А. В. ТЕРЕХОВ, В. Н. ЧЕРНЫШОВ,
А. В. ПЛАТЕНКИН, А. В. СЕЛЕЗНЕВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Тамбов
Издательский центр ФГБОУ ВО «ТГТУ»
2023

Министерство науки и высшего образования Российской Федерации

**Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Тамбовский государственный технический университет»**

**А. В. ТЕРЕХОВ, В. Н. ЧЕРНЫШОВ,
А. В. ПЛАТЕНКИН, А. В. СЕЛЕЗНЕВ**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Утверждено Ученым советом университета
в качестве учебного пособия для студентов направлений подготовки
09.03.03, 09.04.03 «Прикладная информатика» (профиль «Прикладная информатика в юриспруденции»), 40.03.01 «Юриспруденция» специальности 40.05.01 «Правовое обеспечение национальной безопасности» очной и заочной форм обучения

Учебное электронное издание

Тамбов
Издательский центр ФГБОУ ВО «ТГТУ»
2023

УДК 51(075.8)
ББК 221я73
И74

Рецензенты:

Кандидат юридических наук, доцент, заведующий кафедрой уголовного права и процесса Института права и национальной безопасности ФГБОУ ВО «ТГУ им. Г. Р. Державина»
Е. А. Попова

Кандидат юридических наук, доцент, заведующий кафедрой «Безопасность и правопорядок» ФГБОУ ВО «ТГТУ»
М. Г. Диева

И74 **Информационная безопасность** и правовые основы защиты персональных данных [Электронное издание] : учебное пособие / А. В. Терехов, В. Н. Чернышов, А. В. Платенкин, А. В. Селезнев. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ», 2023. – 1 электрон. опт. диск (CD-ROM). – Системные требования : ПК не ниже класса Pentium II ; CD-ROM-дисковод ; 2,50 Mb ; RAM ; Windows 95/98/XP ; мышь. – Загл. с экрана.

ISBN 978-5-8265-2648-4

Затронуты различные аспекты проблем информационной безопасности. Необходимое внимание уделено ведущей роли государства, которое защищает информационные права и свободы личности с учетом обеспечения информационной безопасности общества и государства.

Предназначено для студентов направлений подготовки 09.03.03, 09.04.03 «Прикладная информатика» (профиль «Прикладная информатика в юриспруденции»), 40.03.01 «Юриспруденция» специальности 40.05.01 «Правовое обеспечение национальной безопасности» очной и заочной форм обучения.

УДК 51(075.8)
ББК 221я73

ISBN 978-5-8265-2648-4

ВВЕДЕНИЕ

Новые технологии, глобальные коммуникационные сети, охватывая практически все сферы деятельности человека и общества, меняют не только качество жизни людей, но и многократно увеличивают риски и угрозы в информационной сфере, несут реальные угрозы информационной безопасности личности, общества и государства. При этом правовая база, гарантирующая нам основные информационные права и свободы, являющаяся фундаментом системы обеспечения информационной безопасности, во многом определяет ее современные возможности. Поэтому изучение различных аспектов обеспечения информационной безопасности, в том числе и правовых, является весьма важным.

В Российской Федерации проведена существенная работа по созданию и совершенствованию обеспечения ее информационной безопасности. Сформирована правовая основа обеспечения информационной безопасности. Приняты Закон Российской Федерации «О государственной тайне» от 21.07.1993 № 5485-1, федеральные законы «Об информации, информационных технологиях и о защите информации», «О персональных данных», ряд других законов, ведется работа по их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере. Реализуется государственная программа Российской Федерации «Информационное общество» (с изменениями и дополнениями от 29.04.2023 г.).

С учетом этого в учебном пособии значительное внимание уделено ведущей роли государства, которое законодательно обеспечивает условия для конкуренции в информационной индустрии, юридически защищает информационные права и свободы личности, при этом обеспечивая защищенность национальных интересов в информационной сфере, координируя усилия различных субъектов общества.

Учебное пособие способствует формированию необходимых компетенций по таким дисциплинам, как «Правовые основы информационной безопасности», «Информационная безопасность», а также может быть полезно при изучении дисциплины «Информационное право». Представленный материал, отражая изменения, связанные с совершенствованием законодательства Российской Федерации в сфере обеспечения информационной безопасности, ориентирован на студентов направлений подготовки 09.03.03, 09.04.03 «Прикладная информатика» (профиль «Прикладная информатика в юриспруденции»), 40.03.01 «Юриспруденция» специальности 40.05.01 «Правовое обеспечение национальной безопасности» очной и заочной формы обучения, а также может быть полезен и для других профилей подготовки, изучаются вопросы, связанные с обеспечением информационной безопасности.

1. РАЗВИТИЕ И СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. ПРИОРИТЕТНАЯ РОЛЬ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОСТРОЕНИИ ГЛОБАЛЬНОГО ИНФОРМАЦИОННОГО ОБЩЕСТВА

Об информационном обществе сегодня написано множество работ, в которых большинство западных и отечественных авторов понимают под ним общество, которое возникает следом за постиндустриальным обществом. При этом в процессе развития социальной системы неизбежно происходят существенные изменения в сфере оборота информации (производстве, распространении, а также ее потреблении), что приводит к кардинальным изменениям во всех сферах жизни общества, трансформируя сложившуюся на этапе постиндустриального развития систему связей и отношений [20, 31].

Становление информационного общества, породило не только позитивные ожидания, связанные с положительными переменами в жизни социума, но, к сожалению, породило и серьёзные проблемы, в том числе связанные с информационной безопасностью.

Решение этих проблем является весьма важным, так как от этого напрямую зависят национальные интересы в информационной сфере (включая соблюдение основных конституционных прав и свобод человека и гражданин), а также и существование самого информационного общества.

Процессы становления информационного общества во многом определила Окинавская хартия глобального информационного общества, принятая 22 июля 2000 г. лидерами стран G8 и ориентированная на развитие информационного общества и мировое движение под знаком «информация для всех» [20].

Основные принципы вхождения государств и стран в информационное общество, а также основные положения, которые определяют осуществление политики по формированию и развитию информационного общества были сформулированы в июле 2000 г. в Окинаве «восьмеркой» ведущих стран в рамках принятой ими Хартии Глобального информационного общества.

В этих положениях были отмечены следующие наиболее важные факторы, влияющие на формирование общества XXI в., среди которых

можно выделить: революционное воздействие информационно-коммуникационных технологий (ИКТ) на образ жизни людей, их образование и работу, а также взаимодействие правительства и гражданского общества, являющееся одним из важных стимулов развития мировой экономики, позволяющим эффективно решать социальные и экономические проблемы, открывая огромные возможности; стимулирование ИКТ экономической и социальной трансформации, состоящей в ее способности способствовать людям и обществу в использовании идей и знаний.

Информационное общество дает возможность членам этого общества раскрыть более полно свой потенциал, а также реализовывать свои устремления, но для этого должны приниматься меры, которые позволяют, чтобы ИКТ способствовали не только достижению целей обеспечения устойчивого экономического роста, но и повышению общественного благосостояния, а также стимулированию социального согласия, укреплению демократии, международной стабильности. В Хартии отмечалось, что основой устойчивости глобального информационного общества являются демократические ценности, стимулирующие развитие человека, среди которых в первую очередь необходимо отметить такие, как свободный обмен информацией, знаниями, уважение к особенностям других людей, а также взаимная терпимость.

Основные этапы становления информационного общества в нашей стране: формирование основ государственного регулирования в сфере информатики и информатизации (1991 – 1995 гг.); смена приоритетов государства от информатизации к выработке полноценной информационной политики (1995 – 1999 гг.); переход к государственной информационной политике для построения российского информационного общества (1999 г. – по настоящее время) [29].

Необходимо отметить, что ведущую роль в становлении информационного общества играет государство, координируя усилия различных субъектов общества, законодательно обеспечивая условия для конкуренции в информационной индустрии, юридически защищая информационные права и свободы личности, при этом обеспечивая защищенность национальных интересов в информационной сфере.

Формирование информационного общества невозможно представить без обеспечения национальной безопасности в информационной сфере. Согласно Доктрине информационной безопасности Российской Федерации (утв. Президентом РФ 05.12.2016 № Пр-1895) – «информационная безопасность Российской Федерации (далее – информационная безопасность) – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при

котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства».

Именно государство обеспечивает основные конституционные права личности, защищающее права и интересы личности, а также общества и государства в информационной сфере. Одной из приоритетных составляющих национальной безопасности Российской Федерации является обеспечение информационной безопасности, которая существенно влияет на защищенность, в том числе и правовую, национальных интересов России в различных сферах жизнедеятельности общества и государства. Совершенствование правового обеспечения информационной безопасности Окинавская хартия глобального информационного общества выделяет среди приоритетов при построении глобального информационного общества.

Правовое обеспечение информационной безопасности выступает как единая система правового регулирования общественных отношений в области противодействия угрозам национальным интересам Российской Федерации в информационной сфере.

Специфика правоотношений по обеспечению информационной безопасности определяется, прежде всего, особенностями информационной сферы, т.е. сферы жизни общества, связанной с созданием, распространением, преобразованием и потреблением информации.

На начало XXI века приходится появление программных документов и интенсивное развитие законодательства, регулирующего вопросы обеспечения информационной безопасности. Взамен фрагментарному регулированию правоотношений в данной сфере (так, ранее действовали Закон РФ «О государственной тайне», отдельные положения Гражданского кодекса РФ, Уголовного кодекса РФ, Кодекса РФ об административных правонарушениях), наметились тенденции к развитию самостоятельной (информационной) общности законодательства и института правового обеспечения информационной безопасности внутри нее [20]. Среди нормативно-правовых актов, направленных на регулирование отношений в сфере информации, принятых в начале этого века, можно назвать Федеральный закон от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне», Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных», четвертая часть Гражданского кодекса РФ, Федеральный закон 09.02.2009

№ 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», Федеральный закон от 29.12.2010 № 4Э6-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» и ряд других).

Активная работа по подготовке, обсуждению законопроектов, принятию законов и изменений к законам позволяет своевременно совершенствовать правовое обеспечение информационной безопасности, усиливая роль права в вопросах регулирования деятельности, по обеспечению информационной безопасности в условиях формирования информационного общества.

1.2. ОБЩАЯ ХАРАКТЕРИСТИКА ЗАКОНОДАТЕЛЬСТВА ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Как справедливо отмечает И. Л. Бачило, информационное законодательство в современном обществе призвано играть особую роль. При этом эффективность права тем выше, чем оно точнее учитывает потребности развития общества, адекватно отвечая требованиям объективных экономических законов, точно выражая в юридических нормах задачи, поставленные жизнью [20].

В одном из докладов Совета Федерации подчеркивалось, что формирование информационного общества в России – системная и долгосрочная задача, от решения которой напрямую зависят возможности увеличения конкурентоспособности экономики нашей страны, укрепления безопасности, а также обеспечение государственных гарантий конституционных прав наших граждан в информационной сфере. При этом развитие информационного общества невозможно представить без формирования группы законов, которые бы комплексно обеспечивали правовую защищенность интересов личности, общества и государства в информационной среде.

Классификатор правовых актов, который был утвержден Указом Президента РФ от 15.03.2000 № 511, выделил информационную безопасность в:

- отрасли информации и информатизации (120.070.000);
- отрасли безопасности и охраны правопорядка (160.040.030).

Это свидетельствует о том, что законодательство в области обеспечения информационной безопасности может быть отнесено как к законодательству о безопасности, так и к информационному законодательству, объединяя при этом нормы, которые содержатся в нормативных актах других отраслей законодательства, в том числе относящиеся к гражданскому праву (защита коммерческой тайны), к консти-

туционному праву (например – защита тайны личной жизни, тайны переписки и переговоров) и др.

Национальное законодательство в рассматриваемой сфере включает нормы Конституции РФ, а также положения федеральных и иных законов, в которых находят закрепление основные информационные права и свободы, положения, напрямую касающиеся информационной безопасности.

В Конституции РФ, в частности, рассматриваемым вопросам, посвящены ст. 23, ст. 26, ст. 28, ст. 42 и др. (см. рис. 1) [1, 32].

Основные информационные права и свободы, положения, напрямую касающиеся информационной безопасности, закрепленные в Конституции РФ:

– право на неприкосновенность частной жизни, личную и семейную тайну (ч. 1 ст. 23);
– на защиту своей чести и доброго имени (ч. 1 ст. 23);
– на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ч. 2 ст. 23);
– на пользование родным языком, на свободный выбор языка общения, воспитания, обучения и творчества (ч. 2 ст. 26);
– свобода совести, свобода вероисповедания (ст. 28);
– свобода мысли и слова (ч. 1 ст. 29);
– право на свободу выражения собственных мнений и убеждений (право свободно выбирать, иметь и распространять любые убеждения (ст. 28);
– никто не может быть принужден к выражению своих мнений и убеждений или отказу от них (ч. 3 ст. 29);
– право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ч. 4 ст. 29);
– свобода массовой информации (ч. 5 ст. 29);
– право граждан обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления (ст. 33);
– право каждого на достоверную информацию о состоянии окружающей среды (ст. 42);
– право на образование (ч. 1 ст. 43);
– свобода всех видов творчества и преподавания (ч. 1 ст. 44);
– право на пользование учреждениями культуры, на доступ к культурным ценностям (ч. 2 ст. 44);
– на получение квалифицированной юридической помощи (ст. 48).

Рис. 1. Некоторые нормы Конституции РФ, обеспечивающие основные информационные права и свободы, касающиеся информационной безопасности

Следует отметить, что в Конституции СССР 1977 г. и в Конституции РСФСР 1978 г. тема права на информацию самостоятельно не выделялась. Она была включена в систему политических прав и свобод.

Конституция РФ, как основной закон, является базовым источником норм права, регулирующих обеспечение информационной безопасности, закрепив в ст. 23, 24, 29, 42, 44 основные информационные права и свободы граждан, а также установив гарантии их защиты. Другие законы не могут противоречить Конституции (основному закону).

Гарантируя информационные права и свободы, Конституция РФ в ч. 3 ст. 55 предусматривает возможность ограничения данных прав лишь федеральным законом. Но такие ограничения допускаются лишь в той мере, в какой это необходимо для достижения целей защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Это позволяет обеспечивать гарантии информационных прав и свобод граждан, но при условии разумного ограничения их.

Конституция РФ, отдавая приоритет правам и свободам человека (в том числе и в информационной сфере) и провозглашая их высшей ценностью, отмечает в ст. 2, что признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства.

На всех этих этапах основные информационные права, закрепленные в Конституции РФ, являются основой и ориентиром формирования информационного общества. Идеальных конституций в мире нет, тем более конституций переходного периода в развитии общества. Нельзя исключать принятия необходимых поправок к Конституции РФ, когда это обусловливается объективными потребностями общественного развития, а не личными интересами тех или иных политиков, политических сил, и не затрагивает фундаментальные конституционные установления и ценности [22].

Конституция РФ облекает в юридическую форму баланс интересов (в том числе и в информационной сфере) всех социальных групп общества. Наличие такого баланса определяет состояние защищенности, на которое и направлено правовое обеспечение информационной безопасности.

На сегодняшний день Конституция РФ содержит в своем тексте вполне значимый потенциал правовых преобразований, т.е. она одновременно позволяет и в определенных пределах уточнять и менять условия социального компромисса и реализовать правовые изменения, которые подтягивают наше общество и государство к уровню высших мировых достижений в сфере политико-правового развития.

При этом стоит отметить, что основные положения, затрагивающие основные информационные права и свободы, закрепленные

в Основном законе нашей страны, отвечая демократическим ценностям, являются надежной правовой основой формирования информационного общества [30, 33].

Часть информационных прав и свобод получила подтверждение в документах стран – участников СНГ, в частности в Модельном информационном кодексе от 3 апреля 2008 г., в Конвенции о правах и основных свободах человека от 26 мая 1995 г. и др. [33].

В основе законодательства об обеспечении информационной безопасности лежат основополагающие принципы и нормы международного права, которые закреплены в международных актах, таких как:

– Всеобщая декларация прав человека (от 10 декабря 1948 г.);

– Европейская конвенция о защите прав человека и основных свобод (от 4 ноября 1950 года);

– Международный пакт о гражданских и политических правах (от 16 декабря 1966 г.);

– Декларация Совета Европы о средствах массовой информации и правах человека (23 января 1970 г.).

Эти основополагающие документы закрепляют не только основополагающие информационные права и свободы человека и гражданина, но и возможность их ограничения (в интересах защиты нравственности, права, свобод и законных интересов других лиц).

Окинавская хартия глобального информационного общества, принятая 22 июля 2000 г. лидерами стран G8, провозгласила право каждого человека на благоприятную информационную среду, отметила необходимость создания безопасного и свободного от преступности киберпространства, как одну из задач мирового сообщества [33].

Несомненно, важную роль для законодателя имеют и акты Европейского суда по правам человека, которые признают право государства принимать законы, ограничивающие распространение информации и идей, несмотря на их достоинства («как произведений искусства или как вклада в публичное обсуждение проблем», в том числе устанавливать контроль и классификацию информационной продукции, а при нарушении закона – применять штрафные меры, конфискацию и другие санкции, вплоть до уголовных, когда это необходимо в интересах защиты нравственности и благополучия конкретных лиц или групп лиц (таких, как дети), нуждающихся в особой охране в связи с недостатком зрелости или состоянием зависимости).

Как было отмечено выше, согласно ч. 3 ст. 55 Конституции РФ, права и свободы человека и гражданина могут быть ограничены лишь федеральным законом. При этом следует отметить, что Статьей 71 Конституции РФ вопросы, касающиеся безопасности, регулирова-

ния и защиты прав и свобод человека и гражданина отнесены ст. 71 Конституции РФ к вопросам федерального ведения.

Отдельные нормы, посвященные обеспечению информационной безопасности, содержались в части 1 Гражданского кодекса РФ (закрепивший, в частности, в качестве объекта регулирования такие нематериальные информационные блага, как честь и доброе имя, деловая репутация, неприкосновенность частной жизни, личная и семейная тайна, право авторства и др.), уголовном кодексе РФ и Кодексе РФ об административных правонарушениях (устанавливающих ответственность за разглашение информации ограниченного доступа, преступления и правонарушения в сфере компьютерной информации) и др. Вместе с тем, правое регулирование указанных отношений осуществлялось большей частью фрагментарно и не являлось основной целью принимаемых законодательных актов.

Действующий в настоящее время Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» (в ред. от 05.10.2015) среди основных принципов обеспечения безопасности на первое место ставит соблюдение и защиту прав и свобод человека и гражданина, а также законность, при этом, отмечая системность и комплексность применения информационных, правовых и иных мер обеспечения безопасности.

Справедливо считают, что началом формирования законодательства в сфере обеспечения информационной безопасности явилось принятие следующих правовых актов:

– Закона РФ от 27.12.1991 № 2124-1 «О средствах массовой информации» (установившего недопустимость цензуры и ответственность за злоупотребление свободой СМИ);

– Закона РФ от 21.07.1993 № 5485-1 «О государственной тайне» (определившего исчерпывающий перечень сведений, составляющих государственную тайну, а также соответствующие ограничения для нее);

– Федерального закона от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации», для своего времени достаточно полно регулировавшего вопросы, связанные с защитой информации и прав субъектов в области информационных процессов и информатизации (в настоящее время утратил силу);

– Федерального закона от 04.07.1996 № 85-ФЗ «Об участии в международном информационном обмене», закреплявшего определение «информационная безопасность», устанавливавшего ограничения вывода информации за пределы России, недопущение монополизации при международном информационном обмене, запрещавшего

распространение на территории России недостоверной, ложной иностранной документированной информации (в настоящее время утратил силу) и ряда других законов.

Важно, что эти законы, при имевшихся в них недостатках, были приняты, основываясь на базовых международно-правовых и конституционных нормах и принципах, таким образом, составив основу законодательства об обеспечении информационной безопасности.

Совершенствование законодательства об обеспечении информационной безопасности в дальнейшем было связано с устранением отдельных дефектов законов (пробелы, противоречия, дублирование, технические ошибки), конкретизацией изложенных в них норм в специальных законодательных актах, систематизации информационного законодательства.

Задача по совершенствованию нормативной правовой базы обеспечения информационной безопасности РФ во многом была определена в результате принятия Доктрины информационной безопасности Российской Федерации (утв. Президентом РФ 05.12.2016 № Пр-1895) [4]. Задача совершенствования нормативной правовой базы обеспечения информационной безопасности РФ имела определяющее значение для большинства актуальных преобразований в России. Несомненно, административная реформа, реформа в области технического регулирования невозможны без качественного изменения правовых актов, регулирующих сферу обеспечения информационной безопасности. Доктрина явилась основополагающим документом, призванным активизировать деятельность законодателя по принятию законов, которые направлены на эффективное регулирование различных направлений деятельности по обеспечению информационной безопасности. Изменения, которые произошли благодаря этому, были направлены как на конкретизацию, так и на более детальное регулирование вопросов обеспечения информационной безопасности, которые затрагивают различные сферы человеческой деятельности применительно к различным видам информации.

Законы – важнейший вид нормативных правовых актов, принимаемых федеральным парламентом. Общим законом, регулирующим вопросы защиты информации, в настоящее время является Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ст. 16), заменивший действовавшие ранее Федеральный закон «Об информации, информатизации и защите информации» и Федеральный закон «Об участии в международном информационном обмене», раскрывающий значение термина «защита информации» [10].

В целях более полного обеспечения безопасности информации ограниченного доступа приняты Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Федеральный закон от 30.12.2004 № 218-ФЗ «О кредитных историях», Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» и другие, касающиеся вопросов регулирования деятельности, которая направлена на обеспечение защищенности интересов личности, общества и государства, необходимость реализации механизмов защиты которых назрела до принятия Доктрины информационной безопасности РФ. Был уточнен перечень информации, составляющей коммерческую тайну, введено определение персональных данных, установлена ответственность за их разглашение, определен контролирующий орган в данной сфере. Впервые законодательно было обеспечено противодействие инсайдерской деятельности.

Таким образом, можно говорить, что состояние защищенности сегодня обеспечено и в отношении частных информационных ресурсов, так как регулирование отношений, связанных с защитой информации, обеспечивается правовой базой, исходя из баланса прав и законных интересов граждан, общества и государства.

Значительный объем норм, которые касаются обеспечения информационной безопасности в части защиты объектов интеллектуальной собственности (представляющие фактически собой различные виды информации), законодатель поместил в части 4 Гражданского кодекса РФ, где объединены разрозненные законодательные акты, которые действовали до этого (Закон РФ № 5351-1 «Об авторском праве и смежных правах» от 09.07.1993, Патентный закон РФ № 3517-1 от 23.09.1992, № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.1992 и др.) [3].

В целях регулирования отношений, связанных с использованием электронных (электронных цифровых) подписей, которые предназначены для защиты электронных документов и существенно упрощающих возможности гражданского оборота в информационной сфере, позитивным является принятие таких федеральных законов, как № 1-ФЗ «Об электронной цифровой подписи» от 10.01.2002 (утратил силу), а также Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи», действующий в настоящее время [12].

Важным шагом в регулировании отношений, связанных с обеспечением информационной безопасности, явился Федеральный закон

от 29.12.2010 (в ред. от 28.04.2023) № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Этот закон принят в целях обеспечения правовой охраны и защиты детей от информации, наносящей вред их здоровью, нравственному и духовному развитию, так как согласно ст. 14 Федерального закона 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации», предусмотрено введение нормативов оборота информационной продукции, не рекомендуемой для пользования ребенку, а государство обязано принимать меры по его защите от информации, пропаганды и агитации, которая наносит вред его здоровью, нравственному и духовному развитию (в частности, от распространения печатной, аудио- и видеопродукции, пропагандирующей насилие и жестокость, порнографию, наркоманию, антиобщественное поведение). В этом законе дано определение этих терминов: «информационная безопасность детей», «пропаганда насилия и жестокости», «информационная продукция, доступная детям», «информационная продукция для детей», «возрастная категория информационной продукции», «изображение или описание насилия и жестокости», «информация порнографического характера», а также представлена классификация информации по критерию допустимости ее для детей определенного возраста. Законом введены четкие ограничения и запрет распространения определенной информации, установлены основания, а также порядок проведения экспертизы информационной продукции. Названный выше закон является одним из примеров адекватного и продуманного подхода законодателя к решению насущных проблем, так как его принятие явилось результатом серьезных социальных исследований, зарубежного законодательства, соответствующей работы, проведенной общественными комитетами, активного обсуждения проблемы на конференциях по информационно-психологической безопасности. Таким образом наблюдается применение законодателем комплексного подхода к обеспечению безопасности детей от информационной продукции, причиняющей вред их здоровью и развитию.

Еще одним важным шагом в противодействии распространению вредной информации стало принятие Федерального закона от 25.07.2002 (ред. от 28.12.2022) № 114-ФЗ «О противодействии экстремистской деятельности», который установил основные принципы противодействия распространения экстремистских материалов, посягающих на права и законные интересы личности, общества и государства.

Названные выше законодательные акты в сфере обеспечения информационной безопасности в значительной мере направлены на установление режима конфиденциальности в отношении определенных групп информации (государственная тайна, коммерческая тайна, пер-

сональные данные и пр.); на регулирование деятельности по защите информации, на защиту от вредной информации, носящей противоправный характер.

Российское законодательство в сфере обеспечения информационной безопасности имеет наработанную базу, а также перспективы для дальнейшего реформирования, что является ответной реакцией на глобальные изменения в мире и появление новых угроз. Основные принципы, лежащие в основе государственной политики обеспечения информационной безопасности РФ, были определены действующей Доктриной информационной безопасности (рис. 2).

Исходя из вышеизложенного, можно сказать, что формирование законодательства в сфере обеспечения информационной безопасности проходит системно и достаточно интенсивно.

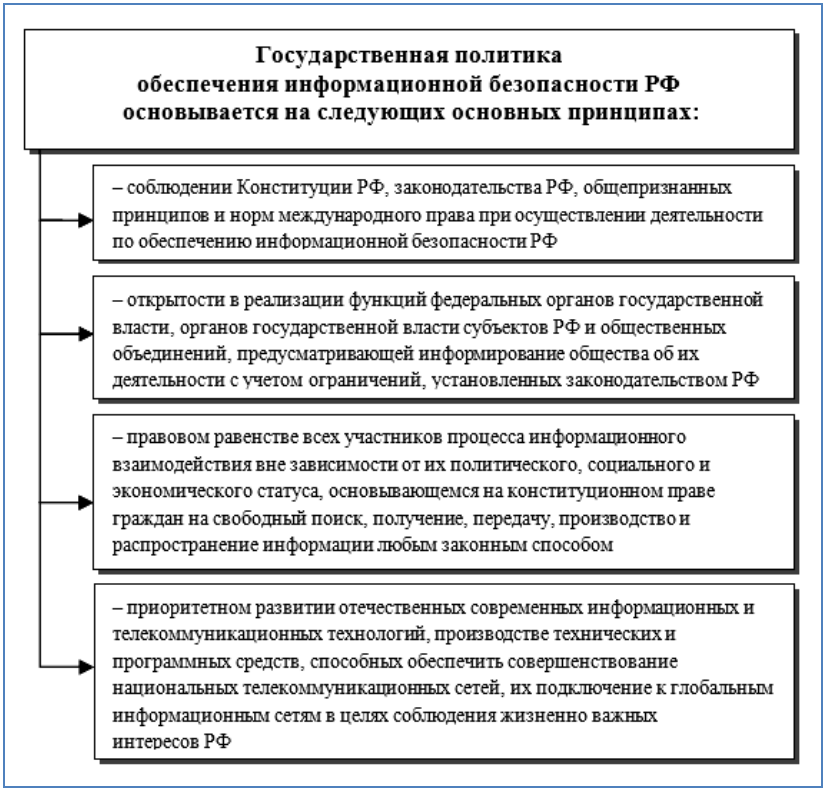

Рис. 2. Основные принципы, лежащие в основе государственной политики обеспечения информационной безопасности РФ

Таким образом, в Российской Федерации мы можем наблюдать активное развитие как информационного законодательства в целом, так и законодательства об информационной безопасности по различным направлениям (приняты федеральные законы «О коммерческой тайне, «О персональных данных», «Об электронной подписи», «О защите детей от информации, причиняющей вред их здоровью и развитию и др.)

В настоящее время одним из приоритетов в области защиты прав человека становится укрепление государственных гарантий неприкосновенности частной жизни при использовании информационных и коммуникационных технологий.

В области развития отрасли информационных и коммуникационных технологий на передний план выходят задачи повышения конкурентоспособности российской продукции, формирование условий для ее широкого использования при создании отечественных информационных систем и сетей связи, технических средств обеспечения информационной безопасности объектов национальной информационной инфраструктуры.

В сфере обеспечения безопасности национальной информационной инфраструктуры необходимо повышать безопасность услуг связи и обработки информации, оказываемых гражданам, организациям и органам государственной власти и местного самоуправления [34].

Действующая Доктрина информационной безопасности как раз и является тем документом, который задает вектор движения в решении современных проблем в рассматриваемой сфере.

2. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТА ИНФОРМАЦИИ

2.1. ПРАВОВАЯ ОСНОВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Становление информационного общества породило не только позитивные ожидания, связанные с положительными переменами в жизни социума, но, к сожалению, породило и серьезные проблемы, в том числе связанные с информационной безопасностью. Решение этих проблем является весьма важным, так как от этого напрямую зависят национальные интересы в информационной сфере (включая соблюдение основных конституционных прав и свобод человека и гражданин), а также существование самого информационного общества [33, 34].

Необходимо отметить, что ведущую роль в становлении информационного общества играет государство, координируя усилия различных субъектов общества, законодательно обеспечивая условия для конкуренции в информационной индустрии, юридически защищая информационные права и свободы личности, при этом обеспечивая защищенность национальных интересов в информационной сфере.

За последние годы в Российской Федерации проведена существенная работа по созданию и совершенствованию обеспечения информационной безопасности. Сформирована правовая основа обеспечения информационной безопасности. Приняты Закон Российской Федерации «О государственной тайне», федеральные законы «Об информации, информационных технологиях и о защите информации», «О персональных данных», ряд других законов, ведется работа по их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере. Реализуется государственная программа Российской Федерации «Информационное общество».

В Российской Федерации правовую базу в области информационной безопасности составляют соответствующие международные договоры РФ; Конституция РФ; законы федерального уровня (включая федеральные конституционные законы, кодексы); указы Президента РФ; постановления Правительства РФ; нормативные правовые акты федеральных министерств и ведомств; нормативные правовые акты субъектов РФ, органов местного самоуправления) и т.д.

Среди нормативно-методических документов государственных органов РФ можно выделить Доктрину информационной безопасности РФ, руководящие документы ФСТЭК, приказы ФСБ.

(Основные положения нормативных документов в области информационной безопасности более детально изучаются в рамках дисциплины «Информационное право»).

Кроме того, к нормативно-методическим относятся Стандарты информационной безопасности, из которых выделяют: международные стандарты; государственные (национальные) стандарты РФ; рекомендации по стандартизации; методические указания.

Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют государственная система защиты информации, система защиты государственной тайны, системы лицензирования деятельности в области защиты государственной тайны и системы сертификации средств защиты информации.

Вместе с тем, стоит отметить, что состояние информационной безопасности Российской Федерации должно в полной мере соответствовать растущим потребностям общества и государства.

Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение.

В России, как и во всем мире, растет популярность Интернета. При этом существенные проблемы информационной безопасности связаны и с тем, что преступники и злоумышленники все чаще используют его в своих целях. За 2022 год в России утекло более 667 млн записей с персональными данными, что почти в три раза больше уровня 2021 г., подсчитали в InfoWatch [27]. Проблемы защищенности информационных ресурсов, обеспечения доступа к ним, а также защита от вредного и опасного содержимого, в том числе и в рамках обеспечения основных конституционных прав и свобод на информацию, безусловно, являются одними из наиболее важных.

Состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства, составляет понятие ***информационной безопасности Российской Федерации***, основные положения которой изложены в Доктрине информационной безопасности Российской Федерации, определяющей вектор многоплановых усилий государства в сфере обеспечения информационной безопасности [4].

Государственное регулирование в сфере применения информационных технологий предусматривает, наряду с другими аспектами, регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации информационных технологиях и защите информации» (ред. от 31.07.2023); развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем; создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети «Интернет» и иных подобных информационно-телекоммуникационных сетей [10].

При этом государственные органы, органы местного самоуправления в соответствии со своими полномочиями участвуют в разработке и реализации целевых программ применения информационных технологий; создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Информационные системы (согласно ст. 13. Федерального закона «Об информации, информационных технологиях и о защите информации») включают в себя: государственные информационные системы (федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов); муниципальные информационные системы, созданные на основании решения органа местного самоуправления; иные информационные системы.

Оператором информационной системы (если иное не установлено федеральными законами) является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы. В случаях и в порядке, установленных федеральными законами, оператор информационной системы должен обеспечить возможность размещения информации в сети Интернет в форме открытых данных.

Важно отметить, что права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране, независимо от авторских и иных прав на такие базы данных.

Установленные Федеральным законом «Об информации, информационных технологиях и о защите информации» требования к государственным информационным системам распространяются и на муниципальные информационные системы (если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении).

В соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного самоуправления, принимающих решения о создании информационных систем, могут устанавливаться особенности эксплуатации государственных информационных систем и муниципальных информационных систем.

Порядок создания и эксплуатации информационных систем, не являющихся государственными информационными системами или муниципальными информационными системами, определяется операторами таких информационных систем в соответствии с требованиями, установленными Федеральным законом «Об информации, информационных технологиях и о защите информации» или другими федеральными законами.

Защита информации согласно ст. 16 Федерального закона «Об информации, информационных технологиях и о защите информации» представляет собой принятие правовых, организационных и технических мер, направленных на:

– обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

– соблюдение конфиденциальности информации ограниченного доступа;

– реализацию права на доступ к информации.

При создании информационных систем необходимо учитывать, что обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

– предотвращение несанкционированного доступа к информации и(или) передачи ее лицам, не имеющим права на доступ к информации;

– своевременное обнаружение фактов несанкционированного доступа к информации;

– предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

– недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

– возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

– постоянный контроль за обеспечением уровня защищенности информации;

– нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации (этот пункт был введен после известных «санкционных» событий Федеральным законом от 21 июля 2014 г. № 242-ФЗ – Собрание законодательства Российской Федерации, 2014, № 30, ст. 4243, вступил в силу с 1 сентября 2016 года).

Необходимо отметить, что в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям [10].

Также необходимо учитывать, что Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Нарушение указанных требований Федерального закона «Об информации, информационных технологиях и о защите информации» влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Системный подход к описанию информационной безопасности предлагает выделение следующих составляющих информационной безопасности [10]:

– законодательная, нормативно-правовая и научная база;

– структура и задачи органов (подразделений), обеспечивающих безопасность ИТ;

– организационно-технические и режимные меры и методы (Политика информационной безопасности);

– программно-технические способы и средства обеспечения информационной безопасности.

Целью реализации информационной безопасности какого-либо объекта является построение Системы обеспечения информационной безопасности данного объекта.

2.2. ГОСУДАРСТВЕННЫЕ ОРГАНЫ, ОБЕСПЕЧИВАЮЩИЕ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Выработку политики информационной безопасности, подготовку законодательных актов и нормативных документов, контроль над выполнением установленных норм обеспечения безопасности информации осуществляют соответствующие государственные органы.

Как предполагается основными положениями Доктрины информационной безопасности, в Российской Федерации функционирует система обеспечения информационной безопасности, которая является частью системы обеспечения национальной безопасности страны.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации.

Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются: Президент Российской Федерации, Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с законодательством Российской Федерации участие в решении задач обеспечения информационной безопасности Российской Федерации.

Президент Российской Федерации руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности Российской Федерации; санкционирует действия по обеспечению информационной безопасности Российской Федерации; в соответствии с законодательством Российской Федерации формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности Российской Федерации; определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности Российской Федерации, а также меры по реализации Доктрины Информационной безопасности.

Палаты Федерального Собрания Российской Федерации на основе Конституции Российской Федерации по представлению Президента Российской Федерации и Правительства Российской Федерации формируют законодательную базу в области обеспечения информационной безопасности Российской Федерации.

Правительство Российской Федерации в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента Российской Федерации Федеральному Собранию приоритетных направлений в области обеспечения информационной безопасности Российской Федерации координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, а также при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

Совет Безопасности Российской Федерации согласно Закону от 28 декабря 2010 г. № 390-ФЗ (с изменениями и дополнениями на 10.03.2023 г.) «О безопасности») проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации, оперативно подготавливает проекты решений Президента Российской Федерации по предотвращению таких угроз, разрабатывает предложения в области обеспечения информационной безопасности Российской Федерации, а также предложения по уточнению отдельных положений настоящей Доктрины, координирует деятельность органов и сил по обеспечению информационной безопасности Российской Федерации, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации решений Президента Российской Федерации в этой области.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту Российской Федерации и в Правительство Российской Федерации.

Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности Российской Федерации.

Органы исполнительной власти субъектов Российской Федерации взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности Российской Федерации; вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности Российской Федерации.

Органы местного самоуправления обеспечивают соблюдение законодательства Российской Федерации в области обеспечения информационной безопасности Российской Федерации.

Органы судебной власти осуществляют правосудие по делам о преступлениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности Российской Федерации.

В состав системы обеспечения информационной безопасности Российской Федерации могут входить подсистемы (системы), ориентированные на решение локальных задач в данной сфере.

Как было указано выше, весьма важная роль принадлежит Совету Безопасности Российской Федерации (см. официальную страничку http://www.scrf.gov.ru), в рамках которого действует Межведомствен-

ная комиссия по информационной безопасности, результаты работы которой периодически, обсуждаются на заседаниях и находят свое отражение в решениях Совета безопасности (рис. 3).

Состав Совета Безопасности Российской Федерации утвержден Указом Президента Российской Федерации от 25 мая 2012 г. № 715 (с изменениями на 17.03.2023 г.). Председателем Совета Безопасности Российской Федерации является Президент Российской Федерации Путин Владимир Владимирович. В состав Совета согласно указанному выше документу входят Постоянные члены Совета Безопасности Российской Федерации и члены Совета Безопасности Российской Федерации (см. сайт http://www.scrf.gov.ru/council/composition/).

На межведомственные комиссии и аппарат Совета безопасности Российской Федерации (и в частности на межведомственную комиссию по информационной безопасности, в сфере ее компетенции согласно Положению о Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности (утв. Указом Президента РФ от 6 мая 2011 г. № 590 (ред. от 07.03.2020)) возлагаются задачи в области обеспечения информационной безопасности Российской Федерации в соответствии с Федеральным законом от 28 декабря 2010 г. № 390-ФЗ «О безопасности» (ред. от 10.07.2023) и Положением о Совете Безопасности Российской Федерации (функции, возлагаемые на Межведомственную Комиссию по информационной безопасности, см. на рис. 4).

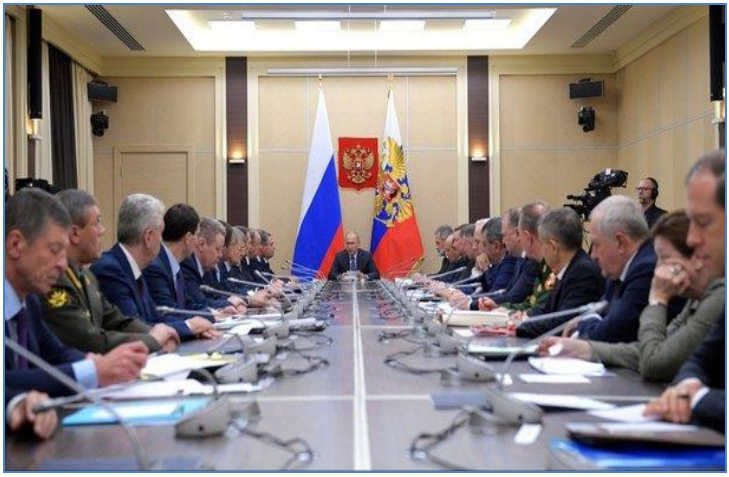

Рис. 3. Заседание Межведомственной комиссии по информационной безопасности

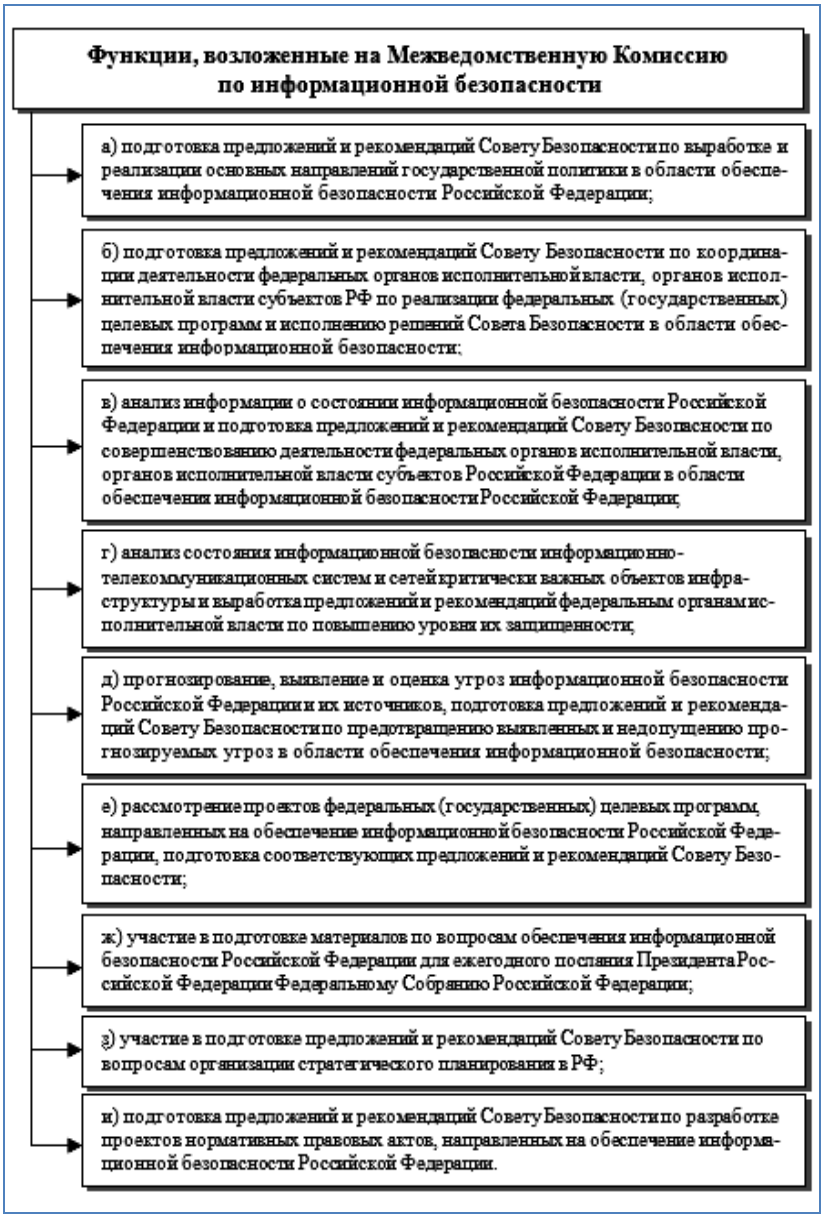

Рис. 4. Функции, возлагаемые на Межведомственную Комиссию по информационной безопасности

В состав Комиссии входят представители федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, органов местного самоуправления, а также организаций (далее – органы и организации), в том числе по согласованию.

Персональный состав Комиссии утверждается Секретарем Совета Безопасности по представлению руководителей органов и организаций, представители которых входят в ее состав.

Комиссия для осуществления своих функций имеет право:

а) взаимодействовать по вопросам, входящим в компетенцию Комиссии, с самостоятельными подразделениями Администрации Президента Российской Федерации, с соответствующими органами и организациями, запрашивать и получать от них в установленном порядке необходимые материалы и информацию;

б) пользоваться в установленном порядке банками и базами данных Администрации Президента Российской Федерации и федеральных органов государственной власти;

в) использовать государственные, в том числе правительственные, системы связи и коммуникации;

г) привлекать в установленном порядке для осуществления аналитических и экспертных работ ученых и специалистов;

д) подготавливать предложения о заключении в установленном порядке договоров с научно-исследовательскими организациями, учреждениями и специалистами на выполнение работ и проведение исследований в области обеспечения безопасности общества и государства в экономической и социальной сфере;

е) обобщать и представлять в Совет Безопасности информацию по вопросам, входящим в компетенцию Комиссии.

Работа Комиссии осуществляется по планам, утверждаемым Секретарем Совета Безопасности.

Информационно-аналитическое и организационно-техническое обеспечение деятельности Комиссии осуществляет аппарат Совета Безопасности, а также при необходимости – органы и организации, представители которых входят в состав Комиссии.

Важной составной частью информационной безопасности являются вопросы защиты информации, составляющей государственную тайну. Поэтому вопросы защиты государственной тайны постоянно находятся в поле зрения Межведомственной комиссии по защите государственной тайны (далее именуется – Межведомственная комиссия или МВК) образована в соответствии с Законом Российской Федерации «О государственной тайне» и Указом Президента Российской Федерации от 6 октября 2004 г. № 1286 «Вопросы Межведомственной комис-

сии по защите государственной тайны». Положение о МВК утверждено Указом Президента РФ от 6 октября 2004 г. № 1286 (ред. от 03.08.2018).

Межведомственная комиссия по защите государственной тайны (далее Межведомственная комиссия) – коллегиальный орган, который осуществляет координацию деятельности федеральных органов государственной власти, а также органов государственной власти субъектов Российской Федерации (далее органы государственной власти) по защите государственной тайны, которая осуществляется в интересах разработки и выполнения государственных программ, нормативных правовых актов и методических документов, служащих для обеспечения реализации федерального законодательства о государственной тайне.

К полномочиям Межведомственной комиссии относятся:

– координация деятельности органов государственной власти, органов местного самоуправления и организаций, которая касается вопросов связанных с реализацией федерального законодательства в области государственной тайны;

– рассмотрение в установленном порядке и представление Президенту Российской Федерации, а также в Правительство РФ предложений касающихся правового регулирования вопросов защиты и совершенствования системы защиты государственной тайны в РФ, а также необходимых предложений по организации разработки и выполнения государственных программ, нормативных правовых актов и методических документов, направленных на реализацию процессов обеспечения федерального законодательства о государственной тайне;

– формирование перечня должностных лиц органов государственной власти, которые наделяются полномочиями по отнесению соответствующих сведений к государственной тайне;

– формирование перечня сведений, отнесенных к государственной тайне;

– формирование перечня особорежимных объектов РФ для представления его затем в Правительство РФ;

– определение соответствующего порядка рассекречивания носителей, содержащих сведений, составляющих государственную тайну, в случае, когда происходит ликвидация организации-фондообразователя и при этом отсутствует ее правопреемник;

– осуществление рассекречивания и продления сроков засекречивания документов КПСС, Правительства СССР, а также других архивных документов, когда организация-фондообразователь и ее правопреемник отсутствуют;

– рассмотрение в случаях, определяемых Законом Российской Федерации «О государственной тайне», запросов органов государственной власти, органов местного самоуправления, организаций, а также граждан о рассекречивании сведений, отнесенных к государственной тайне;

– рассмотрение вопросов о возможности передачи сведений, составляющих государственную тайну, другим государствам и международным организациям, а также представляет в Правительство РФ соответствующие экспертные заключения;

– принятие решения о передаче органом государственной власти, органом местного самоуправления, организацией другому органу государственной власти, органу местного самоуправления, организации сведений, которые составляют государственную тайну, если происходит изменение их функций, форм собственности, либо ликвидация или прекращение работ с использованием сведений, которые составляют государственную тайну;

– организация разработки и представление в Правительство РФ предложений о порядке определения размеров ущерба, который может быть нанесен безопасности РФ вследствие несанкционированного распространения сведений, составляющих государственную тайну, а также ущерба, который может быть нанесен организациям и гражданам из-за засекречивания находящейся в их собственности информации;

– организация разработки и представление в Правительство РФ предложений по правилам отнесения сведений, составляющих государственную тайну, к различным степеням секретности;

– рассмотрение (по поручениям Президента РФ и Правительства РФ) экспертных заключений в целях определения размеров возможного ущерба, который может быть нанесен безопасности Российской Федерации из-за несанкционированного распространения сведений, которые составляют государственную тайну, а также ущерба, нанесенного организациям и гражданам в связи с засекречиванием находящейся в их собственности информации соответствующей информации;

– рассмотрение (по поручениям Президента РФ и Правительства РФ) проектов международных договоров РФ о совместном использовании и защите сведений, составляющих государственную тайну, а также обеспечивает организацию разработки необходимых предложений и экспертных заключений, осуществляет участие по данным вопросам в международном сотрудничестве;

– выработка заключений на решения руководителей органов государственной власти, которые связаны с изменением действующих (в органах государственной власти, органах местного самоуправления

и организациях) перечней сведений, подлежащих засекречиванию, которые могут привести к изменению перечня сведений, отнесенных к государственной тайне, приостанавливает или опротестовывает их решения;

– координирование работы по техническому регулированию в отношении продукции (работ, услуг), сведения о которых составляют государственную тайну, а также работы по организации сертификации средств защиты информации;

– проведение работ по лицензированию деятельности организаций, связанной с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также осуществлением мероприятий и(или) оказанием услуг по защите государственной тайны;

– решение вопроса о возможности продления 30-летнего срока засекречивания сведений, составляющих государственную тайну;

– выдача по запросу межведомственной комиссии (образуемой для рассмотрения обращений граждан РФ в связи с ограничениями их права на выезд из РФ) заключений о том, что сведения особой важности или совершенно секретные сведения, о которых гражданин был осведомлен на день подачи заявления о выезде из Российской Федерации, сохраняют либо утратили соответствующую степень секретности;

– координирование деятельности в сфере подготовки (а также переподготовки, повышения квалификации) специалистов по вопросам защиты государственной тайны;

– разработка методических рекомендаций по организации и проведению государственной аттестации руководителей организаций, которые ответственны за обеспечение защиты сведений, составляющих государственную тайну, определение перечня организаций, осуществляющих образовательную деятельность, по окончании которых выдается документ об образовании (квалификации), который дает право указанным руководителям считаться прошедшими государственную аттестацию.

Кроме вышеназванных, Межведомственная комиссия осуществляет и иные полномочия согласно федеральному законодательству, касающемуся государственной тайны.

В Межведомственную комиссию входят руководители федеральных органов исполнительной власти, Администрации Президента Российской Федерации, Аппарата Правительства Российской Федерации или их заместители.

В состав Межведомственной комиссии входят руководители федеральных органов исполнительной власти, Администрации Прези-

дента Российской Федерации, Аппарата Правительства Российской Федерации и(или) их заместители.

При необходимости в состав Межведомственной комиссии могут быть включены другие должностные лица.

Организационно-техническое обеспечение деятельности Межведомственной комиссии осуществляет центральный аппарат Федеральной службы по техническому и экспортному контролю.

Решения Межведомственной комиссии, принятые в соответствии с ее полномочиями, обязательны для исполнения органами государственной власти, органами местного самоуправления, организациями, должностными лицами и гражданами.

Члены Межведомственной комиссии обладают равными правами при принятии решения.

В случае несогласия с принятым решением каждый член Межведомственной комиссии имеет право изложить в письменном виде свое особое мнение по рассматриваемому вопросу, которое подлежит обязательному приобщению к протоколу заседания.

Решение не может быть принято в случае несогласия с ним члена Межведомственной комиссии, представляющего федеральный орган государственной власти, Администрацию Президента Российской Федерации, иной государственный орган, к чьей компетенции, в соответствии с федеральным законодательством, отнесен рассматриваемый вопрос.

Решения Межведомственной комиссии при необходимости представляются Президенту Российской Федерации, в Правительство Российской Федерации, а также направляются (в части, их касающейся) в органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, в организации независимо от их организационно-правовой формы и формы собственности.

При необходимости, по решениям Межведомственной комиссии, принятым в соответствии с настоящим Положением, могут разрабатываться проекты указов и распоряжений Президента Российской Федерации, постановлений и распоряжений Правительства Российской Федерации, которые представляются на рассмотрение в установленном порядке.

Следует отметить, что до 2003 года полномочия, связанные с обеспечением правительственной связи и информационными технологиями правительственного назначения, выполняло Федеральное агентство правительственной связи и информации при Президенте РФ (ФАПСИ). В его исключительном ведении были также вопросы лицензирования и сертификации в области криптографической защиты

информации. В 2003 году ФАПСИ Указом Президента РФ было расформировано, а его функции были переданы и распределены между Министерством обороны и Федеральной службой безопасности Российской Федерации.

Полномочия Федеральной службы безопасности Российской Федерации (ФСБ России) (рис. 5) в области отнесения сведений к государственной тайне и их защиты отражены в Федеральном законе «Об органах Федеральной службы безопасности в Российской Федерации».

Органы Федеральной службы безопасности представляют собой единую централизованную систему, в которую входят:

1) Федеральная служба безопасности Российской Федерации;

2) управления (отделы) Федеральной службы безопасности Российской Федерации по отдельным регионам и субъектам Российской Федерации (территориальные органы безопасности), например, Управление Федеральной службы безопасности по Тамбовской области;

3) управления (отделы) Федеральной службы безопасности Российской Федерации в Вооруженных Силах Российской Федерации, войсках и иных воинских формированиях, а также в их органах управления (органы безопасности в войсках).

Федеральная служба безопасности Российской Федерации является федеральным органом исполнительной власти, осуществляя соответствующие функции по защите государственной тайны (см. рис. 6) в соответствии с федеральным законодательством.

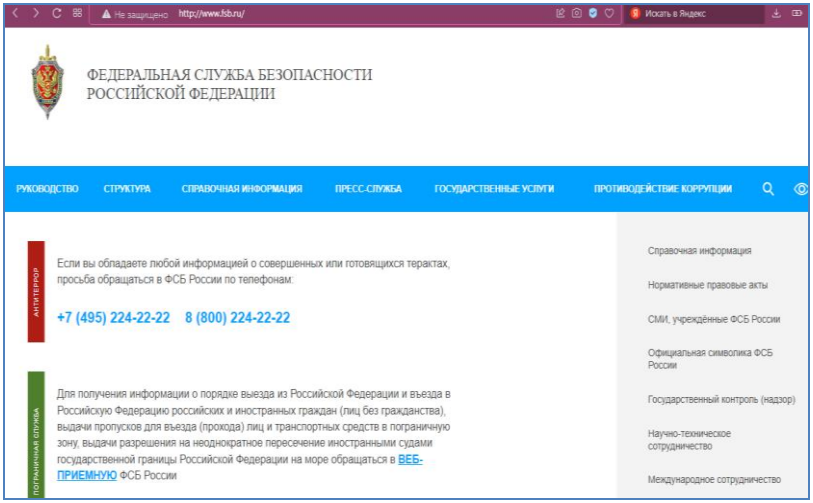

Рис. 5. Официальный сайт http://www.fsb.ru ФСБ Российской Федерации

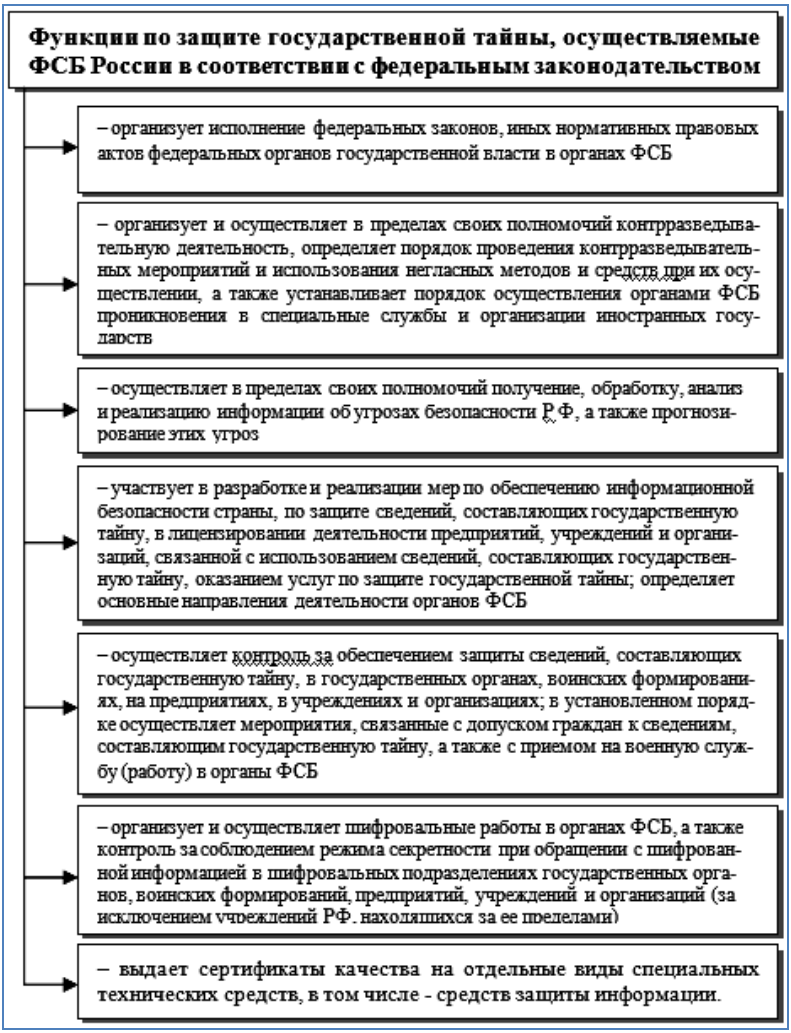

Рис. 6. Функции по защите государственной тайны, осуществляемые ФСБ России в соответствии с федеральным законодательством

В целях решения задач обеспечения безопасности Российской Федерации военнослужащие органов федеральной службы безопасности могут быть прикомандированы к Государственным органам, предприятиям, учреждениям и организациям независимо от форм собственности.

Функции Министерства обороны РФ в области защиты государственной тайны определены Федеральным законом «Об обороне» от 31 мая 1996 года № 61-ФЗ, Положением о Министерстве обороны РФ, рядом постановлений Правительства РФ (рис. 7).

Министерство обороны РФ (http://www.mil.ru) является одним из основных владельцев сведений, составляющих государственную тайну. Кроме функций по их защите, МО РФ выполняет ряд специфических функций, связанных с защитой государственной тайны, к которым относятся, лицензирование, сертификация средств защиты информации по требованиям безопасности информации в интересах

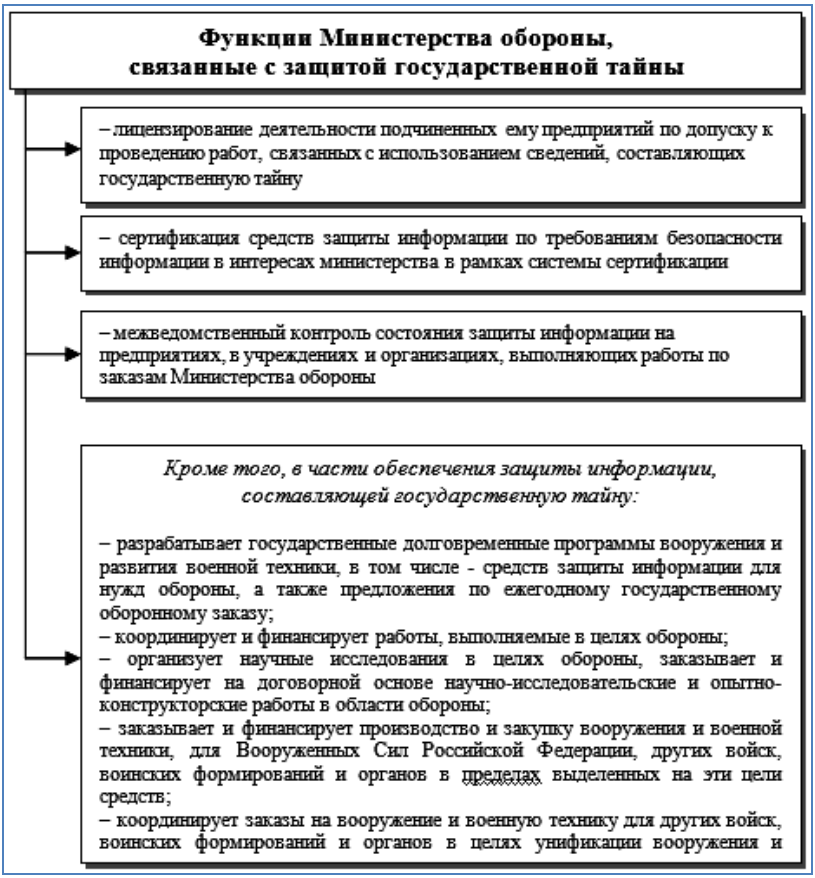

Рис. 7. Функции Министерства обороны, связанные с защитой государственной тайны

министерства в рамках системы сертификации, межведомственный контроль состояния защиты информации на предприятиях, в учреждениях и организациях, выполняющих работы по заказам Министерства обороны и ряд других (см. рис. 7).

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций https://rkn.gov.ru (рис. 8) на основании Постановления Правительства РФ от 16 марта 2009 г. № 228 (с изменениями на 30.03.2023 г.) «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (Роскомнадзор) является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы.

Роскомнадзор является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных.

Роскомнадзор находится в ведении Министерства связи и массовых коммуникаций Российской Федерации.

Рис. 8. Официальный сайт https://rkn.gov.ru Федеральной службы по надзору в сфере связи

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций руководствуется в своей деятельности Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и Правительства Российской Федерации, международными договорами Российской Федерации, нормативными правовыми актами Министерства связи и массовых коммуникаций Российской Федерации, а также соответствующим Положением.

В связи с тем, что Федеральная служба по надзору в сфере связи и массовых коммуникаций была преобразована в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций, в настоящее время определены полномочия и порядок организации деятельности новой Службы. Так, на Роскомнадзор возложены функции по контролю и надзору в сфере СМИ, в том числе электронных и массовых коммуникаций, информационных технологий и связи. Так же Служба осуществляет контроль и надзор за соответствием обработки персональных данных требованиям российского законодательства, а также организует деятельность радиочастотной службы. Кроме того, Роскомнадзор является уполномоченным органом власти по защите прав субъектов персональных данных.

Среди полномочий Службы – лицензирование деятельности в области телевизионного вещания и радиовещания, оказания услуг связи, а также изготовления экземпляров аудиовизуальных произведений и программ для ЭВМ. Она ведет реестр операторов, занимающих существенное положение в сети связи общего пользования, и единые общероссийские реестры СМИ. Роскомнадзор регистрирует СМИ, выдает разрешения на распространение продукции зарубежных периодических печатных изданий в РФ, организует проведение работ по изысканию новых радиочастотных каналов.

Служба находится в ведении Минкомсвязи России. Ее руководитель назначается и освобождается от должности Правительством РФ по представлению Министра связи и массовых коммуникаций РФ (Постановление Правительства РФ, которым было утверждено Положение о Федеральной службе по надзору в сфере связи и массовых коммуникаций, а также отдельные нормы иных актов Правительства РФ, касавшиеся работы этой Службы, признаны утратившими силу).

Служба внешней разведки Российской Федерации (СВР) http://svr.gov.ru (рис. 9) в соответствии с Федеральным Законом «О внешней разведке» от 10 января 1996 года № 5-ФЗ является одним из органов внешней разведки Российской Федерации и составной частью сил обеспечения безопасности Российской Федерации.

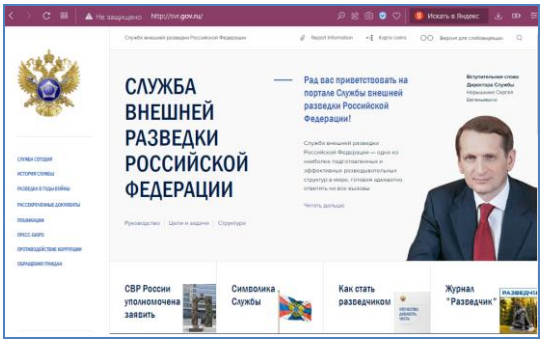

Рис. 9. Официальный сайт http://svr.gov.ru Службы внешней разведки РФ

Этой службе предоставляются следующие полномочия (в сфере защиты государственной тайны и информации):

- организация и обеспечение в пределах своей компетенции защиты государственной тайны в учреждениях Российской Федерации, находящихся за пределами территории Российской Федерации, включая определение порядка осуществления физической и инженерно-технической защиты указанных учреждений, мероприятия по предотвращению утечки по техническим каналам сведений, составляющих государственную тайну;
- обеспечение собственной безопасности, т.е. защита своих сил, средств и информации от противоправных действий и угроз.

Для осуществления своей деятельности Служба внешней разведки Российской Федерации может при собственных лицензировании и сертификации приобретать, разрабатывать (за исключением криптографических средств защиты), создавать, эксплуатировать информационные системы, системы связи и системы передачи данных, а также средства защиты информации от утечки по техническим каналам.

С 18 декабря 1973 г. Государственная техническая комиссия СССР, а в соответствии с Указом Президента РФ от 19 февраля 1999 г. № 212 Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России) являлась федеральным органом исполнительной власти, осуществляющим межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную или служебную тайну, от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования и по противодействию техническим средствам разведки на территории Российской Федерации (техническая защита информации).

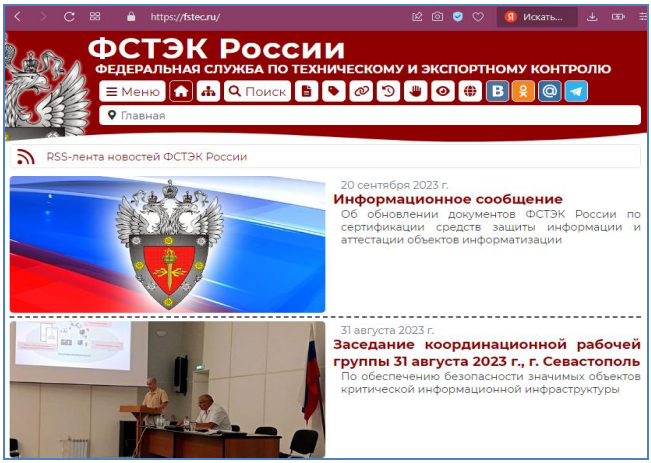

Рис. 10. Официальный сайт http://www.fstec.ru Федеральной службы по техническому и экспортному контролю

В соответствии с Указом Президента Российской Федерации от 9 марта 2004 г. № 314 Гостехкомиссия России была преобразована в Федеральную службу по техническому и экспортному контролю (ФСТЭК России) (см. сайт ФСТЭК http://www.fstec.ru (рис. 10).

Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (ред. от 22.05.2023) определено, что Федеральная служба по техническому и экспертному контролю, ее территориальные органы и подведомственные ей организации являются правопреемниками Гостехкомиссии России, ее территориальных органов и подведомственных ей организаций.

Кроме того, ФСТЭК России является органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну.

Федеральная служба по техническому и экспортному контролю (ФСТЭК) организует деятельность государственной системы защиты информации в Российской Федерации от технических разведок и от ее утечки по техническим каналам.

Приказы, распоряжения и указания ФСТЭК России, изданные в пределах ее компетенции, обязательны для исполнения аппаратами федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, предприятиями, учреждениями и организациями.

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам, в соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (рис. 11).

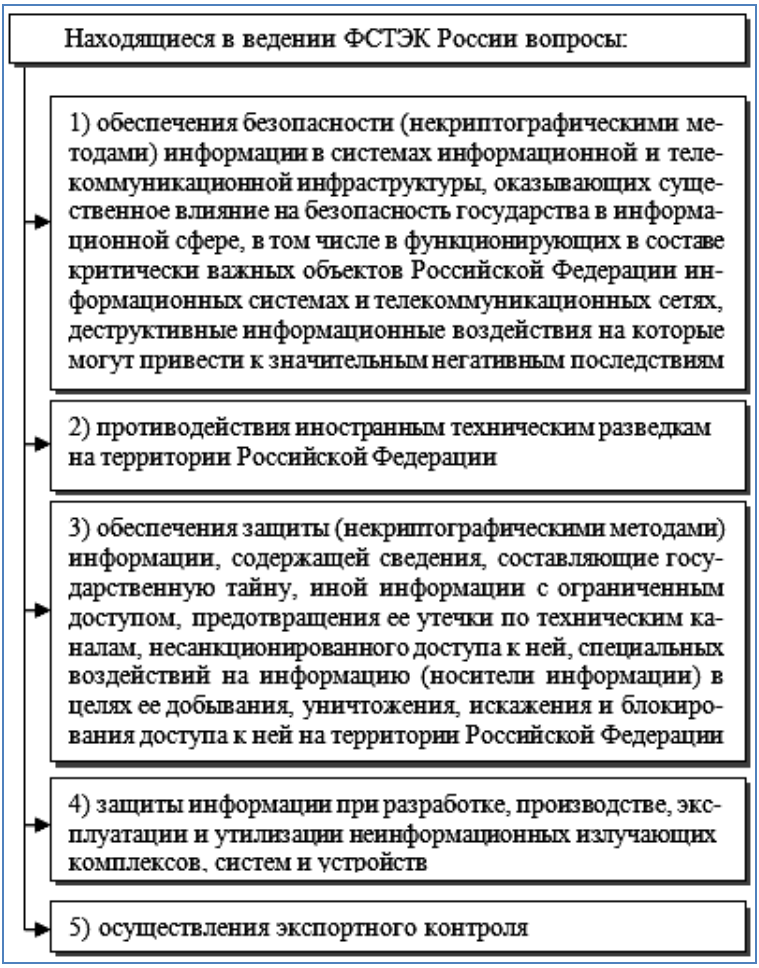

Рис. 11. Вопросы, находящиеся в ведении ФСТЭК России

Защита государственной тайны является видом основной деятельности органа государственной власти, предприятия, учреждения или организации.

2.3. СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ПОЛЕЗНЫЕ ССЫЛКИ

В обеспечении информационной безопасности, несомненно, важную роль играют нормативные правовые акты, стандарты информационной безопасности, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации. Перечень их весьма обширен, а с учетом того, что современные интернет-технологии позволяют обеспечить доступ к документам, актуальным на момент обращения, представляется целесообразным привести полезные ссылки на интернет-ресурсы, содержащие правовую базу, аналитику, материалы по обеспечению информационной безопасности, национальные стандарты в области информационной безопасности.

https://www.rst.gov.ru/portal/gost/home/standarts
РОССТАНДАРТ. Федеральное агентство по техническому регулированию и метрологии. Каталог национальных и международных стандартов с возможностью поиска по имеющейся базе. Действующие стандарты по направлению «Искусственный интеллект»

http://www.fstec.ru
Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России), федерального органа исполнительной власти, осуществляющего межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственную или служебную тайну, от её утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию и по противодействию техническим средствам разведки на территории Российской Федерации. Содержит нормативные правовые акты и информационные материалы.

https://fstec.ru/dokumenty/vse-dokumenty/perechni/natsionalnye-standarty
Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). Национальные стандарты Стандарты в области информационной безопасности.

http://www.azi.ru
Сайт Межрегиональной общественной организации «Ассоциация защиты информации» (АЗИ), деятельность которой направлена на создание благоприятных условий для реализации потребностей граждан, бизнеса и органов государственной власти в продуктах и технологиях защиты информации. АЗИ активно взаимодействует с аппаратом Совета Безопасности РФ, ФСБ России, ФСТЭК России, другими министерствами и ведомствами, а также со многими финансово-экономическими структурами. Содержит нормативные правовые акты и информационные материалы.

https://infolaw.su/
Электронная версия журнала «Информационное право». Представляет аналитические публикации по вопросам информационного права, в том числе защиты персональных данных, информационной безопасности.

http://www.itsec.ru/articles2/allpubliks
Электронный архив публикаций журнала «Информационная безопасность». Содержит информационно-аналитические материалы по вопросам защиты информации.

httphttp://www.itsec.ru/rass.php
Архив электронной газеты «Информационная безопасность». Содержит публикации по вопросам информационной безопасности.

http://www.secuteck.ru/articles2/allpubliks
Электронный архив публикаций журнала «Системы безопасности». Содержит информационно-аналитические материалы по вопросам защиты информации.

www.garant.ru
Интернет-версия системы «Гарант» (Правовая информационно-поисковая система).

www.consultant.ru
(Интернет-версия системы «КонсультантПлюс». (Правовая информационно-поисковая система).

3. СОВРЕМЕННЫЕ ПРОБЛЕМЫ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

3.1. НОВЫЕ ВЫЗОВЫ И УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Одной из первоочередных задач, стоящих перед мировым сообществом в XXI веке, является построение информационного общества. При этом, как уже сложившиеся, так и те общественные отношения, которые возникают при формировании такого общества, требуют правового регулирования, а также решения связанных с этим проблем.

На современном этапе развития общества, для которого характерно динамичное развитие и применение информационных технологий, неминуемо появляются проблемы, связанные с обеспечением защиты общества от использования этих технологий в преступных целях. Трансграничный характер преступности в сфере высоких технологий, обусловленный развитием глобальных информационных систем и, в первую очередь, Интернета, усложняет противодействие ей и представляет угрозу международной безопасности.

Согласно опубликованному на сайте РБК анализу за 2022 год, «в России количество утекших записей персональных данных и платежной информации выросло в 2,67 раза по сравнению с предыдущим годом и составило более 667 млн единиц, свидетельствуют данные исследования ГК InfoWatch «Россия: утечки информации ограниченного доступа в 2022» [28]. «Таким образом, – констатируют эксперты, – число скомпрометированных записей в прошлом году более чем в 4,5 раза превысило население страны. Причем каждая утечка в 2022 году по объему выросла на треть по сравнению с периодом годом ранее и содержала около 940 тыс. записей. Эксперты по кибербезопасности также отмечают: порядка 80% утечек имеют гибридный вектор воздействия, когда в краже информации могли участвовать как внешние, так и внутренние нарушители; вдвое выросла доля утечек информации категории «коммерческая тайна»; заметнее всего выросла доля утечек среди организаций отраслевой группы «Ретейл & HoReCa» – практически в пять раз, среди промышленных, транспортных и энергетических компаний – почти в три раза; на малый бизнес пришлось более 20% утечек – этот результат вдвое больше, чем в 2021» [28].

Проблема противодействия использованию возможностей информационно-телекоммуникационных технологий, которые могут

использоваться как для причинения ущерба интересам государства, общества, личности, так и для приготовления и совершения террористических актов, осуществления пропаганды терроризма и насильственного экстремизма, представляется весьма важной в связи с обязанностью государства по обеспечению защиты конституционных прав и свобод человека и гражданина в информационной сфере.

На современном этапе развития общества среди актуальных угроз информационной безопасности можно выделить следующие.

1. *Разработка, создание и использование средств воздействия и нанесения ущерба информационным ресурсам и телекоммуникационным системам государства*. *К таким средствам относятся*:

– средства, позволяющие осуществлять радиоэлектронное, а также иное воздействие, которые могут быт быть применены для не только временного, но и для необратимого подавления радиоэлектронных средств и систем;

– средства воздействия на программные ресурсы электронных управляющих модулей в целях их вывода из строя или изменения алгоритма их работы;

– средства, обеспечивающие воздействие на процесс передачи информации в целях его прекращения или дезорганизации за счет воздействия на среду распространения сигналов и алгоритмов функционирования;

– средства дезинформации, позволяющие создавать в информационном пространстве виртуальную картину обстановки, которая будет отличаться от действительности либо искажать ее;

– средства, обеспечивающие целенаправленное влияние на психическое состояние и подсознание людей, например, в целях дезорганизации, подавления воли и т.д.

2. *Целенаправленное информационное воздействие на критически важные структуры*. При этом могут быть созданы прямые угрозы национальной безопасности в результате применения информационного оружия в отношении как военных, так и сугубо гражданских объектов, систем и институтов государств, приводящие к нарушению нормального функционирования.

Так, например, несанкционированные воздействия на управляющие системы могут существенно повлиять на инфраструктуры, связанные с жизнеобеспечением, передачей энергии, ядерными объектами, управлением полетами и т.д., что может приводить катастрофе.

Несанкционированное получение информации о научно-технических разработках оборонного характера или двойного применения

может быть использовано например для незаконного производства в оружия (в том числе и с использованием методов 3D-печати), а также в террористических целях.

Несанкционированные воздействия (для кражи, искажения либо уничтожения информации) на информационные системы правоохранительных органов могут повлиять на обеспечение законности и правопорядка, снизить эффективность противодействия преступности.

Воздействия злоумышленников на информационные ресурсы в кредитно-финансовой сфере (в том числе позволяющие осуществить несанкционированный перевод, хищение банковских средств, незаконные операции со счетами, нарушение работы информационных систем и сетей банковских учреждений и сетей межбанковского обмена) оказывают негативное влияние на эффективную работу в этой сфере, приносят огромные убытки.

Применение информационного оружия для воздействия на инфраструктуру телекоммуникаций может привести к блокированию систем управления и принятия решений на уровне государства.

Деструктивное информационное воздействие на информационные системы транспорта, связи и управления противовоздушных, противоракетных и других систем обороны способно обезоружить государство перед лицом потенциального агрессора, существенно снизив его потенциальные возможности для самообороны.

К катастрофическим последствиям может привести нарушение производственного процесса на предприятиях повышенной технической и экологической опасности (с использованием радиоактивных материалов, химическое, биологическое, топливное производство).

Нарушение работы средств связи, процессов управления и функционирования транспорта, а также служб, задействованных для ликвидации негативных последствий стихийных бедствий, для спасения людей в чрезвычайных ситуациях, может привести к значительному материальному ущербу, гибели людей и усугубить ситуацию.

3. *Информационное воздействие* может быть осуществлено для подрыва политической, экономической и социальной системы и стабильности государств, психологического воздействия на граждан для достижения цели дестабилизации общества (яркими примерами тому являются, среди прочего, технологии «цветных революций»).

Использование целенаправленного информационного воздействия противоборствующими сторонами в условиях глобального информационного пространства ставит на качественно новый уровень

их современные возможности, усложняя тем самым решение задач по обеспечению информационной безопасности.

4. *Несанкционированное использование возможностей* информационно-телекоммуникационных систем путем неправомерного вмешательства в их работу. Информационные атаки такой направленности имеют тенденции к росту. Ни одно государство на сегодняшний день не застраховано от таких негативных действий.

Преступные группировки, отдельные хакеры, специальные подразделения для осуществления своих целей используют самые современные технологии в этой сфере, обобщают накопленный опыт, которым в некоторых случаях эффективно обмениваются, используя не только открытые, но и защищенные, скрытые каналы передачи такой информации, что затрудняет противодействие им, в том числе и со стороны правоохранительных органов.

В современном мире отмечается рост противоречий между потребностями общества, связанными с увеличением возможностей свободного доступа к информации и обмену ей, а с другой стороны, важностью определенных ограничений по доступу к определенной информации и обмену ей на законном основании.

Национальное законодательство многих стран весьма широко трактует вмешательство в информационные системы, а некоторые действия вообще не криминализируются.

Злоумышленники могут осуществлять противоправные действия по каналам трансграничных информационных сетей в отношении объектов, находящихся на территории другого государства (при этом оставаясь вне его юрисдикции), таким образом, затрудняя применение ответных мер.

Совершенствование технологической защиты информационных сетей, да и в целом обеспечение информационной безопасности в этой сфере, хотя и затратное с финансовой точки зрения, но, безусловно, необходимо.

Глобализация угроз в этой сфере, несомненно, должна привести к гармонизации, «синхронизации» национальных законодательств, путем выработки универсальных положений в рамках международно-правовой базы, определяющей ответственность за правонарушения в информационном пространстве.

5. *Деятельность как запрещенных международных террористических, экстремистских и преступных сообществ, организаций, групп, так и отдельных граждан*, которая представляет угрозу не только

информационным ресурсам, но и критически важным структурам государств.

Противоправность действий объединяет информационная преступность и информационный терроризм. Однако цели, преследуемые кибертеррористами, являются более опасными.

Для осуществления своих планов и совершения противоправных действий могут использоваться различные средства. С помощью специальных компьютерных программы, технических средств и технологий они имеют возможности для разрушения, искажения, манипулирования отдельными элементами информационной инфраструктуры, похищения важной информации, ее модификацию. При этом весьма опасным является вывод из строя систем связи (с помощью разного рода информационных атак), захват либо блокирование каналов СМИ, а также использование современных информационных средств в целях распространения дезинформации (панических слухов, угроз террористических актов и объявления собственных требований).

Кибертеррористы всегда стремятся получить широкий резонанс в обществе в ответ на свои действия, поэтому потенциальные возможности использования трансграничной информационной сети привлекают их.

6. *Использование информационных технологий и средств* во вред основным правам и свободам человека, реализуемым в информационной сфере.

Перед современным обществом все более остро возникают проблемы, обусловленные процессами информатизации, связанными с развитием информационных сетей, когда огромные массивы информации, например, касающиеся граждан и их личной жизни, могут быть доступны злоумышленникам. Но возможные угрозы здесь определяются не только доступностью определенной информации, но и напротив, возможным неправомерным ограничением доступа граждан к информации, гарантии доступа к которой, декларируются Конституцией, например, эта информация может касаться жизни, здоровья, безопасности, деятельности государственных органов и другой открытой социально и личностно значимой информации.

Гарантии запрещения сбора, хранения, использования, передачи и распространения информации о частной жизни человека (при отсутствии на то его согласия) должен обеспечивать режим международной информационной безопасности. Он также должен обеспечивать гарантии доступа граждан к информации, за исключением случаев, предусмотренных законом.

7. *Трансграничное распространение информации*, запрещенной к распространению согласно международным и национальным нормативным и правовым актам.

В данном контексте важную роль играет глобализация информационного пространства, которая оказывает существенное влияние на традиционные понятия, «размывая» географические, государственные, административные границы или зоны юрисдикции. Это определяет задачу четкого определения источников угроз как внутреннего, так и внешнего характера.

В таких условиях может возникать ситуация, когда обеспечивается правовой режим информационного обмена внутри государства, но оказывается сниженным уровень защиты от проникновения на свою территорию информации со стороны других государств, которая запрещена к распространению (информации деструктивного характера, информации направленной на разжигание социальной, национальной и религиозной вражды, информации, исходящей от террористических групп и т.д.).

При подготовке и совершении преступлений (например, предусмотренных статьями 206, 208, 211, 272-274, 277 УК РФ и рядом других) могут быть использованы глобальные компьютерные сети.

Конвенция о киберпреступности от 23.11.2001 г. играет значимую роль для расследования террористической и экстремистской деятельности, осуществляемой с применением информационно-телекоммуникационных технологий. Но следует отметить, что в силу несогласия Российской Федерации с некоторыми положениями Конвенции (а именно, п. b ст. 32 Конвенции, согласно которому любая из договаривающихся сторон может без согласия другой стороны получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным) наша страна не подписала этот документ и не участвует в названной Конвенции.

Определение юрисдикции сторон в отношении совершенных правонарушений является одной из существенных проблем правового регулирования в рассматриваемой сфере. Согласно положениям Статьи 22 упомянутой выше Конвенции, юрисдикция устанавливается по принципу территориальности (в том числе, принадлежности самолета или судна) или гражданства правонарушителя. Однако при этом нельзя не учитывать экстерриториальную сущность глобальных информационно-телекоммуникационных сетей.

В настоящее время в федеральном законодательстве существует тенденция к расширению сферы правового регулирования противодействия терроризму и экстремизму.

Наличие законодательно закрепленных норм, связанных с доступом к информации, влияет на позитивный эффект формирования в России системы раскрытия государственной информации, обеспечения прозрачности деятельности органов государственной власти, в том числе посредством размещения в глобальной сети Интернет всей информации, находящейся в распоряжении государственных органов, на которую не распространяется режим ограниченного доступа. Это во многом способствует обеспечению доступа граждан к информации, находящейся в распоряжении органов государственной власти и местного самоуправления.

Вопросы законодательного определения информации ограниченного доступа и критерии отнесения сведений к этому виду информации, а также определения границ между открытой и закрытой информацией имеют важнейшее значение.

Федеральным законом «Об информации, информационных технологиях и о защите информации» в статье 9 предусмотрены различные формы и условия ограничения доступа к информации.

Так, правовой режим секретной информации установлен Законом Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне». При этом следует отметить, что этот закон достаточно четко определяет порядок отнесения сведений к государственной тайне, тем не менее, судебная практика показывает, что проблемы реализации правовых норм имеют место. Перечень сведений, отнесенных к государственной тайне, на текущий момент определен Указом Президента РФ от 30.11.1995 № 1203 (ред. от 25.03.2021) [11].

Федеральный закон «Об информации, информационных технологиях и о защите информации» устанавливает условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну. Положительную роль при этом выполняет Указ Президента Российской Федерации от 6 марта 1997 г. № 188 (в ред. Указов Президента РФ от 23.09.2005 № 1111, от 13.07.2015 № 357) «Об утверждении Перечня сведений конфиденциального характера» (см. http://fstec.ru/component/attachments/download/280).

Интенсивное развитие информационных технологий, появление новых угроз на пути к информационному обществу ставит проблемы, которые еще предстоит решить не только нашей стране. При этом сле-

дует отметить, что к настоящему времени имеются все необходимые предпосылки для более скоординированных действий, направленных на их решение.

Среди основополагающих документов, которые затрагивают вопросы противодействия использованию информационных технологий в преступных целях можно назвать следующие: Окинавская хартия Глобального информационного общества, подписанная главами существовавшей на тот момент «восьмерки» от 22 июля 2000 г.; Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г.; Конвенция Совета Европы о киберпреступности от 23 ноября 2001 г.; Декларация принципов построения информационного общества, принятая на Всемирной встрече на высшем уровне в Женеве в декабре 2003 г. и другие. Важно отметить, что Окинавская хартия Глобального информационного общества содержит призыв, обращенный к международному сообществу, к согласованности действий по созданию безопасного и свободного от преступности киберпространства.

В рамочном решении Совета Евросоюза об атаках на информационные системы, подписанном еще 24 февраля 2005 г. в Брюсселе, было отмечено негативное влияние, которое оказывают различия и пробелы в законодательстве об обеспечении информационной безопасности государств – членов Европейского Союза. При этом была особенно подчеркнута необходимость защиты информационных систем и банков данных от преступных посягательств террористических групп и иных преступных организаций. В этом документе указывалось также на необходимость принятия совместных решений на уровне Европейского Союза, целью которых является недопущение срыва процесса создания безопасного информационного общества, а также формирования пространства свободы, безопасности и правосудия.

Динамичное развитие информационных технологий и активное использование их во многих сферах деятельности, к сожалению, расширяет и возможности совершения преступлений.

Так, в условиях развития информационных технологий возникает необходимость своевершенствования правового регулирования отношений, связанных с массовой рассылкой незапрашиваемых электронных сообщений (так называемым «спамом»). Нормативное определение понятия «спам» впервые было дано в постановлении Правительства РФ от 10 сентября 2007 г. № 575 «Об утверждении Правил оказания телематических услуг связи».

Массовую рассылку незапрашиваемых электронных сообщений нередко используют для распространения вредоносных программ, влекущих за собой несанкционированное блокирование, копирование информации, нарушение работы сети ЭВМ и прочее. Такая рассылка проводится без согласия получателя незапрашиваемой информации («спама») на использование его адреса и при сокрытии или замене информации, идентифицирующей лицо, от имени которого делается рассылка (или без указания действительного адреса, по которому получатель может направить требование о прекращении рассылки).

В соответствии со ст. 14.3 Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ за нарушение законодательства о рекламе на рекламораспространителя – юридическое лицо может быть наложен штраф.

В России существуют законы, защищающие пользователей от спама, например: Федеральный закон № 38 «О рекламе» от 13.03.2006 и федеральный закон № 152 «О персональных данных» от 27.07.2006. В обоих законах четко указано, что рассылка должна проводиться только с согласия получателя.

При этом существует определенная проблема правового регулирования интернет-пространства, заключающаяся в том, что отправителя сообщения и его получателя могут разделять тысячи километров и границы государств, в связи с чем не всегда возможно эффективно противодействовать спаму со стороны уполномоченных органов (например, отправитель спама по электронной почте зачастую находится вне их юрисдикции).

В нашей стане, исполняя положения государственной программы Российской Федерации «Информационное общество», были внесены изменения в Федеральный закон от 21 июля 2014 г. № 272-ФЗ «О связи», направленные на защиту абонентов от «спама» (незаказанных абонентом рассылок рекламного характера) и сетевого мошенничества (в котором среди прочего имеется требование «прекратить оказание услуг по пропуску по своей сети трафика, содержащего осуществляемую с нарушением требований настоящего Федерального закона рассылку»).

Методический документ «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.), Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных» и ряд других ведомственных документов на сегодняшний день содержат положения о необходимости принятия мер по защите информации от спама.

Наиболее детальное правовое регулирование проблема спама получило в США. С 2003 года там действует федеральный закон, получивший название Controlling the Assault of Non-Solicited Pornography and Marketing Act (более известный как CAN-Spam Act). Данным нормативным актом подробно регулируются отношения по распространению как рекламного спама, так и спама других видов. В данном законе прямо указывается, что отправителем спама (в частности, рекламного) признается либо лицо, его отправившее, либо тот, чьи товары или услуги рекламируются. Нормативным актом также устанавливается незаконность отправки сообщений пользователю без его согласия, а также при сообщении им о своем нежелании получать новые сообщения.

Очевидно, что вопрос о противодействии спаму не может и не должен быть решен в рамках одного государства [26].

Вопросы борьбы со «спамом» нашли отражение и в Декларации принципов построения информационного общества. «Спам» представляет для пользователей, сетей и в целом для Интернета серьезную проблему, масштабы которой, как указывается в Декларации, к сожалению, возрастают.

Среди разновидностей хакерских атак быстро набирают популярность так называемые DDoS-атаки (сокр. от англ. Distributed Denial of Service, Распределенный отказ обслуживания), т.е. множество запросов от огромного числа компьютеров со всего мира, зараженных вирусами. Цель атаки заключается не в том, чтобы проникнуть в систему, а в том, чтобы парализовать ее работу.

Технология, которая легла в основу этой разновидности хакерских атак, была создана исключительно в мирных целях. Она активно использовалась для изучения пропускной способности каналов передачи данных и для проверки их поведения в условиях пиковых нагрузок. Однако вскоре эта технология и инструменты попали в руки тех, кто нашел им иное применение.

Первые случаи хакерских DDoS-атак были зарегистрированы в 1996 г. В настоящее время DDoS стал гораздо большей проблемой, чем «спам». «Спам», как нежелательные почтовые рассылки, в глобальном масштабе – всего лишь незначительные помехи на уровне 1%.

Объем же DDoS-данных, как считают специалисты, достигает 5%, и последствия DDoS-атаки гораздо серьезнее.

По данным отчета, опубликованного CDN-провайдером Akamai Technologies о DDoS атаках, Австралия, Япония и Индия являются странами с наибольшим количеством атак на веб-приложения и API в регионе. DDoS-атаки на финансовые услуги в Европе увеличились на 73% в 2022 году.

[Финансовые услуги: Исследование Akamai https://tr-page.yandex.ru/translate?lang=en-ru&url=https%3A%2F%2Fwww.yahoo.com%2Fentertainment%2Ffinancial-services-akamai-research-shows-113200068.html]

В большинстве европейских стран и США приняты специальные акты, прямо и недвусмысленно определяющие хакерские атаки и ответственность за их реализацию. В Российском законодательстве наиболее близкие статьи УК: статья 272 «Неправомерный доступ к компьютерной информации» и статья 273 «Создание, использование и распространение вредоносных программ для ЭВМ» с максимальными сроками наказания пять и семь лет соответственно.

Позитивным является тот факт, что на уровне государства для планирования и осуществления государственной политики в сфере информационной безопасности в настоящее время наблюдается тенденция к выявлению проблем и угроз, которые уже имеются, а также будут оказывать существенное влияние в ближайшей перспективе. Положительную роль сыграло принятие Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры российской федерации» (ред. 10.07.2023 г.). Он регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (критической информационной инфраструктуры) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Так, в документе стратегического планирования Российской Федерации под названием «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» (Утверждены Указом Президентом Российской Федерации 12.04.2021 г., № 213) определяются основные угрозы в области международной информационной безопасности. При этом основные угрозы в области международной информационной безопасности связаны с использованием информационных и коммуникационных технологий (рис. 12).

Основные угрозы международной информационной безопасности:

а) использование информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности;

б) использование информационно-коммуникационных технологий в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) использование информационно-коммуникационных технологий в экстремистских целях, а также для вмешательства во внутренние дела суверенных государств;

г) использование информационно-коммуникационных технологий в преступных целях, в том числе для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества;

д) использование информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру

е) использование отдельными государствами технологического доминирования в глобальном информационном пространстве для монополизации рынка информационно-коммуникационных технологий, ограничения доступа других государств к передовым информационно-коммуникационным технологиям, а также для усиления их технологической зависимости от доминирующих в сфере информатизации государств и информационного неравенства.

Рис. 12. Основные угрозы международной информационной безопасности, связанные с использование информационных и коммуникационных технологий

3.2. ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В ОБЛАСТИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Действующие нормативные и правовые акты Российской Федерации задают вектор поступательного движения нашей страны, ориентированный на высокую степень интеграции Российской Федерации в мировое информационное общество.

«Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы» (утв. Указом Президента РФ 9 мая 2017 г. № 203) определяет цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Цели, национальне интересы и приоритеты, указанне в Статегии, напрямую связанные с проблемами обеспечения информационной безопасности:
- обеспечение безопасности граждан и государства;
- развитие свободного, устойчивого и безопасного взаимодействия граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления повышение эффективности государственного управления, развитие экономики и социальной сферы
- формирование информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений;
- развитие информационной и коммуникационной инфраструктуры Российской Федерации;
- создание и применение российских информационных и коммуникационных технологий, обеспечение их конкурентоспособности на международном уровне.

Таким образом, государство активно нацелено на формирование современной информационно-телекоммуникационной инфраструктуры, совершенствование системы государственных гарантий конституционных прав и свобод человека и гражданина в информационной сфере, противодействие использованию потенциала информационных технологий в целях угрозы национальным интересам России, совершенствование российскими специалистами информационных технологий, которые позволят добиться серьезного влияния на процессы развития глобальных общедоступных информационных сетей.

Процессы глобализации в настоящее время влияют на все без исключения страны современного мира. Глобальное информационное пространство таит в себе угрозы, с которыми не могут не считаться целые страны. Поэтому выработка основ государственной политики в области международной информационной безопасности, несомненно, важна, так как во многом определяет стратегическое планирование в этой сфере.

Указ Президента Российской Федерации от 12.04.2021 г. № 213 «*Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности*» – это документ стратегического планирования РФ, который отражает официальные взгляды на сущность международной информационной безопасности, определяет основные угрозы международной информационной безопасности, цель, задачи государственной политики РФ в области международной информационной безопасности, а также основные направления ее реализации.

Под **международной информационной безопасностью** понимается «такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности».

Система обеспечения международной информационной безопасности представляет собой совокупность международных и национальных институтов, регулирующих деятельность в глобальном информационном пространстве в целях предотвращения (минимизации) угроз международной информационной безопасности.

Цель государственной политики в области международной информационной безопасности – содействие установлению международно-правового режима, при котором создаются условия для предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве, а также для формирования с учетом национальных интересов Российской Федерации системы обеспечения международной информационной безопасности.

Достижение цели государственной политики в области международной информационной безопасности осуществляется путем решения задач по развитию на глобальном, региональном, многостороннем и двустороннем уровнях сотрудничества Российской Федерации с иностранными государствами по вопросам формирования системы обеспечения международной информационной безопасности, а также противодействия основным угрозам международной информационной безопасности.

Таким образом, Указ Президента Российской Федерации от 12.04.2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» утвердил основы государственной политики России

в области международной информационной безопасности. Они направлены:

– на продвижение российских подходов к формированию системы обеспечения международной информационной безопасности и российских инициатив в этой сфере;

– на содействие созданию международно-правовых механизмов предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве;

– на организацию межведомственного взаимодействия.

Основными угрозами в данной сфере являются использование IT-технологий в военно-политической и иной сферах для подрыва суверенитета государств, нарушения их территориальной целостности, а также в террористических, экстремистских и преступных целях.

Подготовка предложений по формированию, совершенствованию и реализации госполитики в области международной информационной безопасности, а также контроль за исполнением органами госвласти решений по вопросам координации деятельности в указанной сфере осуществляется органами Совета Безопасности РФ.

Информационная безопасность сегодня становится важнейшим компонентом национальной и международной безопасности, а информационные технологии стали одним из важнейших политико-экономических и военных ресурсов, дающих, с одной стороны, существенные преимущества тем, кто ими владеет, а с другой стороны увеличивают риски, связанные с возможными уязвимостями. Информационная сфера – весьма чувствительный фактор жизнедеятельности общества, глобализация информационных процессов повлекла за собой возникновение целого спектра проблем безопасности. Само понятие «информационная безопасность» превратилось из узкотехнического в широкоупотребительное.

Таким образом, совместная деятельность государств, реализующая приоритетные направления государственной политики в сфере обеспечения информационной безопасности, преследует своей целью более эффективную защиту их законных интересов в информационном пространстве.

3.3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА В УСЛОВИЯХ ЦИФРОВОЙ РЕАЛЬНОСТИ

Современные достижения в использовании и развитии информационных технологий, достижения, связанные с развитием технологий искусственного интеллекта, больших данных вносят огромный вклад в

развитие всех процессов, способствуют становлению новой «цифровой реальности».

Все, что тесно связано с безопасностью личности, общества, а также государства в условиях цифровой реальности невозможно отделить от такого понятия, как информационная безопасность, которое рассматривается в Доктрине информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [4].

Формируемая «цифровая реальность» базируется на последних достижениях, связанных с развитием информационных технологий, захватывая в свою сферу привычные, и вновь появляющиеся общественные отношения и институты. Уже никого не удивляют возможностями новой цифровой реальности, в том числе не имеющей аналогов в прежнем мире. Общество спешит воспользоваться Новыми возможности «цифровой реальности», становятся обыденными и уже не удивляют нас. Это касается и растущего потенциала использования Интернета вещей, криптовалюты, технологий криптозащиты, облачных технологий, например, не только для хранения информации, но и для идентификации личности, предоставления услуг и т.д.

Но мы должны прекрасно понимать, что появление этой цифровой реальности непосредственно связано с необходимостью эффективного решения старых и новых задач, адаптации человечества в изменяющихся условиях, когда появляющиеся технические, технологические, финансовые и иные возможности позволяют реализовать новые потребности личности, общества и государства. Но, к сожалению, это снова ведет к появлению определенных проблем у человечества. Бытует шутка, что «компьютер позволяет решать проблемы, которых до него просто не было».

Готовность к цифровой реальности, «зрелость» личности общества и государства, эффективность парирования и предупреждения существующих и возможных угроз в целом определяют ту «цену», те последствия, которые определяются в цифровой реальности. Чтобы не оказаться «мартышкой с гранатой», человечество должно осознавать, насколько это небезопасно, как например, при глобальном использовании технологий искусственного интеллекта.

Отсутствие правовой базы порождает «закон джунглей», но и наличие такой базы, если оно не отвечает существующей реальности, не является весьма позитивным.

Процесс активной цифровизации общественных отношений повлек за собой проблемы, связанные с тем, что называют «цифровыми правами», «информационными правами». Те гарантии в этой сфере, что дает нам Конституция Российской Федерации, приходится рассматривать уже на более высоком уровне, с учетом «цифровой реальности». В более сложном мире мы в полной мере должны не только иметь, но и безопасно реализовывать соответствующие права, среди которых можно выделить право на: создание, распространение информации, конфиденциальность, защиту персональных данных, использование возможностей информационно-телекоммуникационных сетей, а также использование и защиту цифровых произведений, неприкосновенность частной информационной сферы и др. [34].

«Хартия глобального информационного общества» (Окинава, 22 июля 2000 г.) в свое время явилась ответом на вызовы появляющейся «цифровой реальности» со стороны ведущих государств, осознавших обязательность признания и защиты «цифровых прав».

Являясь одним из важных документов, интегрирующим основные взгляды на обеспечение «цифровых прав», этот документ декларирует необходимость обеспечения должной политики государств и развития нормативной базы, благоприятствующих совместной работе, направленной на совершенствование глобальных информационных сетей с учетом недопущения действий, препятствующих всеобщему использованию сети, позволяющих сократить возможное отставание некоторых стран в цифровых технологиях, максимально обеспечить возможности людей в вопросах глобального доступа к цифровым технологиям и возможностям сети. Важно отметить, что в Хартии ведущими государствами было провозглашено единодушное согласие с основными принципами и подходами, которые касаются действенных возможностей защиты частной жизни, в том числе и при обработке персональных данных, в условиях осуществления свободного информационного обмена, развития и применения современных способов идентификации, электронной подписи, возможностей криптографических и иных средств позволяющих обеспечить безопасность и достоверность при обороте информации.

Кроме того, в Хартии констатируется обязательство государств обеспечивать согласованную политику по противодействию киберпреступности, обеспечению безопасного киберпространства, своевре-

менному информированию мировой общественности о возможных вызовах, угрозах и противодействию им.

В нашей стране основные права человека, гарантированные Конституцией и международно-правовыми актами (свобода выражения мнения, свобода получать и распространять информацию, независимо от публичных властей и вне зависимости от государственных границ; право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени; право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений и т.д.), находят свое отражение и конкретизируются в рамках законодательства, действующего в конкретных временных рамках [1]. И как справедливо указал Председатель Конституционного суда РФ Валерий Зорькин, «При этом законодатель призван обеспечить оптимальный уровень такой конкретизации. Он не должен забегать вперед, но и не должен отставать от запросов развития. Очевидно, наступило время конкретизации прав и свобод человека и гражданина применительно к цифровой реальности» [31].

С учетом того, что речь идет о «цифровых правах» в контексте конституционных прав и свобод, стоит отметить, что согласно ст. 2 Конституции РФ, «Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства». Поэтому задача государства – не только признавать, но и применительно к существующей реальности обеспечивать адекватную и своевременную защиту «цифровых прав».

Нельзя не согласиться с мнением Валерия Зорькина о том, что имеются существенные проблемы, в первую очередь, связанные с тем, что «существующее законодательство далеко не в полной мере отвечает потребностям времени, поскольку многие законы слабо связаны как с указанным базовым законом, так и между собой. В связи с этим информационное законодательство нуждается в систематизации, избавлении от повторов и приведении его понятийного аппарата в стройное, непротиворечивое состояние» [31].

К сожалению, отсутствие Информационного кодекса Российской Федерации не способствует такой систематизации законодательства. А ведь уже почти десятилетие назад эта идею попытались реализовать в подготовленной Институтом государства и права РАН в 2014 г. Концепции проекта Информационного кодекса Российской Федерации. «В основу концепции положено право граждан на информацию и формы его реализации. В советское время информационное право рассматривалось в качестве элемента административного права,

основным методом которого является метод императивных предписаний со стороны государственных органов». С учетом реалий нашего времени и основываясь на положениях действующей Конституции РФ, важным представляется выработка конституционно-правовой концепции информационного права на основе конституционного права граждан на информацию.

В условиях «цифровой реальности» централизованный подход и системные решения государства, несомненно, дают свои положительные плоды при решении проблем обеспечения безопасности личности, общества и государства. Особая роль здесь принадлежит Доктрине информационной безопасности Российской Федерации, Гражданскому кодексу РФ (часть 4), Федеральному закону «Об информации информационных технологиях и защите информации», Федеральному закону «О государственной тайне» и др.

Так, среди первоочередных задач и национальных интересов в информационной сфере в Доктрине информационной безопасности Российской Федерации в первую очередь указываются: «обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации».

Весьма важным является то, что Стратегия национальной безопасности Российской Федерации (утверждена Указом Президента РФ от 2 июля 2021 г. № 400) выделяет в качестве одного из национальных интересов России вопросы, связанные с аспектами безопасного информационного пространства, а также защиту нашего общества от деструктивного информационно-психологического воздействия. Документом также устанавливается перечень задач, решение которых позволит обеспечить информационную безопасность граждан, общества и государства (п. 57 Стратегии).

Еще в начале 2021 года Президент РФ поручил Правительству РФ и СПЧ разработать проект концепции обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве и проект плана мероприятий по реализации этой концепции, включающего меры по повышению цифровой грамотности граждан РФ и их обучению навыкам информационной безопасности и цифровой гигиены

(подп. «г» п. 3 перечня поручений Президента РФ от 28 января 2021 г. № Пр-133).

Сказанное выше весьма актуально. Так как, к большому сожалению, как это отмечается МВД в краткой характеристике состояния преступности в Российской Федерации за январь – март 2023 года «С использованием информационно-телекоммуникационных технологий совершается практически каждое третье преступление. При этом раскрываемость IT-преступлений возросла до 35,1%» [3].

Как было отмечено выше, роль законодательных мер в обеспечении безопасность личности, общества и государства в условиях цифровой реальности переоценить невозможно. Ведь, как известно, «Мудрый законодатель постарается предупредить преступление, чтобы не быть вынужденным наказывать за него». К сожалению, меры прогнозирования и планирования не смогли эффективно отреагировать на рост количества преступлений в рассматриваемой сфере.

Предупреждение преступлений в этой сфере в рамках системного подхода и особенностей предупреждения преступности должно осуществляется строго на принципах законности, научной обоснованности, гуманизма, своевременности и необходимой достаточности, системности.

Несомненно, «спасение утопающих» – это дело и самих «утопающих». Виктимологическая профилактика и предупреждение неотделимы от мероприятий, которые позволяют повысить правовой уровень граждан, обеспечить их цифровую грамотность, познакомить из с основами (как правовыми, так и иными) обеспечения информационной безопасности и «цифровой гигиены».

Обеспечение безопасности личности, общества и государства в условиях цифровой реальности – задача комплексная. Важно при этом не забывать, что безопасность оценивается по самому слабому звену в цепочке элементов обеспечения безопасности.

4. ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Под персональными данными обычно подразумевают различные сведения о физическом лице, такие как его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другую информацию.

Одним из принципов, лежащих в основе всех действий, связанных с оборотом информации, должен быть принцип законности. Поэтому важным является наличие соответствующей правовой основы в рассматриваемой сфере.

Правовую основу обращения с персональными данными физических лиц в целях реализации конституционных прав человека, в том числе права на неприкосновенность частной жизни, личную и семейную тайну составляет законодательство Российской Федерации в области персональных данных, которое основывается на Конституции Российской Федерации и международных договорах Российской Федерации и состоит из Федерального закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и других определяющих случаи и особенности обработки персональных данных федеральных законов.

В Федеральном законе от 27.07.2006 г. № 152-ФЗ «О персональных данных» определены основные понятия, связанные с персональными данными. Приведем ниже некоторые из них.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Знание определений используемых терминов позволяет правильно понимать и исполнять требования нормативных и правовых актов в этой сфере.

Весьма важно отслеживать и изменения в нормативных актах, в чем существенную помощь оказывают информационные ресурсы и информационные сообщения на сайтах таких ведомств, как Роскомнадзор (https://rkn.gov.ru/), ФСТЭК – Федеральная служба по техническому и экспортному контролю (https://fstec.ru/), ФСБ – Федеральная служба безопасности Российской Федерации, http://pravo.gov.ru/ – Официальный интернет-портал правовой информации и др.

Следует отметить, что к настоящему времени наработана весьма обширная правовая база, регулирующая работу с персональными данными. Отвечая на запросы времени, она постоянно уточняется и дополняется. Некоторые из таких документов, включая и Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных», приведены ниже.

Нормативные правовые акты в области персональных данных.

✓ Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

✓ Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных»;

✓ Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»;

✓ Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»;

✓ Постановление Правительства Российской Федерации от 29.06.2021 № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных»;

✓ Постановление Правительства РФ от 21.03.2012 № 211 (ред. от 15.04.2019) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

✓ Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.);

✓ Директива Европейского Союза № 2002/58/ЕС «О приватности и электронных коммуникациях»;

✓ Трудовой кодекс Российской Федерации от 30.12.2001 г. № 197-ФЗ – Глава 14 «Защита персональных данных работника»;

✓ Федеральный закон от 19.12.2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

✓ Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

✓ Федеральный закон Российской Федерации от 25.07.2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»;

✓ Федеральный закон от 30.12.2015 г. № 439-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»;

✓ Федеральный закон от 21.07.2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»;

✓ Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

✓ Указ Президента Российской Федерации от 30.05.2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»;

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

✓ Распоряжение Президента Российской Федерации от 10.07.2001 г. № 366-РП «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»;

✓ Постановление Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

✓ Постановление Правительства Российской Федерации от 03.11.1994 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использования атомной энергии и уполномоченном органе по космической деятельности»;

✓ Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

✓ Постановление Правительства Российской Федерации от 06.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

✓ Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

✓ Постановление Правительства РФ от 04.03.2010 г. № 125 «О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию»;

✓ Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

✓ Распоряжение Правительства Российской Федерации от 15.08.2007 г. № 1055-Р «О плане подготовки проектов нормативных актов, необходимых для реализации Федерального закона «О персональных данных»;

✓ Приказ ФСБ России от 09.02.2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации. Положение ПКЗ 2005)»;

✓ Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер

по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

✓ Приказ Минкомвязи России от 20.07.2017 г. № 373 «О признании утратившими силу приказов Министерства связи и массовых коммуникаций РФ» от 21 декабря 2011 № 346, от 28 августа 2015 № 315 и п. 9 приказа Министерства связи и массовых коммуникаций РФ от 24 ноября 2014 № 403.

Важно отметить, что в соответствии с частью 3 статьи 17 Конституции РФ «любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения.

«В Российской Федерации не должны издаваться законы, отменяющие или умаляющие права и свободы человека и гражданина» (Согласно части 2 статьи 55 Конституции РФ)

«Права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства». (Согласно части 3 статьи 55)

4.2. НЕКОТОРЫЕ ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» выделяет следующие основные принципы обработки персональных данных.

Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных», определяя принципы и условия обработки персональных данных, устанавливает общий запрет на обработку персональных данных без согласия субъекта персональных данных, закон предусматривает случаи, когда такое согласие не требуется. Отдельно регулируются отношения по обработке специальных категорий персональных данных (сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни). Обработка указанных категорий сведений не допускается без предварительного согласия субъекта персональных данных, за исключением случаев, когда персональные данные являются общедоступными, обработка данных необходима для обеспечения жизни и здоровья лица; обработка проводится в связи с осуществлением правосудия, а также иных обстоятельств.

Принципы обработки персональных данных

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.
2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.
6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Важнейшей гарантией прав субъекта персональных данных является обязанность операторов и третьих лиц, получивших доступ к персональным данным, обеспечивать их конфиденциальность (кроме случаев их обезличивания и общедоступных персональных данных), а также право субъекта персональных данных на защиту своих прав и законных интересов, в том числе на возмещение убытков и(или) компенсацию морального вреда в судебном порядке.

Контроль и надзор за обработкой персональных данных возложен на федеральный орган исполнительной власти, осуществляющий

функции по контролю и надзору в сфере информационных технологий и связи, который наделяется соответствующими правами и обязанностями. В частности, уполномоченный орган вправе осуществлять проверку информационной системы обработки персональных данных, предъявлять требования по блокированию, удалению недостоверных или полученных незаконным путем персональных данных, устанавливать постоянный или временный запрет на обработку персональных данных, проводить расследования в порядке административного производства о нарушениях закона.

Федеральный закон № 152-ФЗ устанавливает принципы трансграничной передачи данных, при которой должна обеспечиваться адекватная защита прав субъектов персональных данных.

Следует отметить, что в прошлом году в законе «О персональных данных» появились положения, которые ограничивают сбор персональных данных, если они не являются необходимыми для исполнения договора. Введена добровольная сдача биометрических данных. Такие же ограничения установлены и законом о защите прав потребителей, введена административная ответственность за нарушение этих норм.

Недопустимо, когда операторы персональных данных запрашивают избыточные сведения. Потребители часто сталкиваются с тем, что личные сведения становятся разменной монетой. Интерес к персональным данным потребителя нередко превалирует над интересом заключить договор.

Еще одно нововведение в законодательстве – это запрет на использование иностранных мессенджеров для передачи платежных документов или предоставления информации, которая содержит персональные данные. Их перечень утвержден Роскомнадзором и размещен на сайте ведомства.

Вот лишь некоторые важные изменения, которые необходимо учитывать при обработке персональных данных (ПД) с 1 марта 2023 года.

Новый порядок направления уведомлений об изменениях

Согласно новым правилам, оператор ПД обязан уведомить Роскомнадзор об изменениях представленных им ранее сведений об обработке ПД, произошедших за месяц, в срок не позднее 15 числа следующего месяца (ч. 7 ст. 22 Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных"). Подается уведомление в отношении всех изменений.

За невыполнение требований организацию могут привлечь к административной ответственности по ст. 19.7 КоАП РФ – оштрафовать на сумму до 5 тыс. руб.

Обязанность хранить доказательства уничтожения ПД в течение 3 лет

Вступили в силу и будут действовать до 1 марта 2029 года Требования к подтверждению уничтожения ПД (утв. Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 октября 2022 г. № 179).

С 1 марта 2023 года операторы при уничтожении ПД должны составить специальный документ – акт об уничтожении персональных данных.

Минимальный срок, в течение которого необходимо хранить акты об уничтожении ПД и выгрузку из журналов регистрации событий – 3 года.

За невыполнение требований возможно привлечение к ответственности по ч. 5 ст. 13.11 КоАП РФ. – Штраф за нарушение установлен в размере до 90 тыс. руб)

Правильное сообщение об утечке персональных данных

Вступил в силу Порядок взаимодействия Роскомнадзора и операторов ПД в рамках ведения реестра учета инцидентов в области ПД (утв. Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14 ноября 2022 г. № 187).

Под инцидентом следует понимать любой факт, повлекший неправомерную передачу (предоставление, распространение, доступ) ПД. Операторы обязаны уведомлять Роскомнадзор о таких фактах, повлекших нарушение прав субъектов ПД.

Уведомление может быть первичным (должно быть представлено в течение 24 часов) или дополнительным (предоставляется в течение 72 часов).

Первичное уведомление должно содержать сведения о произошедшем инциденте, его возможных причинах, предполагаемом вреде субъекту ПД, а также возможные меры по устранению вреда. *Дополнительное уведомление* должно содержать сведения о результатах внутреннего расследования инцидента с указанием виновных лиц в случае, если в ходе расследования они были выявлены.

Новые правила оценки вреда
Вступили в силу и будут действовать до 1 марта 2029 года Требования к оценке вреда, который может быть причинен субъектам ПД в случае нарушения Федерального закона "О персональных данных"
(утв. Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27 октября 2022 г. № 178).
Оценку вероятного вреда должно осуществлять лицо, ответственное за организацию обработки ПД либо созданная оператором комиссия. Для целей оценки вреда указанные субъекты определяют одну из степеней вреда, который может быть причинен субъекту ПД в случае нарушения Федерального закона "О персональных данных". Степени разделены на три категории: высокую, среднюю или низкую.
Результаты оценки необходимо зафиксировать в акте оценки вреда.
Если нарушение будет выявлено в ходе проводимой Роскомнадзором проверки, его нужно будет устранить. Роскомнадзор вправе выдать компании соответствующее предписание.

Следует не пренебрегать возможностью оперативно получать информацию о нововведениях в законодательстве и соответствующих разъяснениях специалистов на сайте Роскомнадзора на соответствующих страницах, например «Новости», «Персональные данные» и др.

4.3. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ЗАКОНА О ПЕРСОНАЛЬНЫХ ДАННЫХ

В случае нарушений требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» согласно действующему законодательству предусматриваются различные виды ответственности: дисциплинарная, административная, гражданско-правовая и уголовная ответственность (примеры представлены ниже).

Дисциплинарная ответственность
Нарушение: Разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника
Норма : Подпункт "в" п. 6 ч. 1 ст. 81 ТК РФ) *Санкция:* Увольнение

Нарушение: Иные нарушения в области персональных данных при их обработке
Норма: Статья 90 и 191 ТК РФ *Санкция:* Выговор, замечание

Гражданско-правовая ответственность
Нарушение: Причинение лицу убытков в результате нарушения правил обработки его персональных данных
Норма : Статья 15 ГК РФ
Санкция: Возмещение убытков

Нарушение: Причинение гражданину морального вреда (нравственных страданий) вследствие нарушения правил обработки персональных данных
Норма : Статья 24 Закона № 152-ФЗ, ст. 151 ГК РФ
Санкция: Компенсация морального вреда (независимо от возмещения имущественного вреда и понесенных субъектом убытков)

Административная ответственность за невыполнение требований законодательства в области обработки персональных данных установлена статьями:
- ст. 13.11 Кодекса Российской Федерации об административных правонарушениях (КоАП РФ) «Нарушение законодательства Российской Федерации в области персональных данных;
- ст. 19.4 КоАП РФ «Неповиновение законному распоряжению должностного лица органа, осуществляющего государственный надзор (контроль), должностного лица организации, уполномоченной в соответствии с федеральными законами на осуществление государственного надзора, должностного лица органа, осуществляющего муниципальный контроль»;
- ст. 19.4.1 КоАП РФ «Воспрепятствование законной деятельности должностного лица органа государственного контроля (надзора)», должностного лица организации, уполномоченной в соответствии с федеральными законами на осуществление государственного надзора, должностного лица органа муниципального контроля;
- ст. 19.5 КоАП РФ «Невыполнение в срок законного предписания (постановления, представления, решения)» органа (должностного лица), осуществляющего государственный надзор (контроль), организации, уполномоченной в соответствии с федеральными законами на осуществление государственного надзора (должностного лица), органа (должностного лица), осуществляющего муниципальный контроль;
- ст. 19.7 КоАП РФ «Непредставление сведений (информации)»;
Дела об административных правонарушениях, предусмотренных статьями 13.11, 13.14, 19.4, 19.4.1, 19.5, 19.7 КоАП РФ, возбуждаются уполномоченным органом и рассматриваются судом.

Уголовная ответственность
Норма : Статья 137 (ч.1, 2) УК РФ
Нарушение: Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации.

Спектр отношений, связанных с обработкой персональных данных, достаточно широк. Эти отношения регулируются действующим Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

При этом действие указанного Федерального закона не распространяется на отношения, возникающие при:

– обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

– организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

– обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

Следует отметить, что «предоставление, распространение, передача и получение информации о деятельности судов в Российской Федерации, содержащей персональные данные… осуществляются в соответствии с Федеральным законом от 22 декабря 2008 года № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

ЗАКЛЮЧЕНИЕ

Обеспечение информационной безопасности, защита информационного пространства России от современных угроз является одним из приоритетных направлений обеспечения национальной безопасности. Необходимо учитывать, что риски и угрозы в информационной сфере возрастают, поэтому за последние годы был сделан ряд важных шагов по обеспечению безопасности России в информационной сфере. Обеспечивая информационную безопасность, Российская Федерация осуществляет активное сотрудничество в рамках Организации Объединенных Наций, БРИКС, Шанхайской организации сотрудничества.

При этом необходимо отметить динамично меняющийся характер вызовов и угроз в этой сфере, значительный рост числа компьютерных атак международными террористическими организациями на органы государственной власти и бизнес-структуры во всех регионах мира, что требует развития и осуществления дальнейших мер противодействию им.

В настоящее время актуальными остаются задачи повышения защищенности информационных систем и сетей связи с использованием отечественных технических и программных средств обеспечения информационной безопасности.

Несомненно, что правовые, и в особенности доктринальные положения в сфере обеспечения информационной безопасности, должны в полной мере отвечать на динамично меняющийся характер вызовов и угроз в этой сфере, осуществляться в рамках гармонизации всего законодательства в рассматриваемой сфере.

СПИСОК ЛИТЕРАТУРЫ

1. **Конституция** Российской Федерации. Принята всенародным голосованием 12 декабря 1993 года // Собр. законодательства РФ. – 2009. – № 4. – Ст. 445.

2. **Всеобщая декларация** прав человека [Электронный ресурс] : принята на третьей сес. Генер. Ассамблеи ООН резолюцией 217 А (III) от 10 дек. 1948 г. // ГАРАНТ : информ.-правовой портал. – URL : http://base.garant.ru/10135532/ (дата обращения: 12.02.2023).

3. **Гражданский кодекс** РФ : федер. закон от 18.12.2006 г. № 230-ФЗ [Электронный ресурс]. – URL : http://base.garant.ru/10164072/

4. **Доктрина** информационной безопасности Российской Федерации (утв. Президентом РФ 05.12.2016 № Пр-1895) [Электронный ресурс]. – URL : http://www.kremlin.ru/acts/bank/41460

5. **Кодекс** Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 04.08.2023) [Электронный ресурс]. – URL : https://www.consultant.ru/document/cons_doc_LAW_34661/

6. **О государственной тайне** : закон РФ от 21.07.1993 № 5485-1 (ред. от 04.08.2023) [Электронный ресурс]. – URL : https://www.consultant.ru/document/cons_doc_LAW_2481/

7. **О коммерческой тайне** : федер. закон от 29.07.2004 № 98-ФЗ (ред. от 14.07.2022) [Электронный ресурс]. – URL : https://www.consultant.ru/document/ cons_doc_LAW_48699/

8. **О персональных данных** [Электронный ресурс] : федер. закон от 27 июля 2006 г. № 152-ФЗ : (с изм. и доп. от 06.02.2023) // КонсультантПлюс. : информ.-правовой портал. – URL : https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=439201&dst=1000000001&cacheid=3439D38F507D06E3CDCCD4DFFF51FF91&mode=splus&rnd=gfVvJQ#ezeBGqT0WdepO4dp

9. **О связи** : федер. закон от 07.07.2003 № 126-ФЗ (ред. от 04.08.2023) [Электронный ресурс]. – URL : https://www.consultant.ru/document/cons_doc_LAW_43224/

10. **Об информации**, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ (ред. от 31.07.2023) [Электронный ресурс] // ГАРАНТ : информ.-правовой портал. – URL : http://base.garant.ru/ 12148555/

11. **Об утверждении** Перечня сведений, отнесенных к государственной тайне : указ Президента РФ от 30.11.1995 № 1203 (ред. от 25.03.2021) [Электронный ресурс]. – URL : https://www.consultant.ru/document/cons_doc_LAW_8522/

12. **Об электронной подписи** : федер. закон от 06.04.2011 № 63-ФЗ (ред. от 04.08.2023) [Электронный ресурс]. – URL : https://www.consultant.ru/document/cons_doc_LAW_112701/

13. **Об утверждении** государственной программы Российской Федерации «Информационное общество» (с изменениями и дополнениями от 29.04.2023 г.) : постановление Правительства РФ от 15 апреля 2014 г. № 313 // Система ГАРАНТ. – URL : http://base.garant.ru/70644220/#block_31

14. **Стратегия** развития информационного общества в Российской Федерации : утв. Президентом РФ 7 февр. 2008 г. № Пр-212 // Рос. газ. – 2008. – 16 февр. – С. 16.

15. **Уголовный кодекс** Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 04.08.2023) [Электронный ресурс]. – URL : https://www.consultant.ru/document/cons_doc_law_10699/

16. Об утверждении перечня сведений, отнесенных к государственной тайне : указ Президента Российской Федерации от 30 ноября 1995 г. (в ред. Указа Президента РФ от 28.02.2016 г. № 90). – URL : http://pravo.gov.ru/proxy/ips/?docbody=&nd=102038480

17. **Об утверждении** Перечня сведений конфиденциального характера : указ Президента Российской Федерации от 6 марта 1997 г. № 188 (в ред. Указов Президента РФ от 23.09.2005 № 1111, от 13.07.2015 № 357) [Электронный ресурс]. – URL : http://fstec.ru/component/attachments/download/280 /

18. **О свободе** совести и о религиозных объединениях : федер. закон от 26.09.1997 № 125-ФЗ (ред. от 24.08.2023 г.) [Электронный ресурс]. – URL : http://ivo.garant.ru/#/document/171640/paragraph/20608:6

19. **Об информации**, информатизации и защите информации : федер. закон от 20 февраля 1995 года № 24-ФЗ [Электронный ресурс]. – URL : http://base.consultant.ru/

20. **Бачило, И. Л.** Информационное право : учебник / И. Л. Бачило. – М. : Высшее образование, Юрайт-Издат, 2009. – 454 с.

21. **Дементьев, О. М.** Развитие мошенничества в киберпространстве как тенденция совершенствования преступности / О. М. Дементьев, М. М. Дубровина, М. А. Ментюкова // Ассоциация «Объединенный университет имени В. И. Вернадского». «Вопросы современной науки и практики. Университет им. В. И. Вернадского». – 2015. – № 3(57). – С. 240 – 246.

22. **Комментарий** к Конституции Российской Федерации / под общ. ред. Л. В. Лазарева. – М. : Проспект, Новая правовая культура, 2009. – 816 с.

23. **Кочеткова, М. Н.** Конституционные основы охраны авторских прав в сети Интернет / М. Н. Кочеткова, Э. В. Сысоев // Вопр. соврем. науки и практики. Ун-т им. В. И. Вернадского. – 2014. – № 2(51). – С. 195 – 200.

24. **Кочеткова, М. Н.** Правовые проблемы защиты авторских прав на произведения, полученных в результате издания по требованию (Print on Demond Publishing) / М. Н. Кочеткова ; под ред. профессора И. М. Рассолова, С. Г. Чубукова // Юридическая наука как основа правового обеспечения интонационного развития России (Кутафинские чтения) : материалы секции информационного права Междунар. науч.-практ. конф. : сб. докл. Москва, 29 ноября 2011 г. – Киров : ООО «Типография Старая Вятка», 2012.

25. **Кочеткова, М. Н.** Технические и правовые проблемы защиты авторских прав на литературные произведения, распространяемые в сети Интернет / М. Н. Кочеткова, Э. В. Сысоев // Вопросы современной науки и практики

Университет им. В. И. Вернадского. – 2014. – № 3(53. – С. 153 – 159. – URL : http://vernadsky.tstu.ru/ru/vjpusk/2014/vjpusk-03.php

26. **Попов, Р. М.** Некоторые проблемы правового регулирования спама / Р. М. Попов // Гражданин и право. – 2013. – № 7.

27. **Правовое обеспечение** информационной безопасности : методические указания / сост. : А. В. Терехов, Е. В. Бурцева. – Тамбов : Изд-во ГОУ ВПО ТГТУ, 2010. – 16 с.

28. **Интернет-портал** «РБК» [Электронный ресурс]. – URL : https://www.rbc.ru/technology_and_media/17/04/2023/643936229a7947134f0ce21c

29. **Интернет-портал** «РИАНОВОСТИ». [Электронный ресурс]. – URL : http://ria.ru/defense_safety/20141001/1026452834.html

30. **Рассолов, И. М.** Информационное право / И. М. Рассолов. – М. : Норма : ИНФРА-М, 2010. – 352 с.

31. **Российская газета** RGRU [сайт] : Зорькин: Задача государства – признавать и защищать цифровые права граждан – URL : https://rg.ru/2018/05/29/zorkin-zadacha-gosudarstva-priznavat-i-zashchishchat-cifrovye-prava-grazhdan.html (дата обращения: 05.05.2023).

32. **Статистика** киберпреступлений 2023 [Электронный ресурс]. – URL : https://clickfraud.ru/statistika-kiberprestuplenij-2022/ (дата обращения: 05.05.2023).

33. **Терехов, А. В.** Использование программного обеспечения с открытым кодом в деятельности государственных органов / А.В. Терехов // Вопросы современной науки и практики. Университет им. В. И. Вернадского. – Тамбов, 2013. – Спец. вып. (44). – С. 126 – 131.

34. **Терехов, А. В.** Конституционные права и свободы как основа формирования информационного общества / А. В. Терехов // Вопросы современной науки и практики. Университет им. В. И. Вернадского. –Тамбов, 2014. – Спец. вып. (49). – С. 117 – 122.

35. **Терехов, А. В.** Проблемы информационной безопасности в информационном обществе / А. В. Терехов // Вопросы современной науки и практики. Университет им. В. И. Вернадского. – 2015. – № 1(55)/2015. – С. 103 – 107.

36. **Защита** компьютерной информации : учебное пособие / А. В. Терехов, В. Н. Чернышов, А. В. Селезнев, И. П. Рак. – Тамбов : Изд-во ТГТУ, 2003. – 80 с.

37. **Терехов, А. В.** Правовые аспекты использования цифровых технологий и обеспечения кибербезопасности / А. В. Терехов, А. М. Арестова // Инновационная юриспруденция: Вопросы теории и практики : сб. науч. тр. по материалам II Междунар. науч.-практ. конф. – Тамбов : Издательство Першина Р.В., 2022. – С. 85 – 89.

38. **Терехов, А. В.** Информационная безопасность в России: проблемы и решения / А. В. Терехов // Тамбовские правовые чтения имени Ф. Н. Плевако : материалы V Междунар. науч.-практ. конф. 28–29 мая 2021 года : в 2 т. ; М-во науки и высш. обр. РФ и др. ; отв. ред. В. Ю. Стромов. – Тамбов : Издательский дом «Державинский», 2021. – . С. 293 – 296.

39. **Терехов, А. В.** Правовые аспекты защиты персональных данных / А. В. Терехов, А. В. Парамонов // Тамбовские правовые чтения имени Ф. Н. Плевако : материалы V Междунар. науч.-практ. конф. 28–29 мая

2021 года : в 2 т. / М-во науки и высш. обр. РФ и др. ; отв. ред. В. Ю. Стромов. – Тамбов : Издательский дом «Державинский», 2021. – С. 274 – 277.

40. **Число** преступлений в сфере IT в России выросло в 10 раз за 6 лет [сайт] : Интерфакс.– URL : https://www.interfax.ru/russia/754322 (дата обращения: 15.05.2023).

41. **Шендрик, А. И.** Информационное общество и его культура: противоречия становления и развития. Опубликовано на Информационном гуманитарном портале «Знание. Понимание. Умение» 2014. [Электронный ресурс] / А. И. Шендрик. – URL : http://www.zpu-journal.ru/e-zpu/2010/4/Shendrik

ОГЛАВЛЕНИЕ

Учебное электронное издание

ТЕРЕХОВ Алексей Васильевич
ЧЕРНЫШОВ Владимир Николаевич
ПЛАТЕНКИН Алексей Владимирович
СЕЛЕЗНЕВ Андрей Владимирович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Учебное пособие

Редактирование И. В. Калистратовой
Графический и мультимедийный дизайнер Т. Ю. Зотова
Обложка, упаковка, тиражирование И. В. Калистратовой

ISBN 978-5-8265-2648-4

Подписано к использованию 02.10.2023.
Тираж 50 шт. Заказ № 114

Издательский центр ФГБОУ ВО «ТГТУ»
392000, г. Тамбов, ул. Советская, д. 106, к. 14
Тел./факс (4752) 63-81-08.
E-mail: izdatelstvo@tstu.ru