарушений и назначить штраф за каждое.

Как показывает практика, организации обрабатывают персональные данные физических лиц, которые получает из трех источников: от работников, с сайта, от контрагентов и клиентов при личном контакте.

Оператор вправе обрабатывать персональные данные с согласия субъекта персональных данных. В зависимости от того, кто и как передает данные оператору, возможны три варианта действий.

Первый вариант: гражданин – не работник передает персональные данные в бумажном виде (например, клиент оформляет договор в офисе). В таком случае согласие стоит оформить отдельным бланком. Рекомендуется получить письменное согласие, даже когда закон не требует письменную

форму. В случае спора именно оператор должен доказывать, что субъект дал согласие на обработку данных (ч. 3 ст. 9 ФЗ о персональных данных). Письменный документ будет служить доказательством такого согласия.

Есть случаи, когда оператор обязан получить письменное согласие (ч. 4 ст. 9 ФЗ о персональных данных). Так, необходимо взять письменное разрешение субъекта персональных данных, чтобы:

- обрабатывать специальные категории персональных данных;
- принимать решения на основе исключительно автоматизированной обработки персональных данных;
- включать сведения в общедоступные источники;
- обрабатывать биометрические персональные данные;
- передавать данные за границу;
- обрабатывать данные ребенка;
- размещать сведения о долгах в подъезде дома.

Второй вариант: гражданин – не работник передает персональные данные в электронном виде через сайт.

При этом стоит учитывать, что к письменному разрешению приравнивается электронная подпись. Согласием считается, если субъект персональных данных сам поставил подпись на документе в бумажном виде или подписал электронный документ электронной подписью (ч. 4 ст. 9 ФЗ о персональных данных).

Согласие можно оформить на сайте как документ, который будет называться «Согласие на обработку персональных данных». Это самый распространенный вариант. Он подойдет для всех случаев, когда организация или предприниматель через свой сайт только собирают контактные данные и информируют о своих товарах или услугах.

Также можно разместить на сайте более подробный документ с названием «Пользовательское соглашение между владельцем и пользователем сайта».

Этот вариант подойдет для тех случаев, когда доступ к сайту – и есть та услуга, которую покупает или бесплатно получает при регистрации пользователь. Пользовательское соглашение позволяет заранее урегулировать возможные конфликты, связанные с тем, какой объем услуг и в каком порядке будет получать пользователь. Кроме того, этот вариант подойдет, если физические лица размещают на сайте организации или предпринимателя какую-либо информацию от своего имени. Пользовательское соглашение позволит владельцу сайта модерировать такую информацию.

Третий вариант: сотрудник передает персональные данные в рам-ках трудовых отношений.

Передача данных – это одно из действий, которые входят в понятие обработки данных (п. 3 ст. 3 Закона о персональных данных). Чтобы обрабатывать персональные данные сотрудника, необходимо получить на это согласие.

Из вышеуказанного правила есть исключения. Так, работодателю не нужно согласие работника, чтобы передать информацию о нем.

Во-первых, госорганам, в силу закона.

Существуют два случая, когда работодатель обязан передать данные госорганам.

Работодатель обязан выполнять свои текущие обязанности (п. 2 ч. 1 ст. 6 ФЗ о персональных данных). Работодатель вправе передавать персональные данные сотрудника без его согласия, когда это необходимо, чтобы выполнить обязанности, которые возложил на работодателя закон.

Работодатель обязан ответить на запрос суда, правоохранительного или иного госоргана (п. 3–4 ч. 1 ст. 6 ФЗ о персональных данных).

Во-вторых, третьим лицам в экстренной ситуации.

Работодатель вправе сообщать персональные данные работника третьей стороне без его согласия в двух ситуациях.

– чтобы предупредить угрозу жизни и здоровью работника. Закон прямо разрешает не получать согласие работника, когда необходимо сообщить персональные данные третьей стороне, чтобы предупредить угрозу жизни и здоровью работника (абз. 2 ст. 88 ТК РФ);
– при несчастном случае. Работодатель обязан немедленно сообщить в организации, которые должны знать о несчастном случае. Если произошел тяжелый несчастный случай, в том числе со смертельным исходом, то необходимо проинформировать родственников пострадавшего (абз. 5 ст. 228 ТК РФ). Перечень органов и сроки, в которые необходимо их оповестить, установила статья 228.1 ТК РФ. Например, необходимо сообщить в местную прокуратуру и территориальное отделение Роструда.

В-третьих, банку для оформления зарплатных карт.

Работодатель вправе передавать данные работника в банк для начисления зарплаты без согласия работника в трех случаях:

– работник и банк напрямую заключили договор на выпуск банковской карты;
– работник выдал доверенность работодателю на представление своих интересов при заключении договора с банком на выпуск зарплатной карты и ее последующем обслуживании.
– работник подписал коллективный договор, в котором указано, что зарплату выплачивают исключительно на банковскую карту.

Есть еще одна ситуация, когда согласие не требуется, – в случае, если при приеме на работу сотрудник соглашается с тем, что зарплату будут выплачивать только на банковскую карту. Работник выражает согласие тем, что подписал трудовой договор и ознакомился с локальными документами организации, которые предусмотрели выплату зарплаты именно на банковскую карту. В этом случае обработку данных предусматривает трудовой договор, за выполнение обязанностей по которому сотрудник

получает зарплату на банковскую карту. Работодатель действует в интересах самого сотрудника в рамках заключенного с ним договора (п. 2 ч. 1 ст. 6 Закона о персональных данных).

Если же трудовой договор и локальные документы организации предусматривают возможность выбрать способ получения зарплаты, то работодатель должен получить согласие. Согласие необходимо получить и в том случае, если способ получения зарплаты не указали.

В-четвертых, профсоюзу в рамках его компетенции.

Профсоюзы вправе получать любую информацию по социально-трудовым вопросам бесплатно и беспрепятственно. Такие правила установила часть 1 статьи 17 и часть 1 статьи 19 Федерального закона «О профессиональных союзах, их правах и гарантиях деятельности» [71].

Роскомнадзор указал, что согласие работника на передачу данных в профсоюз не требуется (абз. 5 п. 4 Разъяснений Роскомнадзора). При этом «представители профессионального союза, получившие... персональные данные работника, обязаны соблюдать требования конфиденциальности и безопасности... а также обеспечить их использование только в целях, для достижения которых они были предоставлены» (письмо Роскомнадзора от 27 июня 2011 г. № ШР-13444 [28]).

В-пятых, третьим лицам в связи с исполнением работником должностных обязанностей

Следует рассмотреть примеры ситуаций, когда работодатель передает персональные данные сотрудника в связи с исполнением его должностных обязанностей

Сотрудник уезжает в командировку.

При командировке секретарь или иной сотрудник вынужден передавать персональные данные командированного сотрудника, чтобы, например, приобрести билеты, забронировать гостиничный номер (ч. 5–5.2 ст. 11 Федерального закона «О транспортной безопасности» [69]).

Сотруднику дали доступ в Интернет. Все работодатели, включая предпринимателей, должны передавать провайдеру список сотрудников, у которых есть доступ в Интернет на рабочем месте.

Руководитель организации или предприниматель обязаны заверить этот список и обновлять его не реже одного раза в квартал. Так установил пункт 22 (1) Правил оказания телематических услуг связи [34].

Сотруднику дали доступ к телефону. Все работодатели, включая предпринимателей, должны передавать оператору телефонной связи список лиц, которые используют телефон на рабочем месте. Руководитель организации или предприниматель обязан заверить этот список и обновлять его не реже одного раза в квартал. Такую обязанность абонент и оператор должны включить в договор между собой.

В-шестых, неограниченному кругу лиц через Интернет. По общему правилу работодатель не вправе без согласия сотрудника публиковать его данные в Интернете, в том числе на корпоративном сайте.

Однако есть исключение – случаи, когда работодатель обязан публично размещать персональные данные работников, в том числе в Интернете (абз. 1 п. 1 Разъяснений Роскомнадзора):

- медицинская организация обязана информировать граждан в доступной форме, в том числе с использованием Интернета, о медицинских работниках, об уровне их образования и об их квалификации (п. 7 ч. 1 ст. 79 ФЗ «Об основах охраны здоровья граждан в РФ»);
- образовательная организация обязана разместить на официальном сайте информацию о персональном составе педагогов. Например, необходимо указать: уровень образования, квалификацию, опыт работы, ученое звание и другие данные;
- госорганы обязаны публиковать в Интернете сведения о руководителях (ст. 13 Федерального закона «Об обеспечении

доступа к информации о деятельности государственных органов и органов местного самоуправления» [70]).

- госорганы должны размещать на официальных сайтах информацию о доходах и об имуществе широкого круга должностных лиц, их супругов и несовершеннолетних детей (ч. 6 ст. 8 Федерального закона «О противодействии коррупции» [73]).

Одним из важнейших институтов в сфере обработки персональных данных является их обезличивание. Согласно п. 9 ст. 3 ФЗ о персональных данных: «Обезличить данные значит сделать невозможным без использования дополнительной информации определение принадлежности персональных данных конкретному человеку».

Организация обезличивает данные в двух случаях:

- компания предпочла обезличивать данные, а не уничтожать их. Оператор обязан уничтожить либо обезличить персональные данные, когда достигнет целей обработки или потеряет интерес к этим целям. Иное может предусмотреть только федеральный закон (ч. 7 ст. 5 ФЗ о персональных данных);
- обязанность обезличивания установлена законом.

В заключение рассмотрения во второй главе выпускной квалификационной работы организационно-правового обеспечения информационной безопасности, следует сделать следующие выводы.

Во-первых, организационные основы обеспечения информационной безопасности конкретизированы в пунктах 10-29 Доктрины информационной безопасности РФ, в которых обозначены основные сферы общественных отношений, включающие организация вооруженной защиты Российской Федерации, борьбы с проявлениями терроризма и экстремизма, контрразведывательной деятельности, сведениями, составляющими государственную тайну, неприкосновенности частной жизни, защиты персональных данных физических лиц и др. Исходя из перечисленных основных сфер общественной жизни, а также учитывая положения п.33

Доктрины информационной безопасности, можно выделить перечень органов, составляющих организационную основу информационной безопасности. На уровне федеральных органов государственной власти организационную основу информационной безопасности составляют: Президент РФ, органы исполнительной власти, органы законодательной и судебной власти, а также Центральный Банк РФ и органы власти субъектов Федерации и органы местного самоуправления.

Во-вторых, информационная безопасность обеспечивается и коммерческими структурами, что связано с необходимостью обеспечения конфиденциальной информации. В основе конфиденциальности лежит идея о том, что конкретная информация не должна быть доступна тем, кто ее не должен видеть. Все виды деловой и личной информации создаются, хранятся и обмениваются. Информация может быть сведениями о продажах, личными и персональными данными, маркетингом, счетами или многими другими документами. Для большинства из этих типов информации нет завышенных требований к конфиденциальности или секретности. Например, существует информация, которая не является критически важным секретом, допустим, если бы общественности стала известна информация о том, сколько компания тратит на электричество или водоснабжение. И, наоборот, для любого бизнеса, осуществляющего крупномасштабные операции с информацией о кредитных картах клиента в качестве платежа либо информация о персональных данных клиента чрезвычайно важно защитить.

Глава 3 Проблемы и практика совершенствования системы обеспечения информационной безопасности

3.1 Практика противодействия приоритетным источникам угроз информационной безопасности

Рассмотрев в предыдущей части настоящей работы вопросы обеспечения информационной безопасности субъектами коммерческой деятельности, следует сделать вывод о том, что в сфере электронной коммерции действующее российское законодательство не способно обеспечить защиту интересов как юридических, так и физических лиц [43]. Более того, сложившаяся ситуация позволяет говорить о том, что законодательная власть становится реальным источником угроз экономической безопасности государства и его граждан.

Указанное обстоятельство подтверждается наличием существенных недочетов в целом ряде законодательных актов. И, в первую очередь, здесь идет речь о законах, предусматривающих использование механизма досудебной блокировки электронных ресурсов.

Возможность злоупотребления указанным механизмом блокировки позволила недобросовестным предпринимателям беспрепятственно чинить помехи конкурентам [21], а новые ограничения, сопряженные с внедрением в российское законодательство положений о локализации персональных данных [44] и норм «права на забвение» [22], лишь увеличили число потенциальных угроз любой деятельности, осуществляемой посредством сети Интернет.

Здесь нужно сказать, что главным образом в результате того, что в законодательных актах, описывающих порядок и условия его применения, абсолютно не учитывается специфика технического обеспечения электронной коммерции. В связи с этим, чтобы разобраться в первопричине

сложившейся ситуации, нам потребуется ознакомиться с рядом технических тонкостей и определений.

Например, адрес rta.customs.ru говорит о том, что официальный сайт Российской таможенной академии размещен в сегменте электронных ресурсов таможенного ведомства, выделенном в доменной зоне Российской Федерации.

Тем не менее, в основе системы доменных имен продолжает лежать использование IP-адресов, указывающих на каком сервере следует искать ту или иную Интернет-страницу. Здесь следует уточнить, что в роли сервера может выступать программная или аппаратно-программная вычислительная система, предназначенная для предоставления услуг в автоматическом режиме. При этом на физическом уровне роль сервера может выполнять целая группа специальных устройств, объединенных на логическом уровне в одно виртуальное вычислительное устройство, использующее один IP-адрес.

Соответствие между IP-адресом сервера и удобным для запоминания адресом в системе доменных имен устанавливается администратором доменного имени. В большинстве случаев, в роли такого администратора выступает непосредственный владелец адреса сайта, но на практике, можно встретить ситуации, когда функции администратора выполняет лицо, получившее соответствующие полномочия от непосредственного владельца домена.

Администратор домена может указать в качестве соответствия любой IP-адрес, включая несуществующий. На практике это может потребоваться при переносе программной составляющей сайта с одного сервера на другой. Например, для восстановления работоспособности электронного ресурса, в случае выявления неполадок используемого серверного оборудования.

В Таким образом, попадание в список подлежащих блокировке электронных ресурсов хотя бы одного доменного имени, указывающего на IP-адрес того или иного сервера, неизбежно приведет к одновременной блокировке всех сайтов, в настройках которых установлена ассоциация с его

IP-адресом. К числу наиболее известных примеров такого развития событий можно привести нашумевший прецедент с блокировкой сайта по адресу drugspace.info, повлекший за собой блокировку 440 других сайтов, использовавших в своей работе IP-адрес того же сервера.

Данный прецедент получил весьма широкую огласку еще в 2013 году. При этом, он примечателен не только числом безосновательно заблокированных электронных ресурсов, но и тем, что среди них оказался официальный сайт международной компании «Group-IB», специализирующейся на борьбе с киберпреступностью и предоставляющей услуги по выявлению и предотвращению различных типов угроз в сети Интернет.

В связи с указанной спецификой, к электронным ресурсам данной компании ежедневно отправляют запросы множество других онлайн-сервисов, заинтересованных в своевременном выявлении киберугроз. Таким образом, блокировка ресурсов компании «Group-IB» может привести к возникновению дополнительных перебоев в работе электронных ресурсов других компаний. Например, в 2016 году обращение к электронному ресурсу по адресу ibjs.group-ib.ru можно обнаружить при загрузке страницы входа в личный кабинет пользователя сервиса «Сбербанк.Онлайн».

Подводя итог вышесказанному можно прийти к выводу, что блокировка запрещенных ресурсов по IP-адресу на практике оказывается далеко не самым эффективным решением. В связи с этим, имеет смысл уделить внимание рассмотрению других способов блокировки и, в первую очередь, способу, основанному на использовании доменных имен.

В первом приближении способ блокировки запрещенных ресурсов по доменному имени может показаться более перспективным, поскольку в отличие от IP-адреса одно доменное имя указывает на один электронный ресурс. Однако, учитывая ранее изложенные особенности функционирования системы доменных имен, становится понятно, что в случае блокировки доменного имени rkn.gov.ru (адрес официального сайта Роскомнадзора),

окажутся заблокированными и все входящие в него поддомены. Например, адреса 398-fz.rkn.gov.ru и eais.rkn.gov.ru (адреса списков запрещенных ресурсов).

Таким образом, можно констатировать, что использование блокировки по доменному имени ставит под угрозу все проекты, предполагающие активное использование адресации с применением поддоменов. И, в первую очередь, это угрожает сервисам, предоставляющим услуги по принципу SaaS (от англ. software as a service).

Данная модель предоставления услуг подразумевает, что в рамках оказания услуги клиенту предоставляется доступ к шаблонному электронному ресурсу, разработанному и настроенному специально под условия решения какой-то узкоспециализированной задачи. Большинство таких сервисов специализируется на предоставлении платформы для ведения электронной коммерции, онлайн-бухгалтерии и онлайн-дневников. Стоит ли говорить, что в нынешнюю эпоху тотальной информатизации, число таких сервисов неуклонно растет.

Рассмотренных примеров уже вполне достаточно, чтобы прийти к выводу о том, что описанные типы блокировки не эффективны, поскольку их применение несет угрозу чрезмерного блокирования и, как следствие, угрозу нарушения работоспособности легальных электронных ресурсов.

Гораздо более рационально выглядит способ блокировки запрещенной информации с использованием конкретных адресов интернет-страниц, содержащих запрещенные материалы. Здесь нужно уточнить, что говоря об адресе конкретной страницы в компьютерной сети, традиционно используют аббревиатуру URL (от англ. Uniform Resource Locator – унифицированный адрес ресурса).

Блокировка по URL и позволяет осуществлять точечное ограниче-ние доступа к запрещенной информации, не нарушая при этом общую работоспособность электронных ресурсов. Однако, на практике такую

блокировку предпочитаю не использовать, поскольку владелец запрещенного ресурса может легко избежать блокировки, например:

- изменив URL страницы с запрещенной информацией;
- организовав доступ к информации с использованием «одноразовых» URL [46, с. 80].

Но существует и еще один способ точечного ограничения доступа к запрещенной информации, подобно блокировке по URL позволяющий осуществлять блокировку конкретной информации, не прибегая к блокировке всего сайта. В основе данного способа лежит применение технологии DPI (от англ. Deep Packet Inspection). Использование данной технологии подразумевает глубокий анализ всех передаваемых провайдером пользователю данных, что, в свою очередь, позволяет превентивно исключить практически все известные способы обхода блокировок электронных ресурсов.

Представляется очевидным, что именно эта технология была бы наиболее эффективна в рамках реализации механизма досудебных блокировок, поскольку она позволяет надежно блокировать доступ к запрещенной информации, не ставя под угрозу работу других электронных ресурсов. Однако, применяемые при использовании DPI алгоритмы глубокого анализа, противоречат отдельным положениям действующего законодательства о порядке обработки персональных данных, а высокая стоимость внедрения и ресурсоемкость ее последующей эксплуатации сделали применение данной технологии абсолютно невыгодным для операторов.

В связи с этим большинство операторов предпочли воспользоваться отсутствием в законодательстве конкретных указаний на технологию, которую необходимо применять при осуществлении досудебных блокировок запрещенной информации. Эти операторы отдали предпочтение способу блокировки по IP.

Такое положение вещей открыло широкий простор для злоупотреблений. В связи с тем, что действующее законодательство совершенно не предусматривает способа, который мог бы использоваться администраторами безосновательно заблокированных сайтов для оперативного обжалования неправомерных блокировок в досудебном порядке, позволяет гарантированно нарушить работоспособность электронного ресурса конкурента на несколько дней или даже недель.

В реалиях действующего законодательства существует лишь два легальных механизма противодействия такой неправомерной блокировке. Наиболее эффективным из этих способов, представляется перенос электронного ресурса на другой сервер. Данный способ представляется весьма ресурсоемким и несет угрозу нарушения работоспособности в случае повреждения файлов сайта при переносе. При этом такой способ эффективен лишь до тех пор, пока злоумышленник не обнаружит факт «переезда» и не укажет в настройках запрещенного ресурса IP-адрес нового сервера.

Другой путь выхода из под неправомерной блокировки представляет судебное разбирательство с оператором связи, блокирующим доступ к ресурсу, по факту клеветы (данное основание для обращения в суд возможно, поскольку используемые операторами страницы-«заглушки», информируют пользователей о том, что ресурс содержит запрещенную информацию), упущенной прибыли (поскольку из-за действий оператора ресурс теряет посетителей) и сопутствующих затрат. Однако на практике данный способ представляется совершенно неэффективным, поскольку процедура разбирательств может растянуться на долгие годы, а суммы компенсаций, назначаемых при рассмотрении таких дел, как правило, ничтожно малы.

Предвидя возможность внесения в действующее законодательство поправок, обязывающих их использовать точечные способы блокировки запрещенной информации, российские провайдеры разработали технологию, сочетающую механизмы блокировки по URL и IP. Как следует из информации на сайте Роскомнадзора [2], внедрение данной технологии не

требует таких существенных затрат как переход на дорогостоящую технологию DPI. Однако важно понимать, что до тех пор, пока сроки перехода российских операторов на технологию точечной блокировки запрещенной информации не будут установлены законодательно, угроза необоснованной блокировки электронных ресурсов не будет гарантированно устранена.

Как можно видеть, объем разъяснений, потребовавшихся для обоснования возможности использования механизма досудебной блокировки электронных ресурсов оказался не столь велик, что выявляет пробелы правового регулирования и необходимость их восполнения.

3.2 Совершенствование системы информационного обеспечения деятельности органов государственной власти

Цифровые технологии, являясь средством и инструментом регулирования общественных отношений кардинально меняют не просто формы и способы взаимодействия общественных институтов, но фундаментально преобразовывают институции, существовавшие на протяжении многих десятков лет. Так, цифровые технологии сделали возможным открытый прямой диалог между властью и обществом в противовес ситуации, когда управляющее публичное воздействие оказывалось практически без обратной связи, в уведомительном порядке. Цифровые технологии лежат в основе сбора, обработки, хранения и быстрого обмена большими массивами данных, которые ложатся в основу планирования, организации и реализации управления во всех сферах деятельности. Цифровые технологии позволяют отказаться от человеческого ресурса в тех областях, где те же самые задачи могут быть решены компьютером, причем более успешно.

Цифровые технологии позволяют создавать носители информации, более эффективные, чем традиционные бумажные. К преимуществам новых носителей информации относится:

- больший объем, вместимость;
- возможность вносить исправление, редактировать;
- компактность;
- отпадение фактора удаленности, поскольку документы на новейших носителях можно пересылать в любую точку планеты;
- возможность интеграции и т.д.

Масштабное распространение цифровых технологий вызывает трансформацию общественных отношений не только в сфере социальных связей или коммерческих взаимоотношений, но и в области публично-управленческих отношений.

Поскольку процесс цифровизации функционально носит вспомогательный или обслуживающий характер, соответственно информационное обеспечение управленческих отношений будет иметь характер и структуру этих отношений, обеспечивая движение информации, обмен ею между структурными компонентами и участниками отношений.

Говоря об информационном обеспечении региональных органов власти, следует помнить о структурном построении государственных органов власти, которые выстроены в соответствии с принципом федерализма, а также отраслевыми принципами. Это означает, что региональные органы власти носят подчиненный характер по отношению к федеральным органам власти и являются относительно самостоятельным их продолжением на местах. А также региональные органы власти выстраиваются в соответствии с принципами функционального разделения полномочий и необходимости решения конкретных хозяйственно-экономических и социальных задач на местах, т.е. в регионах.

Соответственно, информационное обеспечение региональных органов власти направлено на передачу и получение информации от федеральных

органов власти к региональным и обратно, а также циркулирование информации между структурными элементами в рамках решения поставленных задач и распределения полномочий.

Информационное обеспечение деятельности региональных органов исполнительной власти должно решать следующие задачи:

- возможность передачи сведений в полном объеме без потерь и в кратчайшие сроки;
- возможность обеспечения конфиденциальности, коммерческой и государственной тайны;
- обеспечение законодательства в сфере личных данных;
- возможность обработки, хранения и анализа больших массивов данных;
- возможность интеграции массивов данных, полученных от федеральных органов государственной власти, от региональных органов исполнительной власти, от муниципальных органов.

Для решения данных задач должны учитываться факторы организационно-правового обеспечения процесса информатизации, материального обеспечения, финансово-экономического, а также программного обеспечения.

Внедрение цифровых технологий процесс многоаспектный и сопровождается помимо непосредственного технического, научно-понятийным, правовым и организационным обеспечением. Однако в данной сфере необходимость разработки и сопровождения такого явления как цифровые технологии не находит достаточного отклика.

Для понимания пробелов, существующих в научной сфере и в правовом поле, прежде всего, определим понятие и сущность цифровых технологий.

Согласно ГОСТ Р 33.505-2003 под цифровыми технологиями понимаются технологии, использующие электронно-вычислительную аппаратуру для записи кодовых импульсов в определенной

последовательности и с определенной частотой [8]. Цифровые технологии – это прием преобразования обработанной информации из базы данных путем цифрового кодирования при входе и передаче на выход для решения разнообразных задач в короткие отрезки времени.

Универсальность цифровых технологий позволяет использовать их в самом широком спектре специализированной техники, начиная от персональных компьютеров и заканчивая игровыми автоматами, в робототехнике, измерительных приборах, радио- и телекоммуникационных устройствах и многих других устройствах, а также в рамках автоматизации различных процессов.

В целом, цифровые технологии являются элементом более широкого понятия информационных технологий, представляя собой способ шифрования поступающих и исходящих информационных данных, при этом необходимо учитывать, что цифровые технологии используются в ситуации сбора, хранения, обработки, передачи и использования информации.

Под регламентацию ФЗ «Об информации, информационных технологиях и о защите информации» подпадает не только информация, но и информационные технологии, которыеявляются более широким и общим понятием по отношению к цифровым технологиям. Законодатель определяет информационные технологии как «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов» с логической точки зрения охватывает также применение цифровых технологий, которые по своей сути являются способом обработки и предоставления информации. Такой подход был бы оправдан в ситуации стабильного и поступательного развития отношений. Однако в быстроменяющихся условиях, в ситуации, когда технологии являются прорывными, когда социально-экономические, общественные, государственно-правовые последствия внедрения той или иной технологии могут оказаться непредсказуемыми, законодатель должен действовать, если не на опережение технологического регулирования, то

хотя бы максимально сокращая дистанцию между внедрением технологии в общественную жизнь и обеспечением безопасности общественны отношений в рамках применения данной технологии.

Обращение к зарубежному опыту регулирования цифровых технологий приводит к лидеру в области построения Цифровой экономики – Европейскому союзу, который в последние годы обновляет правовую основу регулирования информационных и цифровых технологий. С этой целью страны ЕС внедряют Европейскую цифровую стратегию (The European Digital Strategy) и Стратегию создания Единого цифрового рынка ЕС (Digital Single Market) [83]. Стратегия ориентирована на расширение доступа граждан и организаций к цифровому пространству, регулирование и обеспечение безопасности цифровой среды, создание институциональных условий для поступательного развития экономики и общественных отношений на основе цифровых технологий.

В контексте обеспечения безопасности цифровых технологий и сохранения контроля человека над всеми технологическими решениями, что является принципиальным положением Стратегии, была принята Директива (ЕС) 2016/1148 Европейского парламента и Совета от 6 июля 2016 года «О мерах по обеспечению высокого общего уровня безопасности сетевых и информационных систем на всей территории Союза» [82]. Директива разделяет понятие информационных и цифровых (сетевых) технологий, рассматривая вопросы обеспечения безопасности их применения как важнейшую задачу государств при развитии Цифровой экономики.

Таким образом, европейские законодатели считают необходимым и целесообразным выделение цифровых технологий в самостоятельный предмет регулирования при обеспечении безопасности применения информационных технологий.

В настоящее время цифровые технологии, хотя формально и остаются в рамках законодательного определения как способ обработки и выдачи информации, тем не менее, охватывают более обширные общественные

отношения, нежели оборот, использование и хранение информации. Более того, в ближайшие годы эти отношения будут только усложнятся, тогда как возможности их правового обеспечения будут не сохраняться на прежнем уровне, а сокращаться и ограничиваться.

С учетом сказанного важно внести в законодательство в качестве самостоятельного предмета правового регулирования цифровые технологии, обеспечивая, таким образом, возможность регулирования данного направления развития технологий.

Возвращаясь к вопросу об организационно-правовом факторе информационного обеспечения деятельности региональных органов исполнительной власти, к нему следует отнести построение схемы обмена информации и распределения полномочий между участниками информационного обмена.

В качестве дополнительного фактора следует также назвать наличие компетентных сотрудников, имеющих соответствующую квалификацию, которая позволяет сопровождать процесс информатизации и информационного обеспечения деятельности органов исполнительной власти конкретного региона.

Материальный фактор подразумевает обеспеченность региональных органов исполнительной власти необходимым оборудованием, которое отвечает потребностям информационного сопровождения.

Финансово-экономический фактор информационного обеспечения и сопровождения подразумевает наличие бюджетных средств, необходимых для информатизации управленческого процесса. Следует отметить, что на федеральные программы информатизации управления могут выделяться бюджетные средства федерального центра, однако зачастую на информационное обеспечение управления должны выделяться именно региональные бюджетные средства.

Немаловажным фактором является используемое программное обеспечение, которое должно отвечать потребностям и задачам деятельности

как всей системы региональных органов исполнительной власти, так и отдельных их подразделениям и структурным единицам. Пи разработке такого программного обеспечения необходимо отталкиваться от двух посылок:

- возможность учета единых потребностей и задач исполнительных органов власти в регионах для последующего масштабирования программного обеспечения и использования его в других регионах;
- возможность подключения специальных опций, учитывающих узкоспециализированные задачи конкретных исполнительных органов, что позволит надстраивать программное обеспечение для конкретных органов исполнительной власти в соответствии с их потребностями, планами и задачами.

Это позволит сократить бюджетные затраты на информационное обеспечение деятельности региональных органов исполнительной власти.

Исследование организации управления на цифровых платформах позволило выявить серьезную проблему в данной сфере, связанную с вопросом придания юридической силы документам на новейших носителях информации. Поскольку вся деятельности региональных органов исполнительной власти выражается в документальной форме, данный вопрос не является праздным. Так, поскольку документы обеспечивают управляющую, производственную и иные виды деятельности, значительная их часть имеет юридическую силу, которая без обязательного подтверждения не может быть реализована.

И если традиционные документационные носители обеспечивались печатью, подписью, факсимиле, как способами придать им юридическую силу, то в отношении новейших носителей информации были разработаны иные способы и средства, подтверждающие их действительность и юридическую силу, если таковая имеется.

Правовую основу придания юридической силы новейшим носителям информации составляют следующие акты, регулирующие правоотношения в

сфере электронного документооборота и вопросы, связанные с применением электронной подписи:

- ст.ст. 160, 434 ГК РФ;
- ст. 11 «Об информации, информационных технологиях и о защите информации», ст. 11;
- ст. 9 Федерального закона «О бухгалтерском учете» [67];
- Федеральный закон «Об электронной подписи» [66];
- Приказ Минфина России от 05.02.2021 г. № 14н «Об утверждении Порядка выставления и получения счетов-фактур в электронной форме по телекоммуникационным каналам связи с применением усиленной квалифицированной электронной подписи» [36];
- Приказ ФНС России от 08.06.2021 N ЕД-7-26/547@ «Об утверждении форматов журнала учета полученных и выставленных счетов-фактур, книги покупок и книги продаж, дополнительных листов книги покупок и книги продаж в электронной форме» [37].

Юридическую силу электронному документу придают подтвержденные полномочия создателя, реквизиты и подлинность. Отметим, что даже суды все больше признают юридическую силу электронных документов.

Полномочия создателя электронного документа подтверждаются должностными инструкциями, приказами и другими документами. То есть лицо должно быть официально уполномочено на создание конкретного электронного документа.

Формат электронного документа — структура содержательной части электронного документа, удобная для хранения и автоматической обработки. Эта структура может быть разной, главное, чтобы программное обеспечение смогло распознать и вывести информацию на экран пользователю.

Оборот цифровых документов, имеющих юридическую силу, подтверждается тем, что электронные документы являются письменными

доказательствами (п. 3 ст. 75 Арбитражного процессуального кодекса Российской Федерации (далее – АПК РФ) [3]).

В условиях большого количества и многообразия форм нарушений при использовании электронной цифровой подписи назрела необходимость внедрения дополнительных механизмов защиты в данной сфере.

В настоящее время актуальны вопросы, связанные с:

– оптимизацией процедур использования электронной подписи (в частности, возможности получения гражданином ключа сертификата электронной подписи удаленно, без личного присутствия – через нотариуса, который должным образом идентифицирует личность);
– совершенствованием нормативно-правовой базы, которая регулирует правоотношения в сфере применения электронной подписи в контексте развития цифровой экономики (речь идет о минимизации рисков мошенничества с электронной подписью и повышении качества работы удостоверяющих центров).

Таким образом, в настоящее время, с учетом распространения и повсеместного использования документов на новейших информационных носителях, остро стоит вопрос обеспечения их подлинности и придания им юридической силы, однако созданный инструмент – цифровая подпись – как показывает практика в настоящее время в недостаточной степени решает поставленные задачи, поэтому практика его развития будет продолжаться и совершенствоваться.

В условиях информатизации регионального управления все большее значение отводится решению задач, связанных с оптимизацией функционирования системы информационных технологий, их взаимоувязывания, создания программных продуктов для обеспечения взаимодействия различных структур в государственном и частном секторе, которые должны обеспечивать высокий уровень технологической безопасности, качественное решение социальных задач, высокую

экономическую эффективность. Решению этих задач способствует создание современной, полнофункциональной и эффективной системы автоматизации учета и диспетчеризации действий управляющих субъектов. При этом создаваемая автоматизированная система должна обладать высокой технологичностью, полнотой функциональности и глубокой синергией.

На сегодняшний день строительство систем телеметрии является одной из приоритетных задач с точки зрения повышения эффективности публичного управления на региональном уровне. Не удивительно, что реализацией такого рода систем занимается большое количество организаций. Однако, с одной стороны, возрастающий объем телеметрии требует все более качественной обработки первичных данных в части очистки и верификации, т. к. с ростом количества поставляемых телеметрией «сырых» данных снижается достоверность и качество оценки состояния системы регионального управления. С другой стороны, высокий уровень фрагментации информационного пространства делает низкоэффективной оценку состояния регионального управления в целом, т. к. отсутствует единое информационное пространство, в котором должны функционировать все заинтересованные субъекты. В результате фрагментации планирование и строительство телеметрии происходит изолированно, исходя из представлений отдельных организаций или органов, без учета уже имеющихся в регионе источников данных, находящихся в ведении других государственных и частных организаций. Это, в свою очередь, затрудняет возможность эффективного анализа собираемой технологической информации. Например, сбор данных от граждан о приоритетном направлении расходования бюджетных средств, оценка эффективности потраченных средств в прошлом бюджетном периоде, анализ данных о поставщиках в интересующей области позволяет сформировать план по расходованию бюджетных средств в следующем периоде с учетом потребностей населения, а также возможности получения качественных товаров и услуг с экономией бюджетных средств. Имея информацию от всех

источников измерений, можно более эффективно планировать работу ведомств и органов региона [17, с. 210].

Таким образом, ввиду отсутствия простых и эффективных инструментов создания единого информационного пространства собираемой технологической информации, наращивание объемов телеметрии в регионе происходит недостаточно эффективно.

Следует рассмотреть возможность внедрения в деятельность региональных органов исполнительной власти на примере внедрения описанной системы. Так, Информационно-мониторинговая управляющая система (ИМУС), позволяет:

- выстраивать планы закупок для государственных и муниципальных нужд с учетом оценки эффективности реализованных в прошлые периоды проектов;
- отслеживать движение бюджетных средств и их эффективное расходование;
- отражать эффективность деятельности (в соответствии с заранее заданными параметрами и критериями) государственных органов, ведомств и управлений;
- получать оперативную информацию о реализации того или иного проекта;
- выявлять сбои во взаимодействии между гражданами и государственными структурами;
- обеспечивать полноценное участие общественности в планировании деятельности государственных органов, контроле и оценке их деятельности;
- выявлять успешный опыт управленческого воздействия и распространять его на иные структурные единицы.

Повышение эффективности и производительности системы связано с развитием ЕИТП на облачной платформе.

Функциональность ЕИТП на облачной платформе заключается в следующем:

- сокращение затрат на разработку новой функциональности за счет единого хранилища данных, единой НСИ, единого окружения;
- простота добавления новой функциональности;
- возможность быстрого подключения сторонних сервисов к единому хранилищу данных;
- возможность использования ресурса сторонних разработчиков для быстрого развития ЕИТП;
- возможность быстрого обновления отчётов и расчётных функций при изменениях нормативной базы организации, отрасли или федерального уровня.

Перспективные планы развития предлагаемой системы должны учитывать следующие факторы:

Во-первых, развитие целесообразно только после перехода на облачную платформу, т.к. реализация, внедрение и поддержка новой функциональности в текущей архитектуре существенно более затратно, чем модернизация ЕИТП и дальнейшее его развитие в совокупности

Во-вторых, развитие функциональности осуществляется:

- в процессе сопровождения в части небольших доработок;
- в рамках отдельного проекта, формируемого на основе концепции развития.

В заключение третьей главы выпускной квалификационной работы можно сделать следующие выводы.

Во-первых, в сфере электронной коммерции действующее российское законодательство не способно обеспечить защиту интересов как юридических, так и физических лиц. Сложившаяся ситуация позволяет говорить о том, что законодательная власть становится реальным источником угроз экономической безопасности государства и его граждан. Указанное обстоятельство подтверждается наличием существенных недочетов в

законах, предусматривающих использование механизма досудебной блокировки электронных ресурсов. Рационально выглядит способ блокировки запрещенной информации с использованием конкретных адресов интернет-страниц, содержащих запрещенные материалы. Но существует и способ точечного ограничения доступа к запрещенной информации, подобно блокировке по URL позволяющий осуществлять блокировку конкретной информации, не прибегая к блокировке всего сайта. В основе данного способа лежит применение технологии DPI. Использование данной технологии подразумевает глубокий анализ всех передаваемых провайдером пользователю данных, что, в свою очередь, позволяет превентивно исключить практически все известные способы обхода блокировок электронных ресурсов.

Во-вторых, цифровые технологии сделали возможным открытый прямой диалог между властью и обществом в противовес ситуации, когда управляющее публичное воздействие оказывалось практически без обратной связи, в уведомительном порядке. Цифровые технологии лежат в основе сбора, обработки, хранения и быстрого обмена большими массивами данных, которые ложатся в основу планирования, организации и реализации управления во всех сферах деятельности. Данная система обеспечивает сбор и обработку получаемых данных во всех областях функционирования государственных региональных властей, начиная с процессов бюджетирования и заканчивая оценкой эффективности расходования бюджетных средств отдельно взятой организацией. Повышение прозрачности управляющего воздействия повышает информационную и публичную безопасность региона, снижает уровень коррупционности, повышает эффективность расходования бюджетных средств, повышает удовлетворенность граждан от участия в управлении делами региона.

Заключение

В заключительной части необходимо подвести итоги и сделать выводы.

Констатируя изложенное в настоящей выпускной квалификационной работе, необходимо сделать следующие выводы.

Во-первых, информационная безопасность является составной частью системы национальной безопасности Российской Федерации, имеющая собственное содержание и представляющая собой сложную, многоаспектную категорию. Под информационной безопасностью понимается состояние определенного объекта и деятельность, направленная на организацию обеспечения состояния защищенности данного объекта.

Во-вторых, правовая основа информационной безопасности обозначена в п. 4 Доктрины информационной безопасности. При рассмотрении правовых механизмов, регулирующих те или иные сферы общественных отношений, как правило, затрагиваются также и нормы международного права, являющиеся составной частью правовой системы Российской Федерации. Нормами международного права установлены стандарты защиты информации, однако без учета индивидуальных особенностей национальных правовых систем. В связи с чем, в сфере информационной безопасности приоритет принадлежит национальному законодательству, что также обусловлено высокой степенью анонимности при реализации угроз информационной безопасности, а также значительным влиянием политических и конъюнктурных факторов и что делает невозможным эффективное применение международно-правовых механизмов.

В целом, отношения в сфере обеспечения информационной безопасности регулируются не только Конституцией РФ, но и федеральным законодательством Российской Федерации, нормативными правовыми актами регионального значения, муниципального уровня и локальными нормативными актами организаций и предприятий.

Большинство норм федерального значения в части регулирования информационной безопасности содержат положения, нуждающиеся в конкретизации посредством подзаконного нормотворчества. При этом, количество подзаконных нормативных актов в сфере информационной безопасности достигает несколько сотен. В целом, на уровне подзаконного нормотворчества развиваются и конкретизируются отдельные направления регулирования информационной безопасности. Вместе с тем, данные документы носят достаточно общий характер. Дальнейшая конкретизация отдельных правовых механизмов, регулирующих отношения в сфере информационной безопасности, осуществляется на уровне приказов отдельных федеральных органов исполнительной власти. Содержательный аспект информационного обеспечения деятельности региональных органов исполнительной власти отражен в программных и стратегических документах, направленных на развитие цифровой экономики и обеспечение информационной безопасности.

В-третьих, организационные основы обеспечения информационной безопасности конкретизированы в пунктах 10-29 Доктрины информационной безопасности РФ, в которых обозначены основные сферы общественных отношений, включающие организация вооруженной защиты Российской Федерации, борьбы с проявлениями терроризма и экстремизма, контрразведывательной деятельности, сведениями, составляющими государственную тайну, неприкосновенности частной жизни, защиты персональных данных физических лиц и др. Исходя из перечисленных основных сфер общественной жизни, а также учитывая положения п.33 Доктрины информационной безопасности, можно выделить перечень органов, составляющих организационную основу информационной безопасности. Так, на уровне федеральных органов государственной власти организационную основу информационной безопасности составляют: Президент РФ, органы исполнительной власти, органы законодательной и

судебной власти, а также Центральный Банк РФ и органы власти субъектов Федерации и органы местного самоуправления.

В-четвертых, информационная безопасность обеспечивается и коммерческими структурами, что связано с необходимостью обеспечения конфиденциальной информации. В основе конфиденциальности лежит идея о том, что конкретная информация не должна быть доступна тем, кто ее не должен видеть. Все виды деловой и личной информации создаются, хранятся и обмениваются. Информация может быть сведениями о продажах, личными и персональными данными, маркетингом, счетами или многими другими документами. Для большинства из этих типов информации нет завышенных требований к конфиденциальности или секретности. Например, существует информация, которая не является критически важным секретом, допустим, если бы общественности стала известна информация о том, сколько компания тратит на электричество или водоснабжение. И, наоборот, для любого бизнеса, осуществляющего крупномасштабные операции с информацией о кредитных картах клиента в качестве платежа либо информация о персональных данных клиента чрезвычайно важно защитить.

В-пятых, в сфере электронной коммерции действующее российское законодательство не способно обеспечить защиту интересов как юридических, так и физических лиц. Сложившаяся ситуация позволяет говорить о том, что законодательная власть становится реальным источником угроз экономической безопасности государства и его граждан. Указанное обстоятельство подтверждается наличием существенных недочетов в законах, предусматривающих использование механизма досудебной блокировки электронных ресурсов. Рационально выглядит способ блокировки запрещенной информации с использованием конкретных адресов интернет-страниц, содержащих запрещенные материалы. Но существует и способ точечного ограничения доступа к запрещенной информации, подобно блокировке по URL позволяющий осуществлять блокировку конкретной информации, не прибегая к блокировке всего сайта. В основе данного

способа лежит применение технологии DPI. Использование данной технологии подразумевает глубокий анализ всех передаваемых провайдером пользователю данных, что, в свою очередь, позволяет превентивно исключить практически все известные способы обхода блокировок электронных ресурсов.

В-шестых, в последние десятилетия мы можем наблюдать как внедрение информационных технологий в сферу публичного управления переводит значимость технологий с позиции облегчения умственного труда, расширения объемов перерабатываемой информации, возможности оперировать большими данными в сферу имеющую социально-общественное значение, область, которая связана с объединением групп людей, возможностью выражать свою гражданскую позицию и мнение, взаимодействия государственной политики и частных инициатив, объединением граждан, государственных органов и частных организаций во взаимовыгодных проектах, т.е. информационные технологии расширяют потенциал как гражданского общества, так и государственных структур, выводя на новый уровень сферу их общения и взаимодействия.

Российское государство стоит на пути цифровизации публичного управления, для чего созданы необходимые условия, однако говорить об участии граждан в сфере управления, контроле обществом деятельности государственных служащих, повышении прозрачности государственного управления пока рано. Для этого необходимо как расширение доступа граждан к цифровым технологиям, так и изменении подхода к деятельности и ответственности государственных и муниципальных служащих, формировании понимания ответственности и подотчетности их должностей. Техническое обеспечение данного процесса должно дополнить и ускорить прогресс в данной сфере.

Анализ законодательства об открытости информационных данных в деятельности органов государственной власти предоставил возможность

выделить направления реформирования действующего отечественного законодательства по данному вопросу:

- целесообразно создание в России отдельного государственного органа (агентства, службы или ведомства), который бы контролировал доступ к публичной информации;
- необходимо создание на федеральном уровне электронного портала, где каждый гражданин имел бы возможность задавать вопросы публичным лицам, высказывать свои пожелания и предложения и т.д., что в будущем улучшит имидж государственных органов перед обществом и повысит доверие к деятельности органов государственной власти.

Информационное обеспечение деятельности региональных органов исполнительной власти должно решать следующие задачи:

- возможность передачи сведений в полном объеме без потерь и в кратчайшие сроки;
- возможность обеспечения конфиденциальности, коммерческой и государственной тайны;
- обеспечение законодательства в сфере личных данных;
- возможность обработки, хранения и анализа больших массивов данных;
- возможность интеграции массивов данных, полученных от федеральных органов государственной власти, от региональных органов исполнительной власти, от муниципальных органов.

Монополизация информационного обеспечения снижает качество и безопасность деятельности органов исполнительной власти на уровне регионов. Поэтому, с одной стороны, необходимо создавать в этой сфере конкурентную среду, а с другой, обеспечивать деятельность региональных органов исполнительной власти платформами, разработанными на федеральном уровне.

Список используемой литературы и используемых источников

1. Алексенцев А.И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» // Безопасность информационных технологий. 1999. № 1. С. 44-47.

2. Анализ существующих методов управления доступом к Интернет-ресурсам и рекомендации по их применению» [Электронный ресурс]. URL: http://rkn.gov.ru/docs/Analysys_and_recommendations_comments_fin.pdf (дата обращения: 08.09.2022).

3. Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 г. № 95-ФЗ (ред. от 11.06.2022) // Российская газета. 2002. 27 июля. № 137.

4. Блинова И.В., Попов И.Ю. Теория информации. СПб: Университет ИТМО, 2018. 84 с.

5. Большой юридический словарь. / Под ред. А.Я. Сухарева. М.: ИНФРА-М, 2007. 849 с.

6. Васильева М. М. Сетевые информационные технологии во внешнеполитической деятельности // Власть, 2016. Том. 24. № 11. С. 51-55.

7. Голубчиков С.В., Новиков В.К., Баранова А.В Виды профессиональной тайны и ее защита // Гуманитарные, социально-экономические и общественные науки. 2018. №1. С. 1-7.

8. ГОСТ Р 33.505-2003 Единый Российский страховой фонд документации. Порядок создания страхового фонда документации, являющейся национальным научным, культурным и историческим наследием. М.: ИПК Издательство стандартов, 2003 г.

9. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 г. № 14-ФЗ (ред. от 01.07.2021, с изм. от 08.07.2021) // СЗ РФ. 1996. № 5. Ст. 410.

10. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 г. № 51-ФЗ (ред. от 25.02.2022) // СЗ РФ. 1994. № 32. Ст. 3301.

11. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 г. № 230-ФЗ (ред. от 14.07.2022) // СЗ РФ. 2006. № 52 (Ч. 1). Ст. 5496.

12. Добровольская И.А. Понятие «Информационное пространство»: различные подходы к его изучению и особенности // Вестник РУДН. 2014. № 4. С. 36-40.

13. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 г. № Пр-1895) [Электронный ресурс] // СПС КонсультантПлюс (утратила силу).

14. Закон РФ от 05.03.1992 г. № 2446-1 «О безопасности» [Электронный ресурс] // СПС КонсультантПлюс (утратил силу).

15. Закон РФ от 21.07.1993 г. № 5485-1 (ред. от 14.07.2022) «О государственной тайне» // СЗ РФ. 1997. № 41. Ст. 8220-8235.

16. Закон РФ от 27.12.1991 г. № 2124-1 (ред. от 14.07.2022) «О средствах массовой информации» // Российская газета. 1992. 08 февраля. № 32.

17. Карминский А.М. Методология создания информационных систем: Учебное пособие. М.: ИД ФОРУМ: ИНФРА-М, 2012. 340 с.

18. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 г. № 195-ФЗ (ред. от 14.07.2022) // СЗ РФ. 2002. № 1 (Ч. 1). Ст. 1.

19. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) [Электронный ресурс] // Официальный текст Конституции РФ с внесенными поправками от 14.03.2020 опубликован на Официальном интернет-портале правовой информации http://www.pravo.gov.ru, 04.07.2020.

20. Ларченко Д.А. Правовые основы использования цифровых технологий в деятельности органов государственного жилищного надзора // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2018. Том 4. № 3. С. 188-200.

21. Левшин Н.С. Российские законы как инструмент недобросовестной конкуренции в сфере электронной коммерции // Пробелы в российском законодательстве. 2014. № 5. С.110-114.

22. Левшин Н.С. «Право на забвение» в законодательстве России: от предпосылок до первых результатов. В сборнике материалов II Международной научно-практической конференции «Научно-технический прогресс: актуальные и перспективные направления будущего»: в 2-х томах. 2016. С. 254-256.

23. Мотовилова О.В. Основы теории информации. Ростов н/Д, 2021. 95 с.

24. О принятии Первым комитетом Генассамблеи ООН Резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [Электронный ресурс] // Режим доступа: http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/1922990 (дата обращения: 15.09.2022).

25. Основы законодательства Российской Федерации о нотариате (утв. ВС РФ 11.02.1993 г. № 4462-1) (ред. от 14.07.2022) // Российская газета. 1993. 13 марта. № 49.

26. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7). [Электронный ресурс] // СПС КонсультантПлюс.

27. Петросян М. Е., Разумович Н. Н. Информация и личность. Правовые аспекты: Научно-аналитический обзор литературы США. М., 1979. 230 с.

28. Письмо Роскомнадзора от 27.06.2011 г. № ШР-13444 «О результатах рассмотрения обращения» [Электронный ресурс] // СПС КонсультантПлюс.

29. Постановление Правительства РФ от 02.06.2008 г. № 418 (ред. от 17.12.2021) «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации» // СЗ РФ. 2008. № 23. Ст. 2708.

30. Постановление Правительства РФ от 06.07.2015 г. № 676 (ред. от 23.12.2021) «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // СЗ РФ. 2015. № 28. Ст. 4241.

31. Постановление Правительства РФ от 12.10.2020 г. № 1674 (ред. от 30.03.2022) «О проведении эксперимента по созданию, переводу и развитию государственных информационных систем и их компонентов на единой цифровой платформе Российской Федерации «ГосТех»» (вместе с «Положением о проведении эксперимента по созданию, переводу и развитию государственных информационных систем и их компонентов на единой цифровой платформе Российской Федерации «ГосТех») // СЗ РФ. 2020. № 42 (Ч. III). Ст. 6637.

32. Постановление Правительства РФ от 15.04.2014 г. № 313 (ред. от 02.06.2022) «Об утверждении государственной программы Российской Федерации «Информационное общество» // СЗ РФ. 2014. № 18 (Ч. II). Ст. 2159.

33. Постановление Правительства РФ от 15.07.2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении

в органе (организации), обеспечивающем информационную безопасность органа (организации)» [Электронный ресурс] // Официальный интернет-портал правовой информации http://pravo.gov.ru, 19.07.2022.

34. Постановление Правительства РФ от 31.12.2021 г. № 2607 «Об утверждении Правил оказания телематических услуг связи» // СЗ РФ. 2022. № 3. Ст. 579.

35. Постановление Суда по интеллектуальным правам от 16.11.2017 № С01-922/2017 по делу № А33-28905/2016 [Электронный ресурс] // СПС КонсультантПлюс.

36. Приказ Минфина России от 05.02.2021 г. № 14н «Об утверждении Порядка выставления и получения счетов-фактур в электронной форме по телекоммуникационным каналам связи с применением усиленной квалифицированной электронной подписи» [Электронный ресурс] Режим доступа: http://pravo.gov.ru.

37. Приказ ФНС России от 08.06.2021 г. № ЕД-7-26/547@ «Об утверждении форматов журнала учета полученных и выставленных счетов-фактур, книги покупок и книги продаж, дополнительных листов книги покупок и книги продаж в электронной форме» [Электронный ресурс] Режим доступа: http://pravo.gov.ru.

38. Принципы международных коммерческих договоров УНИДРУА 2010 / Пер. с англ. А.С. Комарова. М.: Статут, 2013. 758 с.

39. Распоряжение Правительства РФ от 06.05.2008 г. № 632-р (ред. от 10.03.2009) «О Концепции формирования в Российской Федерации электронного правительства до 2010 года» // СЗ РФ. 2008. № 20. Ст. 2372.

40. Распоряжение Правительства РФ от 27.09.2004 г. № 1244-р (ред. от 10.03.2009) «О Концепции использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года и плане мероприятий по ее реализации» // Российская газета. 2004. 07 октября. № 220.

41. Распоряжение Правительства РФ от 29.12.2014 г. № 2769-р (ред. от 18.10.2018) «Об утверждении Концепции региональной информатизации» // СЗ РФ. 2015. № 2. Ст. 544.

42. Расторгуев С.П. Философия информационной войны. М., 2016. 495 с.

43. Смоленский М., Левшин Н. Актуальные проблемы правового обеспечения предпринимательской деятельности в сети Интернет // Научно-практический журнал «Наука и образование: хозяйство и экономика; предпринимательство; право и управление». 2015. №12 (67). С.135-140.

44. Смоленский М., Левшин Н. Локализация персональных данных граждан РФ как составляющая экономической и национальной безопасности России // Научно-практический журнал «Наука и образование: хозяйство и экономика; предпринимательство; право и управление». 2015. № 2 (69). С.111-114.

45. Смоленский М.Б. Коррупция, терроризм, экстремизм, незаконная миграция и экономическая нестабильность: угрозы национальной безопасности, их социальная составляющая и роль правовой культуры и образования таможенных органов в противодействии им // Научно-практический журнал «Наука и образование: хозяйства и экономика; предпринимательство; право и управление». №1(80). 2017. С. 34-40.

46. Смоленский М.Б. Роль информационного права в обеспечении развития систем информационной безопасности и защиты информации в России как фактора национальной безопасности: гражданско-правовой аспект. Ростов-на-Дону: ООО «Мини Тайп», 2020. 96 с.

47. Снытников А.А. Обеспечение и защита права на информацию. М.: Городец-издат, 2001. 344 с.

48. Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 07.02.2008 г. № Пр-212) // Российская газета. 2008. 16 февраля. № 34 (утратила силу).

49. Стрельцов А.А. Обеспечение информационной безопасности России: теоретические и методологические основы. М.: МЦНМО, 2002. 289 с.

50. Теория информации и информационных процессов / Под общ. ред. В.А. Минаева. Орел: Госуниверситет - УНПК. 2021. 443 с.

51. Трудовой кодекс Российской Федерации от 30.12.2001 г. № 197-ФЗ (ред. от 14.07.2022) // СЗ РФ. 2002. № 1 (Ч. 1). Ст. 3.

52. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ (ред. от 14.07.2022, с изм. от 18.07.2022) // СЗ РФ. 2001. № 52 (Ч. 1). Ст. 4921.

53. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 24.09.2022) // СЗ РФ. 1996. № 25. Ст. 2954.

54. Указ Президента РФ от 01.03.2011 г. № 248 (ред. от 06.06.2022) «Вопросы Министерства внутренних дел Российской Федерации» // СЗ РФ. 2011. № 10. Ст. 1334.

55. Указ Президента РФ от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // СЗ РФ. 2022. № 18. Ст. 3058.

56. Указ Президента РФ от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» / СЗ РФ. 2021. № 27 (Ч. II). Ст. 5351.

57. Указ Президента РФ от 03.08.2018 г. № 471 «О некоторых вопросах Межведомственной комиссии по защите государственной тайны» // СЗ РФ. 2018. № 32 (Ч. 2). Ст. 5317.

58. Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

59. Указ Президента РФ от 06.03.1997 г. № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера» // СЗ РФ. 1997. № 10. Ст. 1127.

60. Указ Президента РФ от 07.05.2012 г. № 601 «Об основных направлениях совершенствования системы государственного управления» // Российская газета. 2012. 09 мая. № 102.

61. Указ Президента РФ от 07.08.2004 г. № 1013 (ред. от 03.03.2022) «Вопросы Федеральной службы охраны Российской Федерации» // СЗ РФ. 2004. № 32. Ст. 3314.

62. Указ Президента РФ от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

63. Указ Президента РФ от 11.05.2006 г. № 473 (ред. от 24.09.2007) «Вопросы Федеральной таможенной службы» // СЗ РФ. 2006. № 20. Ст. 2162.

64. Указ Президента РФ от 16.08.2004 г. № 1085 (ред. от 08.12.2021) «Вопросы Федеральной службы по техническому и экспортному контролю» // СЗ РФ. 2004. № 34. Ст. 3541.

65. Федеральный закон от 03.04.1995 г. № 40-ФЗ (ред. от 14.07.2022) «О федеральной службе безопасности» // СЗ РФ. 1995. № 15. Ст. 1269.

66. Федеральный закон от 06.04.2011 г. № 63-ФЗ (ред. от 11.06.2021) «Об электронной подписи» // Российская газета. 2011. 08 апреля. № 75.

67. Федеральный закон от 06.12.2011 г. № 402-ФЗ (ред. от 26.07.2019) «О бухгалтерском учете» // Российская газета. 2011. 09 декабря. № 278.

68. Федеральный закон от 06.12.2021 г. № 390-ФЗ «О федеральном бюджете на 2022 год и на плановый период 2023 и 2024 годов» // Российская газета. 2021. 10 декабря. № 281.

69. Федеральный закон от 09.02.2007 г. № 16-ФЗ (ред. от 14.03.2022) «О транспортной безопасности» // СЗ РФ. 2007. № 7. Ст. 837.

70. Федеральный закон от 09.02.2009 г. № 8-ФЗ (ред. от 30.04.2021) «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // СЗ РФ. 2009. № 7. Ст. 776.

71. Федеральный закон от 12.01.1996 г. № 10-ФЗ (ред. от 21.12.2021) «О профессиональных союзах, их правах и гарантиях деятельности» // СЗ РФ. 1996. № 3. Ст. 148.

72. Федеральный закон от 21.11.2011 г. № 323-ФЗ (ред. от 11.06.2022, с изм. от 13.07.2022) «Об основах охраны здоровья граждан в Российской Федерации» // СЗ РФ. 2011. № 48. Ст. 6724.

73. Федеральный закон от 25.12.2008 г. № 273-ФЗ (ред. от 01.04.2022) «О противодействии коррупции» // СЗ РФ. 2008. № 52 (Ч. 1). Ст. 6228.

74. Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 14.07.2022) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (Ч. 1). Ст. 3448.

75. Федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. от 02.07.2021) «О персональных данных»// СЗ РФ. 2006. № 31 (Ч. 1). Ст. 3451.

76. Федеральный закон от 27.11.2010 г. № 311-ФЗ (ред. от 24.02.2021) «О таможенном регулировании в Российской Федерации» // СЗ РФ. 2010. № 48. Ст. 6252.

77. Федеральный закон от 28.12.2010 г. № 390-ФЗ (ред. от 09.11.2020) «О безопасности» // СЗ РФ. 2011. № 1. Ст. 2.

78. Федеральный закон от 29.07.2004 г. № 98-ФЗ (ред. от 14.07.2022) «О коммерческой тайне» // СЗ РФ. 2004. № 32. Ст. 3283.

79. Федеральный закон от 31.05.2002 г. № 63-ФЗ (ред. от 31.07.2020) «Об адвокатской деятельности и адвокатуре в Российской Федерации» // СЗ РФ. 2002. № 23. Ст. 2102.

80. Цифровая экономика: проблемы правового регулирования / Отв. ред. В.В. Зайцев, О.А. Серова. М.: КНОРУС, 2019. 290 с.

81. Юридические науки: проблемы и перспективы: материалы Междунар. науч. конф. (г. Пермь, март 2012 г.). Пермь: Меркурий, 2012. 120 с.

82. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security

of network and information systems across the Union [Электронный ресурс] Режим доступа: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (дата обращения: 05.09.2022).

83. Strategy EU [Электронный ресурс] Режим доступа: https://ec.europa.eu/info/strategy_en (дата обращения: 05.09.2022).