

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное
учреждение высшего образования
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра «Информационная безопасность»

МЕЖДУНАРОДНЫЕ И РОССИЙСКИЕ НОРМАТИВНЫЕ АКТЫ И СТАНДАРТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие
для студентов очной
и очно-заочной форм обучения

Севастополь
СевГУ
2025

УДК 004.056.5:34(075.8)
ББК 32.973-018.2:67я73
М433

Р е ц е н з е н т :

Ю. Ю. Эндрожикевич - д-р. техн. наук, доцент,
профессор кафедры «Информационная безопасность»

Составитель: Е. А. Контылева

М433 Международные и российские нормативные акты и стандарты по информационной безопасности : учебно-методическое пособие для студентов очной и очно-заочной форм обучения / Севастопольский государственный университет ; сост.: Е. А. Контылева. – Севастополь : СевГУ, 2025. – 141 с. – Текст : электронный.

Учебно-методическое пособие раскрывает актуальность нормативно-правового обеспечения информационной безопасности, представляющее собой совокупность законодательных актов и нормативов, регламентирующих общую организацию работ по защите информации, создание и функционирование систем защиты информации.

Рассматривается организационное обеспечение информационной безопасности, которое состоит из системы государственных органов и должностных лиц, ответственных за организацию работ и обеспечение информационной безопасности, а также контролирующих и судебных органов, осуществляющих надзор и решение правовых вопросов в данной области.

УДК 004.056.5:34(075.8)
ББК 32.973-018.2:67я73

Рассмотрено и рекомендовано к изданию на заседании кафедры «Информационная безопасность», протокол № 9 от 27 марта 2025 г.

© © Контылева Е. А., сост., 2025
© ФГАОУ ВО «Севастопольский
государственный университет», 2025

СОДЕРЖАНИЕ

Введение	5
Список сокращений	6
1. Государственная система обеспечения информационной безопасности	7
1.1. Структура государственной системы обеспечения информационной безопасности	10
1.2. Структура нормативных правовых актов в области информационной безопасности	17
2. Государственные органы обеспечения информационной безопасности Российской Федерации	23
2.1. Совет Безопасности Российской Федерации	23
2.2. Комиссия Совета Федерации по информационной политике	25
2.3. Федеральные органы исполнительной власти в области информатизации	26
2.4. Межведомственная Комиссия по защите государственной тайны	27
2.5. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации	28
2.6. Федеральная служба безопасности Российской Федерации	29
2.7. Федеральная служба по техническому и экспортному контролю	31
2.8. Федеральная служба охраны Российской Федерации	42
2.9. Служба внешней разведки Российской Федерации	44
2.10. Федеральное агентство по информационным технологиям	46
2.11. Федеральная служба по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия	48
2.12. Федеральная служба по интеллектуальной собственности, патентам и товарным знакам	49
2.13. Федеральное агентство по техническому регулированию и метрологии	51

3. Международные профессиональные объединения	54
3.1. Международная организация по стандартизации – International Organization for Standardization (ISO)	55
3.2. Международная электротехническая комиссия (МЭК/IEC)	56
3.3. Британский институт стандартов (BSI)	57
3.4. Институт инженеров по электронике и электротехнике – Institute of Electrical and Electronics Engineers (IEEE)	58
3.5. Ассоциация вычислительной техники – Association for Computing Machinery (ACM)	59
3.6. Консорциум Всемирной Паутины – World Wide Web Consortium (W3C)	61
3.7. Международный союз электросвязи – International Telecommunication Union (ITU)	62
3.8. Организация Объединенных Наций	66
3.9. Совет Европы (комитет министров)	69
4. Основные нормативно-правовые документы в области ИБ	70
Вопросы	115
Выводы	119
Список рекомендуемой литературы	120
Интернет-ресурсы	126
Приложение 1	127
Приложение 2	128
Приложение 3	134

ВВЕДЕНИЕ

В современном обществе информационная безопасность является важнейшим компонентом национальной, региональной и международной безопасности. Информацией и ИКТ всё чаще начинают использоваться в качестве определённых угроз интересам конкурентов. Всё явственнее проявляется стремление различных субъектов (коалиций, государств, организаций, личностей) к единоличному обладанию информационными ресурсами, средствами и технологиями, и их использованию в целях удовлетворения собственных интересов и противодействия интересам вероятных конкурентов в экономическом, коммерческом и даже военном противоборстве. По существу это обстоятельство и породило проблему информационной безопасности, которая обусловлена возрастающей ролью информации в общественной жизни.

В Концепции национальной безопасности РФ, среди важных задач обеспечения национальной безопасности, сформулирована задача укрепления безопасности в информационной сфере, представляющей собой специфическую сферу деятельности субъектов, связанную с созданием, хранением, распространением, передачей, обработкой и использованием информации, и являющейся одной из важнейших составляющих не только России, но и современного общества любого развивающегося государства.

Защищённость национальных интересов РФ в информационной сфере определяется совокупностью сбалансированных интересов личности, общества, и государства и является самостоятельной составляющей национальной безопасности и оказывает непосредственное влияние на защищённость интересов личности, общества государства РФ. Проникая во все сферы деятельности общества и государства, информация приобретает конкретные политические, материальные и стоимостные выражения. В связи с этим принимаются законы и нормативные акты для контроля информации и обеспечения информационной безопасности государства.

СПИСОК СОКРАЩЕНИЙ

Гос. – государственный

ГОСТ – государственный стандарт

Гостехкомиссия – Государственная техническая комиссия

ЗБ (ST) – задание по безопасности

ИСО – Международная организация по стандартизации

МЭК – Международная электротехническая комиссия

ОСТ – отраслевой стандарт

ПД (ПДн) – персональные данные

ПО – программное обеспечение

ПРД – правила разграничения доступа

РФ – Российская Федерация

СВТ – средства вычислительной техники

СЗИ – средства защиты информации

СТР – специальные требования и рекомендации

ТЗ – техническое задание

ТУ – технические условия

ФЗ – Федеральный закон

ФС – Федеральное собрание

ФСБ – Федеральная служба безопасности

ФСТЭК – Федеральная служба по техническому и экспертному контролю

CSE – Институт безопасности коммуникаций (канадская Организация по безопасности ИТ)

СТСРЕС – канадские критерии оценки надежного программного продукта (издаваемые CSE)

ITSEC – европейский стандарт оценки безопасности компьютерных систем

ITSEM – методология оценки безопасности информационных технологий

HCD – проектирование, основанное на участии человека

NSA – Агентство национальной безопасности (США)

1. ГОСУДАРСТВЕННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В современном информационном обществе информация является ценнейшим товаром. Развитие информационных технологий неразрывно связано с разработкой средств обеспечения информационной безопасности, в том числе и правовых. По мере развития и усложнения средств обработки информации безопасность общества все в большей степени зависит от безопасности используемых информационных технологий.

Современный этап развития системы обеспечения информационной безопасности государства и общества характеризуется переходом от тотального сокрытия большого объема сведений к гарантированной защищенности принципиально важных данных, обеспечивающей:

- конституционные права и свободы граждан, предприятий и организаций;
- необходимый уровень безопасности информации, подлежащей защите;
- защищенность систем формирования и использования информационных ресурсов (технологий, систем обработки и передачи информации).

Ключевым моментом политики государства в данной области является осознание необходимости защиты любых информационных ресурсов и информационных технологий, неправомерное обращение с которыми может нанести ущерб их собственнику, владельцу, пользователю или иному лицу.

Нормативно-правовое обеспечение информационной безопасности представляет собой совокупность законодательных актов и нормативов, регламентирующих общую организацию работ по защите информации, создание и функционирование систем защиты информации.

Организационное обеспечение информационной безопасности состоит из системы государственных органов и должностных лиц, ответственных за организацию работ и обеспечение информационной безопасности, а также контролирующих и судебных органов, осуществляющих надзор и решение правовых вопросов в данной области.

В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся:

- акты федерального законодательства;
- 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;
- международные стандарты информационной безопасности;
- государственные (национальные) стандарты РФ;
- рекомендации по стандартизации;
- методические указания.

Федеральные законы и другие нормативные акты предусматривают разделение информации на категории свободного и ограниченного доступа, причем информация ограниченного доступа подразделяется:

- на отнесенную к государственной тайне;
- отнесенную к служебной тайне (информацию для служебного пользования), персональные данные (и другие виды тайн);
- и другую информацию, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу;
- правовой режим защиты информации, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу, устанавливаемый:
 - в отношении сведений, отнесенных к государственной тайне, - уполномоченными государственными органами на основании Закона

Российской Федерации "О государственной тайне" (от 21.07.93 г. N 5485-1, ред. от 29.07.2018);

- в отношении конфиденциальной документированной информации - собственником информационных ресурсов или уполномоченным лицом на основании Закона Российской Федерации "Об информации, информатизации и защите информации" (от 20.02.95 г. N 24-ФЗ, ред. от 10.01.2003);

- в отношении персональных данных - отдельным федеральным законом;

- лицензирование деятельности предприятий, учреждений и организаций в области защиты информации;

- аттестование автоматизированных информационных систем, обрабатывающих информацию с ограниченным доступом на соответствие требованиям безопасности информации при проведении работ со сведениями соответствующей степени конфиденциальности (секретности);

- сертификацию средств защиты информации и средств контроля эффективности защиты, используемых в АС;

- возложение решения вопросов организации лицензирования, аттестации и сертификации на органы государственного управления в пределах их компетенции, определенной законодательством Российской Федерации;

- создание автоматизированных информационных систем в защищенном исполнении и специальных подразделений, обеспечивающих защиту информации с ограниченным доступом, являющейся собственностью государства, а также осуществление контроля защищенности информации и предоставление прав запрещать или приостанавливать обработку информации в случае невыполнения требований по обеспечению ее защиты;

- определение прав и обязанностей субъектов в области защиты информации.

В зависимости от приложения деятельности в области защиты информации (в рамках государственных органов власти или коммерческих

организаций), сама деятельность организуется специальными государственными органами (подразделениями), либо отделами (службами) предприятия.

Государственные органы РФ, контролирующие деятельность в области защиты информации:

- комитет государственной думы по безопасности;
- совет безопасности России;
- федеральная служба по техническому и экспортному контролю (ФСТЭК);
- федеральная служба безопасности России (ФСБ России);
- министерство внутренних дел Российской Федерации (МВД России);
- федеральная служба надзора в сфере информационных технологий и массовых коммуникаций (Роскомнадзор).

Службы, организующие защиту информации на уровне предприятия:

- служба экономической безопасности;
- служба безопасности персонала (Режимный отдел);
- отдел кадров;
- служба информационной безопасности.

Согласно требованиям нормативно-правовых документов на уровне учреждений должен также действовать комплекс нормативных актов по обеспечению защиты информации. В состав документов уровня предприятия входит также проектная и эксплуатационная документация по создаваемым и эксплуатируемым объектам информатизации, инструкции и регламенты по эксплуатации информационных систем и средств защиты, а также организационно-распорядительная документация предприятия (приказы, распоряжения, должностные инструкции сотрудников и др.).

1.1. Структура государственной системы обеспечения ИБ

Система обеспечения информационной безопасности Российской Федерации является частью системы обеспечения национальной

безопасности государства. Организационная структура системы обеспечения информационной безопасности представлена на рис. 1.1.

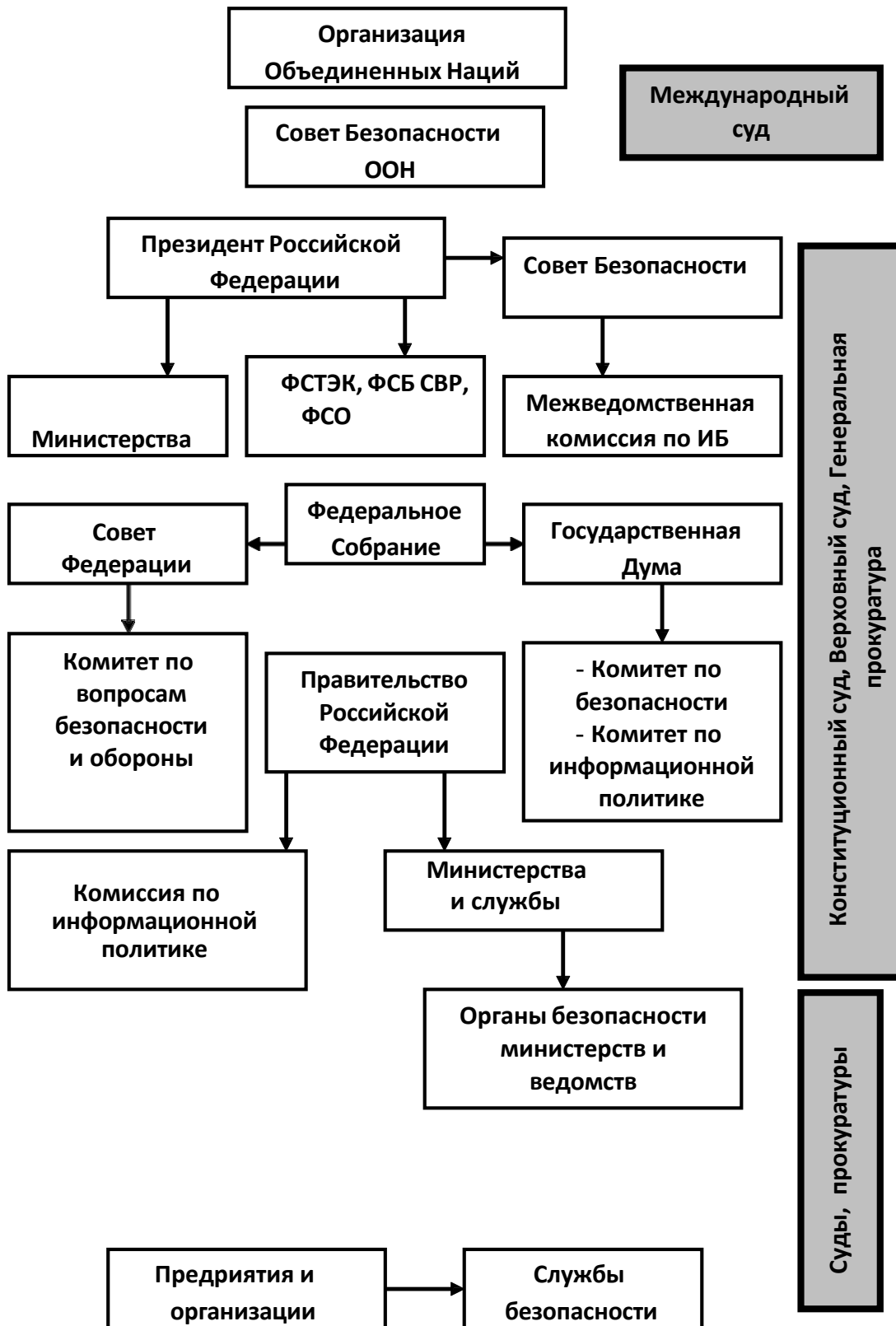


Рис. 1.1 Структура органов обеспечения информационной безопасности

Учитывая глобальный характер процессов информатизации и появление международной киберпреступности, мировое сообщество должно иметь межгосударственные организационные структуры по координации работ в области информационной безопасности.

Основным международным органом является Организация Объединенных Наций и созданный ею Совет Безопасности. Эти органы координируют усилия государств по осуществлению мероприятий в области обеспечения информационной безопасности и борьбе с преступлениями в сфере информационных технологий. Спорные вопросы на межгосударственном уровне решает международный суд.

Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти федерального уровня, уровня субъектов Российской Федерации, ведомственных структур, а также служб предприятий и организаций.

Основными элементами организационной структуры системы обеспечения информационной безопасности Российской Федерации на федеральном уровне являются:

- Президент Российской Федерации;
- Совет Безопасности;
- Совет Федерации;
- Государственная Дума;
- Правительство Российской Федерации;
- федеральные органы исполнительной власти;
- государственные и межведомственные комиссии, создаваемые

Президентом и Правительством Российской Федерации для решения вопросов в соответствии с предоставленными им полномочиями, определяемыми Положениями о комиссиях.

Федеральные министерства и ведомства могут в своем составе создавать соответствующие службы и подразделения для решения вопросов обеспечения информационной безопасности на отраслевом уровне.

Контролирующими и правоохранительными органами федерального уровня, обеспечивающими соблюдение нормативно-правовых норм, являются:

- Конституционный суд;
- Верховный суд;
- Генеральная прокуратура.

Следующим уровнем в системе обеспечения информационной безопасности являются органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, которые могут также создавать различные комиссии.

Наконец, нижним уровнем системы обеспечения информационной безопасности являются структурные подразделения и должностные лица предприятий и организаций.

Информацию об органах государственной власти Российской Федерации можно получить на информационном портале «Сервер органов государственной власти Российской Федерации» <http://www.gov.ru>. Он содержит ссылки на сайты федеральных и региональных органов исполнительной власти, а также сайты Президента, Федерального Собрания (Совета Федерации и Государственной думы), Совета Безопасности, Генеральной прокуратуры, Конституционного, Верховного и Арбитражного судов Российской Федерации, Счетной Палаты, Центральной избирательной комиссии.

Президент Российской Федерации (<http://www.kremlin.ru>) в пределах своих полномочий создает, реорганизует и руководит органами по обеспечению информационной безопасности, определяет приоритетные направления государственной политики в данной области.

Совет Безопасности Российской Федерации (<http://www.scrf.gov.ru>) является конституционным совещательным органом, осуществляющим подготовку решений Президента Российской Федерации по вопросам обеспечения

защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, проведения единой государственной политики в области обеспечения национальной (в том числе информационной) безопасности.

Правовую основу деятельности Совета Безопасности составляют Конституция Российской Федерации, федеральные законы Российской Федерации, международные договоры Российской Федерации, указы и распоряжения Президента Российской Федерации, а также Положение о Совете Безопасности, утверждаемое Президентом Российской Федерации.

Совет Безопасности проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации, разрабатывает важнейшие концептуальные документы в области национальной безопасности и предложения в области обеспечения информационной безопасности, координирует деятельность органов по обеспечению информационной безопасности, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации решений Президента в этой области.

Указом Президента от 28 октября 2005 года № 1244 «Об утверждении Положения о Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности» (с изменениями от 12 июня 2006 года) утверждено Положение о специальной Межведомственной комиссии при Совете Безопасности по информационной безопасности.

Палаты Федерального Собрания (Совет Федерации и Государственная Дума) формируют систему законодательных актов области информационной безопасности в соответствии с Конституцией Российской Федерации.

Совет Федерации имеет комитет по вопросам безопасности и обороны и комиссию по информационной политике. Комиссия по информационной политике создана Постановлением Совета Федерации от 30 января 2002 года

№ 106. Ее создание было обусловлено необходимостью детального изучения и мониторинга информационной ситуации, а также требованиями дальнейшего совершенствования законодательной базы в интересах большей ее

ориентации на формирование единого информационного пространства, решения других вопросов информационной политики Российской Федерации.

К предмету ведения комиссии были отнесены следующие вопросы правового обеспечения:

- государственная политика в сфере средств массовой информации, информационных технологий и информатизации;
- развитие единого информационного пространства Российской Федерации;
- издательская и полиграфическая деятельность;
- информационный обмен, развитие компьютерных сетей общего пользования;
- распространение периодических изданий, книжной и иной печатной, аудио- и видеопродукции;
- межгосударственное сотрудничество в информационной сфере.

В составе Государственной Думы сформированы два комитета: Комитет по безопасности и Комитет по информационной политике.

Правительство Российской Федерации координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, обеспечивает разработку и реализацию федеральных программ в области информационной безопасности. Функции Правительства определены Федеральным Конституционным законом «О Правительстве Российской Федерации» от 17 декабря 1997 года № 2-ФКЗ, (ред. от 28.12.2016) с последующими уточнениями и изменениями конституционными законами от 02.03.2007 № 3-ФКЗ, (ред. от 30.10.2018). Сайт Правительства Российской Федерации: <http://www.government.ru/>.

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

Указом Президента Российской Федерации от 20 мая 2004 года № 649 «Структура федеральных органов исполнительной власти» (ред. от 25.08.2010, с изм. от 30.04.2016) утверждены следующие службы, связанные с обеспечением информационной безопасности, руководство которыми осуществляет Президент: Федеральная служба по техническому и экспортному контролю, Федеральная служба безопасности, Федеральная служба охраны, Служба внешней разведки. В соответствии с данным Указом Президент руководит также деятельностью Министерств внутренних дел, обороны, иностранных дел, юстиции, а также Министерством по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий.

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

Указом Президента Российской Федерации от 8 ноября 1995 года № 1108, (ред. от 06.10.2004) создана Межведомственная комиссия по защите государственной тайны, которая является основным органом, координирующим действия государственных структур по вопросам защиты информации. Указом Президента от 6 октября 2004 года № 1286, (ред. от 03.08.2018) «Вопросы Межведомственной комиссии по защите государственной тайны» заново определены основные направления работы комиссии. Постановлением Правительства от 3 декабря 2004 года № 728, (ред. от 25.08.2008) «О персональном составе Межведомственной комиссии по защите государственной тайны» определен персональный состав комиссии.

Постановлением Правительства Российской Федерации от 13 апреля 2006 года № 213, (ред. от 28.03.2008) «О правительственной комиссии по федеральной связи» создана специальная комиссия по федеральной связи и утверждено Положение о комиссии. К основным функциям Комиссии относится определение приоритетов в реализации основных направлений развития федеральной связи с учетом задач государственного управления, обороны и безопасности государства, обеспечения правопорядка, координация деятельности федеральных органов

исполнительной власти по развитию российской инфраструктуры связи, обеспечению ее интеграции с международными сетями связи, развитию технологий и средств защиты информации.

1.2. Структура нормативных правовых актов в области информационной безопасности

Информационные технологии, являясь основой информационного общества, не могут развиваться в отрыве от других аспектов жизнедеятельности данного общества. Обретая новые возможности благодаря использованию принципиально новых средств и методов обработки информации, общество получает и новые проблемы правового, этического и технологического характера. Стремительное развитие глобального информационного общества требует существенной корректировки его нормативной правовой базы.

Правовое обеспечение информационной безопасности заключается в исполнении существующих или введении новых законов, постановлений и других документов, регулирующих юридическую ответственность должностных лиц, технических специалистов и пользователей за действия (или бездействие), повлекшие утечку, утрату или модификацию защищаемой информации, а также злоумышленников за совершение преднамеренного несанкционированного доступа к информации и нарушение процессов ее обработки.

Специфика современного этапа развития общества заключается в том, что дальнейшее развитие процессов информатизации зависит не только от технологических прорывов, но во многом от того, насколько быстро будут корректироваться существующие нормативные акты и разрабатываться новые, соответствующие изменившимся реалиям жизни. Учитывая глобальный характер процессов информатизации, международное сообщество должно предпринимать согласованные действия по созданию безопасного и свободного от киберпреступности пространства. На сегодняшний день мировое сообщество сформировало единое мнение о том, что эффективное обеспечение информационной безопасности не может быть достигнуто без согласованных

действий по правовому регулированию процессов информатизации и выработки соответствующих международных нормативных документов.

В настоящее время разработаны и продолжают разрабатываться международные, государственные и ведомственные нормативные акты, структуру которых можно представить в виде схемы, представленной на рис. 1.2.



Рис. 1.2. Структура нормативно-правовых актов в области ИБ

Они регламентируют основные понятия и концепции информационной безопасности на межгосударственном и государственном уровне, что позволяет ввести единые стандарты и критерии в области защиты информации.

В соответствии со статьей 15 Конституции Российской Федерации «Общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы. Если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора». В соответствии с этим международные документы, подписанные от имени Российской Федерации, имеют приоритет над соответствующими документами федерального уровня.

Современная база международных актов в области информационной безопасности включает в себя декларации, конвенции, соглашения, рекомендации, а также стандарты. Основными целями использования международных документов являются:

1. Приведение отечественных нормативных документов в области защиты информации в соответствие с международными.
2. Выработка государственной политики в области информатизации в соответствии с мировыми тенденциями развития глобального информационного общества.
3. Предоставление отечественным разработчикам информационных технологий средств и методов создания аппаратно-программных средств и технологий, соответствующих международным стандартам и делающих их конкурентоспособными на международном рынке товаров и услуг.
4. Предоставление соответствующим специалистам правил и критериев оценки защищенности информационных технологий для различных сфер применений.
5. Подготовка кадров специалистов в области информатизации и информационной безопасности, соответствующих современным потребностям глобального информационного общества.

Следует отметить, что Российская Федерация присоединилась к ряду международных конвенций и деклараций, является участницей международных конференций по проблемам информационной безопасности. Международное сотрудничество Российской Федерации в области информационной безопасности является неотъемлемой частью ее взаимодействия со странами мирового сообщества наряду со сферой экономики, политики, культуры. Основными направлениями международного сотрудничества в области информационной безопасности являются:

1. Координация деятельности государств по борьбе с киберпреступлениями.

2. Обеспечение безопасности международного информационного обмена, разработка единых нормативно-технических документов.

3. Координация деятельности государств по борьбе с киберпреступлениями.

4. Обеспечение безопасности международного информационного обмена, разработка единых нормативно-технических документов.

5. Предотвращение использования глобальных телекоммуникаций в качестве инструмента для применения «информационного оружия» недопущение развязывания «информационных войн».

6. Обеспечение защиты конфиденциальной информации в международных информационных системах от несанкционированного доступа со стороны преступных группировок и террористических организаций.

Из всех международных нормативных актов в Российской Федерации в настоящее время используются в основном организационно-технические документы, часть из которых принята в качестве национальных стандартов в области защиты информации (например, ГОСТ Р ИСО/МЭК 15408).

Если касаться национальной нормативной правовой базы, то в целом в области защиты информации в Российской Федерации действуют несколько десятков документов на уровне федеральных законов, указов президента, постановлений правительства и других правовых актов. Базовые концептуальные принципы отношений в информационной сфере определяет Конституция

Российской Федерации. В соответствии с действующим порядком разработка правовых актов, регулирующих отношения в области защиты информации, осуществляется в рамках государственной системы защиты информации. Основные функции системы:

1. Разработка концепций и единой технической политики в области обеспечения информационной безопасности.
2. Совершенствование и защита отечественной информационной инфраструктуры, интеграция России в международное информационное пространство.
3. Координация деятельности федеральных органов государственной власти, а также других государственных структур, обеспечивающих решение задач информационной безопасности.
4. Координация разработки нормативно-правовых, нормативно-технических и организационно-распорядительных документов в области защиты информации.
5. Лицензирование деятельности в сфере информационной безопасности и сертификации средств защиты.
6. Обеспечение конституционных прав и свобод граждан на получение общедоступной информации и обеспечение защиты информации ограниченного доступа (государственная тайна, конфиденциального характера).
7. Организация системы подготовки кадров, фундаментальных и прикладных научных исследований в области информационной безопасности.
8. Осуществление международного сотрудничества в области информационной безопасности, представление интересов Российской Федерации в международных организациях.
9. Предупреждение и пресечение правонарушений в информационной сфере, осуществление судопроизводства по делам о преступлениях.

Все нормативные документы, действующие в настоящее время в Российской Федерации можно разделить по типу на две группы:

1. Документы, составляющие нормативную правовую базу и определяющие правовое пространство в области информатизации и защиты

информации (федеральные законы, кодексы, указы Президента, постановления Правительства).

2. Документы, составляющие нормативно-техническую базу в области информационных технологий и защиты информации (стандарты, критерии и другие документы, непосредственно определяющие организационные и технические требования по защите информации, порядок их выполнения и контроля эффективности принимаемых мер защиты).

По назначению все документы федерального уровня можно разделить на следующие группы.

1. Документы, составляющие концептуальную основу защиты информации.

2. Пакет федеральных законов и кодексов, определяющих систему защиты информации.

3. Пакет нормативных правовых актов в виде указов Президента, постановлений Правительства Российской Федерации, межведомственных и ведомственных (отраслевых) руководящих документов и стандартов, регулирующих механизмы исполнения требований к системе обеспечения информационной безопасности государства.

Среди документов федерального уровня следует особо отметить документы, регламентирующие порядок лицензирования деятельности по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием и сертификацией средств защиты информации.

Ведомственные нормативные документы разрабатываются в целях развития и конкретизации положений федеральных документов по защите информации, с учетом ведомственной (отраслевой) специфики.

Органы законодательной и исполнительной власти субъектов Российской власти, а также органы местного самоуправления в пределах своей компетенции также могут разрабатывать нормативные правовые акты в области информационной безопасности. Указанные акты не должны противоречить соответствующим актам федерального и международного уровней.

Согласно требованиям нормативно-правовых документов на предприятиях и в учреждениях должен также действовать комплекс мер по обеспечению защиты информации. Этот комплекс должен основываться на нормативно-правовых и нормативно-технических документах в области защиты информации федерального и отраслевого уровней.

Нормативные документы уровня предприятия, учреждения или организации разрабатываются в дополнение и в целях конкретизации нормативных правовых актов, нормативной и методической документации технического характера отраслевого уровня. В состав документов уровня предприятия входит также проектная и эксплуатационная документация по создаваемым и эксплуатируемым объектам информатизации, инструкции и регламенты по эксплуатации информационных систем и средств защиты, а также организационно-распорядительная документация предприятия (приказы, распоряжения, должностные инструкции сотрудников и др.).

В связи с возрастанием важности задач обеспечения информационной безопасности многие предприятия разрабатывают и утверждают в виде специального документа концепцию информационной безопасности. На основании концепции затем разрабатывается политика безопасности, которая конкретизирует положения концепции применительно к конкретным функциональным подсистемам единой информационной системы предприятия.

2. ГОСУДАРСТВЕННЫЕ ОРГАНЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

2.1. Совет Безопасности Российской Федерации

Совет Безопасности обеспечивает условия для реализации Президентом его конституционных полномочий по защите прав и свобод человека и гражданина, охране суверенитета Российской Федерации, ее независимости и государственной целостности. Совет Безопасности Российской Федерации образован в 1992 году. Создание при Президенте РФ специального конституционного совещательного органа – Совета Безопасности, обусловлено

необходимостью постоянного анализа и стратегического планирования по всему комплексу вопросов безопасности, подготовки проектов решений Президента в соответствующих сферах.

Совет Безопасности формируется Президентом Российской Федерации, являющимся его председателем, в соответствии с Конституцией и Федеральным Законом «О безопасности». В состав Совета Безопасности входят:

- Председатель Совета Безопасности Российской Федерации, которым по должности является Президент Российской Федерации;
- Секретарь Совета Безопасности Российской Федерации;
- постоянные члены Совета Безопасности и члены Совета Безопасности, включаемые в состав Совета Безопасности и исключаемые из него Президентом Российской Федерации по представлению Секретаря Совета Безопасности.

Секретарь Совета Безопасности входит в число постоянных членов Совета Безопасности и руководит его Аппаратом. Он несет ответственность за обеспечение деятельности Совета Безопасности и исполнение принятых им решений, осуществляет подготовку и организацию заседаний и оперативных совещаний Совета. Секретарь Совета Безопасности назначается на должность и освобождается от должности Президентом Российской Федерации.

Аппарат Совета Безопасности является самостоятельным подразделением Администрации Президента и имеет статус управления.

В соответствии с основными задачами и направлениями деятельности Совет Безопасности образует межведомственные комиссии – основные рабочие органы Совета. В зависимости от возлагаемых на них задач они могут создаваться по функциональному или региональному признаку, на постоянной или временной основе. Межведомственные комиссии Совета Безопасности осуществляют подготовку предложений и рекомендаций Совету Безопасности по основным направлениям внутренней и внешней политики в области обеспечения национальной безопасности, способствуют координации деятельности федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по реализации федеральных программ в

области обеспечения национальной безопасности и исполнению решений Совета Безопасности.

Положение о Совете Безопасности утверждается Президентом Российской Федерации. С момента создания Совета Положение изменялось несколько раз. Последние редакции Положения о Совете Безопасности и его Аппарате утверждены Указом Президента от 7 июня 2004 года № 726, (ред. от 06.05.2011). Сайт Совета Безопасности <http://www.scrf.gov.ru>.

2.2. Комиссия Совета Федерации по информационной политике

Комиссия Совета Федерации по информационной политике создана Постановлением Совета Федерации Федерального Собрания Российской Федерации от 30 января 2002 года № 106, (с изм. от 16.02.2011). Создание Комиссии было обусловлено необходимостью детального изучения и мониторинга информационной ситуации, а также требованиями дальнейшего совершенствования законодательной базы в интересах большей ее ориентации на формирование единого информационного пространства, решения других вопросов информационной политики Российской Федерации.

К предмету ведения Комиссии отнесены следующие вопросы правового обеспечения:

- государственная политика в сфере средств массовой информации, информационных технологий и информатизации;
- развитие единого информационного пространства Российской Федерации;
- издательская и полиграфическая деятельность;
- информационный обмен, развитие компьютерных сетей общего пользования;
- распространение периодических изданий, книжной и иной печатной, аудио- и видеопродукции;
- межгосударственное сотрудничество в информационной сфере;
- содействие информационному обеспечению деятельности Совета Федерации;

- выполнение федеральных и региональных целевых программ по вопросам ведения Комиссии.

Задачи членов Комиссии состоят в изучении и обобщении положения дел в каждом отдельно взятом сегменте инфокоммуникационного сектора экономики, анализе и оценке правоприменительной практики в сфере информации.

Работа ведется совместно с представителями Министерства культуры и массовых коммуникаций Российской Федерации, Федерального агентства по печати и массовым коммуникациям Российской Федерации, Министерства по информационным технологиям и связи Российской Федерации, Министерства экономического развития и торговли Российской Федерации, Медиасоюза и журналистским сообществом.

2.3. Федеральные органы исполнительной власти в области информатизации

Новая система и структура федеральных органов исполнительной власти утверждена Указом Президента Российской Федерации от 9 марта 2004 года № 314 (ред. от 28.09.2017) «О системе и структуре федеральных органов исполнительной власти», а затем Указом от 20 мая 2004 года № 649 «Вопросы структуры федеральных органов исполнительной власти» с последующими изменениями Указами: (ред. от 25.08.2010, с изм. от 30.04.2016) (ред. от 25.08.2010, с изм. от 30.04.2016)

В соответствии с вышеназванными Указами выделен ряд Федеральных министерств, служб и агентств, функционально связанных с обеспечением информационной безопасности, руководство деятельностью которых осуществляет Президент Российской Федерации:

- Федеральная служба по техническому и экспортному контролю (ФСТЭК, в составе Министерства обороны);
- Служба внешней разведки Российской Федерации (СВР);
- Федеральная служба безопасности Российской Федерации (ФСБ);
- Федеральная служба охраны Российской Федерации (ФСО).

Федеральные министерства, службы и агентства, руководство которыми осуществляет Правительство Российской Федерации:

- Федеральная служба по интеллектуальной собственности, патентам и товарным знакам (в составе Министерства образования и науки);
- Федеральное агентство по техническому регулированию и метрологии (в составе Министерства промышленности и энергетики Российской Федерации);
- Министерство информационных технологий и связи Российской Федерации, включающее в себя федеральное агентство по информационным технологиям (Указом Президента РФ от 12 мая 2008 года № 724 преобразовано в Министерство связи и массовых коммуникаций);
- Федеральная служба по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия (Указом Президента РФ от 12 мая 2008 года № 724 служба вновь преобразована в федеральную службу по надзору в сфере связи и массовых коммуникаций и входит в состав Министерства связи и массовых коммуникаций).

Кроме того, на уровне федеральных органов исполнительной власти создан ряд комиссий, в том числе: Межведомственная Комиссия по защите государственной тайны, Правительственная Комиссия по федеральной связи, Правительственная Комиссия по противодействию нарушениям в сфере интеллектуальной собственности, ее правовой охране и использованию.

Указом Президента Российской Федерации от 11 марта 2003 года № 308 упразднено Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) и его функции перераспределены между ФСБ, СВР и ФСО. В составе ФСО образована служба специальной связи и информации.

2.4. Межведомственная Комиссия по защите государственной тайны

Межведомственная комиссия по защите государственной тайны, созданная Указом Президента Российской Федерации от 8 ноября 1995 года № 1108, (ред. от 06.10.2004) является основным органом, координирующим действия государственных структур по вопросам защиты информации. Она действует в

рамках государственной системы защиты информации от утечки по техническим каналам, положение о которой введено в действие Постановлением Правительства от 15 сентября 1993 года № 912-51. В этом Постановлении были определены структура, задачи и функции, а также организация работ по защите информации, содержащей сведения, составляющие государственную тайну.

Функции Межведомственной комиссии по защите государственной тайны в соответствии с Указом Президента Российской Федерации от 30 марта 1994 г. N 614 возложены на государственную техническую комиссию, которая впоследствии переименована в Федеральную службу по техническому и экспортному контролю.

В связи с реорганизацией федеральных органов исполнительной власти функции Комиссии были уточнены Указом Президента Российской Федерации от 6 октября 2004 года № 1286 «Вопросы Межведомственной комиссии по защите государственной тайны». Постановлением Правительства Российской Федерации от 3 декабря 2004 года № 728 утвержден персональный состав Комиссии. В нее вошли представители Министерств обороны, иностранных дел, внутренних дел, образования и науки, финансов, экономического развития и торговли, Аппарата Президента, Совета Безопасности, ФСБ, ФСО, СВР, ФСТЭК.

2.5. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации создано 15 мая 2018 года указом Президента Российской Федерации № 215 на базе Министерства связи и массовых коммуникаций Российской Федерации.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации – федеральный орган исполнительной власти. Вышестоящий орган государственной власти – Правительство Российской Федерации.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации – федеральный орган исполнительной власти, который

занимается выработкой и реализацией государственной политики и нормативно-правовым регулированием в следующих сферах:

- сфере информационных технологий (включая использование информационных технологий при формировании государственных информационных ресурсов и обеспечение доступа к ним),
- сфере электросвязи (включая использование и конверсию радиочастотного спектра) и почтовой связи,
- сфере массовых коммуникаций и СМИ, в том числе электронных (включая развитие сети Интернет, систем телевизионного (в том числе цифрового) вещания и радиовещания и новых технологий в этих областях):
 - сфере печати, издательской и полиграфической деятельности,
 - сфере обработки персональных данных.

Министерство выступает в качестве почтовой администрации Российской Федерации и выполняет функции администрации связи Российской Федерации при осуществлении международной деятельности в области связи.

Министерство осуществляет координацию и контроль деятельности находящихся в его ведении Федеральной службы по надзору в сфере связи и массовых коммуникаций, Федерального агентства связи, Федерального агентства по печати и массовым коммуникациям.

2.6. Федеральная служба безопасности Российской Федерации

Федеральный орган исполнительной власти Российской Федерации, спецслужба, осуществляющая в пределах своих полномочий решение задач по обеспечению безопасности Российской Федерации.

Наделена правом ведения предварительного следствия и дознания, оперативно-розыскной и разведывательной деятельности. В ФСБ России предусмотрена военная, правоохранительная и федеральная гражданская государственная служба. Относится к государственным военизированным организациям, которые имеют право приобретать боевое, ручное, стрелковое и иное оружие.

Руководство деятельностью ФСБ России осуществляется Президентом Российской Федерации.

3 апреля 1995 года Президент Российской Федерации Борис Ельцин подписал Федеральный закон «Об органах федеральной службы безопасности в Российской Федерации», вступивший в силу 10 апреля 1995 года со дня его официального опубликования в Собрании законодательства Российской Федерации^[3]. В соответствии с ним, Федеральная служба контрразведки Российской Федерации была переименована в Федеральную службу безопасности Российской Федерации, при этом не проводилось организационно-штатных мероприятий, сотрудники службы (включая директора и его заместителей) оставались на своих должностях без переназначений и переаттестаций. 23 июня 1995 года соответствующие изменения «задним числом» были внесены в структуру федеральных органов исполнительной власти. Этим же указом были утверждены положение о службе и структуре её центрального аппарата, повторявшей структуру ФСК России за некоторыми исключениями (воссоздано следственное управление, появилось управление специальных операций, а секретариат преобразован в управление делами).

В соответствии со статьёй 8 Федерального закона от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности», деятельность органов ФСБ России осуществляется по следующим основным направлениям:

- контрразведывательная деятельность;
- борьба с терроризмом;
- борьба с особо опасными формами преступности;
- разведывательная деятельность;
- пограничная деятельность;
- обеспечение информационной безопасности.

Иные направления деятельности органов ФСБ России определяются федеральным законодательством:

- борьба с коррупцией.

Права и обязанности Федеральной службы безопасности Российской Федерации установлены статьями 12 и 13 федерального закона «О федеральной службе безопасности» № 40-ФЗ.

Обеспечение информационной безопасности – деятельность органов ФСБ России, осуществляемая ими в пределах своих полномочий:

- при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств;
- при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в России и её учреждениях, находящихся за пределами России.
- лицензирование и сертификация отдельных видов деятельности, предусматривающих допуск к государственной тайне Российской Федерации.

Сайт ФСБ: <http://www.fsb.ru>.

2.7. Федеральная служба по техническому и экспортному контролю

Федеральный орган исполнительной власти России, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности. ФСТЭК России – общегосударственный орган исполнительной власти специальной компетенции, предусмотренный подзаконным актом и действующий неопределённый срок; созданное Российской Федерацией государственное учреждение; политическая, некоммерческая, формальная организация; часть государственного аппарата; юридическое лицо.

Постановлением ЦК КПСС и Совета Министров СССР от 18 декабря 1973 г. № 903-303 «О противодействии иностранной технической разведке» создана Государственная комиссия СССР по противодействию иностранным техническим разведкам (Гостехкомисия СССР, ГТК СССР).

Указом Президента СССР от 22 мая 1991 г. № УП-2003 «Об образовании Государственной технической комиссии СССР по противодействию иностранным техническим разведкам» Гостехкомисия СССР подчинена Президенту СССР.

Указом Президента Российской Федерации от 5 января 1992 г. № 9 «О создании Государственной технической комиссии при Президенте Российской Федерации» создана Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России).

В соответствии с Указом Президента Российской Федерации от 9 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти» вместо существовавшей Государственной технической комиссии при Президенте Российской Федерации был создан (преобразован) федеральный орган исполнительной власти Федеральная служба по техническому и экспортному контролю Российской Федерации.

Указом Президента Российской Федерации от 20 мая 2004 г. № 649 "Вопросы структуры федеральных органов исполнительной власти" ФСТЭК России "переименовывается" из Федеральной службы по техническому и экспортному контролю Российской Федерации в Федеральную службу по техническому и экспортному контролю.

Положение о Федеральной службе по техническому и экспортному контролю (ФСТЭК России) утверждено Указом Президента РФ от 16 августа 2004 г. № 1085 "Вопросы федеральной службы по техническому и экспортному контролю".

Указом Президента Российской Федерации от 20 мая 2004 г. № 649 "Вопросы структуры федеральных органов исполнительной власти" образована Федеральная служба по техническому и экспортному контролю.

ФСТЭК России является федеральным органом исполнительной власти России, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

– обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной

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

- противодействия иностранным техническим разведкам на территории Российской Федерации;

- обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения её утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях её добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;

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

- осуществления экспортного контроля.

- ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля.

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

- ФСТЭК России организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации и руководит ею.

- ФСТЭК России осуществляет свою деятельность непосредственно и (или) через свои территориальные органы. ФСТЭК России и её территориальные органы входят в состав государственных органов обеспечения безопасности. Деятельность ФСТЭК России обеспечивают Государственный научно-

исследовательский испытательный институт проблем технической защиты информации ФСТЭК России (головная научная организация по проблемам защиты информации), а также другие подведомственные ФСТЭК России организации. ФСТЭК России осуществляет свою деятельность во взаимодействии с другими федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления и организациями.

Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации. ФСТЭК России подведомственна Минобороны России.

Основные полномочия ФСТЭК России:

- разрабатывает стратегию и определяет приоритетные направления деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации;
- разрабатывает и вносит в установленном порядке Президенту РФ и в Правительство РФ проекты законодательных и иных нормативных правовых актов по вопросам своей деятельности;
- издаёт нормативные правовые акты по вопросам своей деятельности;
 - разрабатывает и утверждает в пределах своей компетенции методические документы, организует их издание за счёт средств, выделяемых из федерального бюджета ФСТЭК России на эти цели;
 - организует и финансирует работы по изучению излучений различной физической природы, возникающих при использовании неинформационных излучающих комплексов, систем и устройств;
 - осуществляет межотраслевую координацию деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, в федеральных органах исполнительной власти, органах исполнительной власти

субъектов Российской Федерации, органах местного самоуправления и организациях;

- осуществляет в пределах своей компетенции контроль за состоянием работ по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации;

- осуществляет в пределах своей компетенции межведомственный контроль за обеспечением защиты государственной тайны, контроль за соблюдением лицензионных требований и условий, а также рассмотрение дел об административных правонарушениях;

- вносит в установленном порядке представления о применении мер ответственности за нарушения законодательства Российской Федерации по вопросам своей деятельности;

- выдаёт предписания на приостановление работ на объектах федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления и организаций в случае выявления в ходе осуществления контроля нарушений норм и требований, касающихся противодействия техническим разведкам и технической защиты информации;

- организует радиоконтроль за соблюдением установленного порядка передачи служебной информации должностными лицами организаций, выполняющих работы, связанные со сведениями, составляющими государственную и (или) служебную тайну, при использовании открытых каналов радио-, радиорелейных, тропосферных, спутниковых и других линий и сетей радиосвязи, доступных для радиоразведки, подготавливает предложения, направленные на предотвращение утечки информации по указанным каналам;

- организует и проводит лицензирование деятельности по осуществлению мероприятий и (или) оказанию услуг в области защиты государственной тайны (в части, касающейся противодействия техническим разведкам и (или) технической защиты информации), по созданию средств защиты информации, содержащей сведения, составляющие государственную тайну, по технической защите

конфиденциальной информации, по разработке и (или) производству средств защиты конфиденциальной информации, а также лицензирование иных видов деятельности в соответствии с законодательством Российской Федерации;

- организует в соответствии с законодательством Российской Федерации проведение работ по оценке соответствия (включая работы по сертификации) средств противодействия техническим разведкам, технической защиты информации, обеспечения безопасности информационных технологий, применяемых для формирования государственных информационных ресурсов, а также объектов информатизации и ключевых систем информационной инфраструктуры;

- участвует совместно с ФСБ России в проведении специальных экспертиз по допуску организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, а также принимает участие в проведении государственной аттестации руководителей организаций, ответственных за защиту указанных сведений;

- организует разработку программ стандартизации, технических регламентов и национальных стандартов в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, обеспечения безопасности применяемых информационных технологий, а также в области противодействия техническим разведкам и технической защиты информации;

- осуществляет выдачу заключений о возможностях размещения и использования на сухопутной территории Российской Федерации иностранных технических средств наблюдения и контроля, поставляемых иностранной стороной в ходе реализации международных научных и научно-технических программ и проектов, организует и осуществляет контроль за соблюдением организациями-заявителями установленных дополнительных условий и требований, организует проведение необходимых экспертиз;

- обеспечивает проведение экспортного контроля в соответствии с законодательством Российской Федерации и приказами Министра обороны Российской Федерации;

- разрабатывает с участием заинтересованных федеральных органов исполнительной власти и организаций для представления в установленном порядке проекты списков (перечней) товаров (работ, услуг), информации, результатов интеллектуальной деятельности, подлежащих экспортному контролю;
- организует и проводит в установленном порядке государственную экспертизу внешнеэкономических сделок в отношении товаров (работ, услуг), информации, результатов интеллектуальной деятельности, которые могут быть использованы при создании оружия массового поражения, средств его доставки, иных видов вооружения и военной техники;
- участвует в реализации государственной политики в области нераспространения оружия массового поражения и иных наиболее опасных видов оружия, а также в области контроля за экспортом товаров (работ, услуг), информации, результатов интеллектуальной деятельности, которые могут быть использованы при создании оружия массового поражения, средств его доставки, иных видов вооружения и военной техники;
- организует в соответствии с законодательством Российской Федерации государственную аккредитацию организаций, создавших внутрифирменные программы экспортного контроля, и выдает им свидетельства о государственной аккредитации;
- участвует в пределах своей компетенции в подготовке предложений о введении ограничений и (или) запретов на экспорт и (или) импорт товаров (работ, услуг), информации, результатов интеллектуальной деятельности, исходя из национальных интересов и международных обязательств Российской Федерации;
- осуществляет в пределах своей компетенции нетарифное регулирование внешнеторговой деятельности, в том числе выдает лицензии на осуществление операций по экспорту и (или) импорту товаров (работ, услуг), информации, результатов интеллектуальной деятельности в случаях, предусмотренных законодательством Российской Федерации;
- определяет порядок и форму учёта внешнеэкономических сделок в целях осуществления экспортного контроля;

- осуществляет иные функции в установленной сфере деятельности в соответствии с федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации.

ФСТЭК России:

- разрабатывает стратегию и определяет приоритетные направления деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации;

- разрабатывает и вносит в установленном порядке Президенту РФ и в Правительство РФ проекты законодательных и иных нормативных правовых актов по вопросам своей деятельности;

- издаёт нормативные правовые акты по вопросам своей деятельности;

- разрабатывает и утверждает в пределах своей компетенции методические документы, организует их издание за счёт средств, выделяемых из федерального бюджета ФСТЭК России на эти цели;

- организует и финансирует работы по изучению излучений различной физической природы, возникающих при использовании неинформационных излучающих комплексов, систем и устройств;

- осуществляет межотраслевую координацию деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления и организациях;

- осуществляет в пределах своей компетенции контроль за состоянием работ по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации;

- осуществляет в пределах своей компетенции межведомственный контроль за обеспечением защиты государственной тайны, контроль за соблюдением лицензионных требований и условий, а также рассмотрение дел об административных правонарушениях;

- вносит в установленном порядке представления о применении мер ответственности за нарушения законодательства Российской Федерации по вопросам своей деятельности;

- выдаёт предписания на приостановление работ на объектах федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления и организаций в случае выявления в ходе осуществления контроля нарушений норм и требований, касающихся противодействия техническим разведкам и технической защиты информации;

- организует радиоконтроль за соблюдением установленного порядка передачи служебной информации должностными лицами организаций, выполняющих работы, связанные со сведениями, составляющими государственную и (или) служебную тайну, при использовании открытых каналов радио-, радиорелейных, тропосферных, спутниковых и других линий и сетей радиосвязи, доступных для радиоразведки, подготавливает предложения, направленные на предотвращение утечки информации по указанным каналам;

- организует и проводит лицензирование деятельности по осуществлению мероприятий и (или) оказанию услуг в области защиты государственной тайны (в части, касающейся противодействия техническим разведкам и (или) технической защиты информации), по созданию средств защиты информации, содержащей сведения, составляющие государственную тайну, по технической защите конфиденциальной информации, по разработке и (или) производству средств защиты конфиденциальной информации, а также лицензирование иных видов деятельности в соответствии с законодательством Российской Федерации;

- организует в соответствии с законодательством Российской Федерации проведение работ по оценке соответствия (включая работы по сертификации) средств противодействия техническим разведкам, технической защиты

информации, обеспечения безопасности информационных технологий, применяемых для формирования государственных информационных ресурсов, а также объектов информатизации и ключевых систем информационной инфраструктуры;

- участвует совместно с ФСБ России в проведении специальных экспертиз по допуску организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, а также принимает участие в проведении государственной аттестации руководителей организаций, ответственных за защиту указанных сведений;

- организует разработку программ стандартизации, технических регламентов и национальных стандартов в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, обеспечения безопасности применяемых информационных технологий, а также в области противодействия техническим разведкам и технической защиты информации;

- осуществляет выдачу заключений о возможностях размещения и использования на сухопутной территории Российской Федерации иностранных технических средств наблюдения и контроля, поставляемых иностранной стороной в ходе реализации международных научных и научно-технических программ и проектов, организует и осуществляет контроль за соблюдением организациями-заявителями установленных дополнительных условий и требований, организует проведение необходимых экспертиз;

- обеспечивает проведение экспортного контроля в соответствии с законодательством Российской Федерации и приказами Министра обороны Российской Федерации;

- разрабатывает с участием заинтересованных федеральных органов исполнительной власти и организаций для представления в установленном порядке проекты списков (перечней) товаров (работ, услуг), информации, результатов интеллектуальной деятельности, подлежащих экспортному контролю;

- организует и проводит в установленном порядке государственную экспертизу внешнеэкономических сделок в отношении товаров (работ, услуг),

информации, результатов интеллектуальной деятельности, которые могут быть использованы при создании оружия массового поражения, средств его доставки, иных видов вооружения и военной техники;

- участвует в реализации государственной политики в области нераспространения оружия массового поражения и иных наиболее опасных видов оружия, а также в области контроля над экспортом товаров (работ, услуг), информации, результатов интеллектуальной деятельности, которые могут быть использованы при создании оружия массового поражения, средств его доставки, иных видов вооружения и военной техники;

- организует в соответствии с законодательством Российской Федерации государственную аккредитацию организаций, создавших внутрифирменные программы экспортного контроля, и выдает им свидетельства о государственной аккредитации;

- участвует в пределах своей компетенции в подготовке предложений о введении ограничений и (или) запретов на экспорт и (или) импорт товаров (работ, услуг), информации, результатов интеллектуальной деятельности, исходя из национальных интересов и международных обязательств Российской Федерации;

- осуществляет в пределах своей компетенции нетарифное регулирование внешнеторговой деятельности, в том числе выдает лицензии на осуществление операций по экспорту и (или) импорту товаров (работ, услуг), информации, результатов интеллектуальной деятельности в случаях, предусмотренных законодательством Российской Федерации;

- определяет порядок и форму учёта внешнеэкономических сделок в целях осуществления экспортного контроля;

- осуществляет иные функции в установленной сфере деятельности в соответствии с федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации.

Сайт ФСТЭК: <http://www.fstec.ru>.

2.8. Федеральная служба охраны Российской Федерации

Государственная охрана – функция федеральных органов государственной власти в сфере обеспечения безопасности объектов государственной охраны, осуществляемая на основе совокупности правовых, организационных, охранных, режимных, оперативно-розыскных, технических и иных мер.

Государственная охрана осуществляется на основе Конституции Российской Федерации, федеральных конституционных законов, федеральных законов и иных нормативных правовых актов Российской Федерации, а также международных договоров Российской Федерации.

Основными принципами осуществления государственной охраны являются принципы законности, уважения и соблюдения прав и свобод человека и гражданина, централизованного руководства, взаимодействия государственных органов обеспечения безопасности, непрерывности, сочетания гласных и негласных методов деятельности, подконтрольности и поднадзорности.

Федеральная служба охраны Российской Федерации (ФСО России) является федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики, нормативно-правовому регулированию, контролю и надзору в сфере государственной охраны, президентской, правительственной и иных видов специальной связи и информации, предоставляемых федеральным органам государственной власти, органам государственной власти субъектов Российской Федерации и другим государственным органам.

ФСО России осуществляет свою деятельность непосредственно и через территориальные органы.

Руководство деятельностью ФСО России осуществляет Президент Российской Федерации.

Положение о ФСО России и структура федеральных органов государственной охраны утверждаются Президентом Российской Федерации. Правительство Российской Федерации координирует деятельность ФСО России в части, касающейся взаимодействия ФСО России с федеральными органами исполнительной власти.

Основными задачами ФСО России являются:

1) обеспечение безопасности объектов государственной охраны в местах их постоянного и временного пребывания и на трассах проезда (к объектам государственной охраны относятся Президент Российской Федерации, лица, замещающие государственные должности Российской Федерации, федеральные государственные служащие, подлежащие государственной охране в соответствии с федеральным законом от 27 мая 1996 г. № 57-ФЗ «О государственной охране», а также главы иностранных государств и правительств и иные лица иностранных государств во время пребывания на территории Российской Федерации);

2) прогнозирование и выявление угрозы жизненно важным интересам объектов государственной охраны, осуществление комплекса мер по предотвращению этой угрозы;

3) предупреждение, выявление и пресечение противоправных посягательств на объекты государственной охраны и охраняемые объекты - здания, строения и сооружения, в которых размещены федеральные органы государственной власти, прилегающие к указанным зданиям, строениям и сооружениям территории и акватории, подлежащие защите в целях обеспечения безопасности объектов государственной охраны, а также здания, строения и сооружения, прилегающие к ним территории и акватории, находящиеся в оперативном управлении федеральных органов государственной охраны;

4) предупреждение, выявление и пресечение преступлений и иных правонарушений на охраняемых объектах, в местах постоянного и временного пребывания объектов государственной охраны и на трассах их проезда;

5) защита охраняемых объектов;

6) участие в пределах своих полномочий в борьбе с терроризмом;

7) организация и обеспечение эксплуатации, безопасности, совершенствования специальной связи и информации, предоставляемых государственным органам;

8) участие в разработке и реализации мер по обеспечению информационной безопасности Российской Федерации, противодействию

техническим разведкам и защите сведений, составляющих государственную тайну;

9) осуществление государственной политики в области правовой информатизации Российской Федерации и координация работ, производимых в этой сфере;

10) информационно-технологическое и информационно-аналитическое обеспечение государственных органов, техническое обслуживание и программное сопровождение информационно-телекоммуникационных систем и ситуационных центров, а также информационное обеспечение управления государством в военное время и при чрезвычайных ситуациях;

11) обеспечение собственной безопасности. Сайт ФСО:
<http://www.fso.gov.ru>.

2.9. Служба внешней разведки Российской Федерации

Служба внешней разведки Российской Федерации (СВР России) является составной частью сил обеспечения безопасности и призвана защищать безопасность личности, общества и государства от внешних угроз.

Для достижения этих целей Службе внешней разведки предоставляется ряд полномочий, определенных федеральным законом Российской Федерации «О внешней разведке» от 10 января 1996 года № 5-ФЗ (в ред. Федеральных законов от 07.11.2000 № 135-ФЗ, от 30.06.2003 № 86-ФЗ, от 22.08.2004 № 122-ФЗ, от 14.02.2007 № 20-ФЗ).

Общее руководство органами внешней разведки Российской Федерации осуществляет Президент Российской Федерации.

В соответствии с Постановлением Правительства Российской Федерации от 15 апреля 1995 года N 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» (в редакции Постановлений Правительства РФ от 23.04.1996 № 509, от 30.04.1997 № 513,

от 29.07.1998 № 854, от 03.10.2002 № 731, от 17.12.2004 № 807, от 26.01.2007 № 50) СВР уполномочена на ведение лицензионной деятельности в следующих областях:

1. Допуск предприятий к проведению работ, связанных с использованием сведений, составляющих государственную тайну (за рубежом).
2. Проведение работ, связанных с созданием средств защиты информации.
3. Осуществление мероприятий и (или) оказания услуг в области защиты государственной тайны.

На СВР, как орган, уполномоченный на ведение лицензионной деятельности, возлагается:

- организация лицензирования деятельности предприятий;
- организация и проведение специальных экспертиз предприятий;
- рассмотрение заявлений предприятий о выдаче лицензий;
- принятие решений о выдаче или об отказе в выдаче лицензий;
- выдача лицензий;
- принятие решений о приостановлении действия лицензии или о ее аннулировании;
- разработка нормативно-методических документов по вопросам лицензирования;
- привлечение в случае необходимости представителей министерств и ведомств Российской Федерации для проведения специальных экспертиз;
- ведение реестра выданных, приостановленных и аннулированных лицензий.

В соответствии с законом «О внешней разведке» для осуществления своей деятельности Служба внешней разведки Российской Федерации может при собственном 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.

Лицо, допускаемое к сведениям об органах внешней разведки Российской Федерации, проходит процедуру оформления допуска к сведениям, составляющим государственную тайну.

Сайт СВР: <http://www.svr.ru>.

2.10. Федеральное агентство по информационным технологиям

Федеральное агентство по информационным технологиям создано Указом Президента Российской Федерации от 20 мая 2004 года № 649 «Структура федеральных органов исполнительной власти». Постановлением Правительства Российской Федерации от 30 июня 2004 года № 319 «Об утверждении Положения о Федеральном агентстве по информационным технологиям» утверждено соответствующее Положение об агентстве.

Организационно агентство находится в ведении Министерства информационных технологий и связи Российской Федерации. Указом Президента Российской Федерации от 12 мая 2008 года № 724 указанное министерство преобразовано в Министерство связи и массовых коммуникаций.

Федеральное агентство по информационным технологиям является федеральным органом исполнительной власти, осуществляющим функции по управлению государственным имуществом и оказанию государственных услуг в сфере информационных технологий, в том числе в части использования информационных технологий для формирования государственных информационных ресурсов и обеспечения доступа к ним.

Федеральное агентство по информационным технологиям является уполномоченным федеральным органом исполнительной власти в области использования электронной цифровой подписи.

Агентство:

1. Организует подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей.

2. Осуществляет обязательную сертификацию информационных технологий, предназначенных для обработки государственного банка данных о детях, оставшихся без попечения родителей.

3. Организует регистрацию государственных информационных ресурсов и систем.

4. Осуществляет ведение единого государственного реестра сертификатов ключей подписей удостоверяющих центров и реестра сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, а также обеспечивает доступ к ним граждан, организаций, органов государственной власти и органов местного самоуправления.

5. Осуществляет функции государственного заказчика научно-технических и инвестиционных программ и проектов в установленной сфере деятельности.

6. Взаимодействует в установленном порядке с органами государственной власти иностранных государств и международными организациями в установленной сфере деятельности.

7. Обеспечивает защиту сведений, составляющих государственную тайну, в процессе деятельности Агентства, а также контроль и координацию деятельности находящихся в его ведении учреждений и иных организаций в указанной области.

Федеральное агентство по информационным технологиям не вправе осуществлять нормативно-правовое регулирование в установленной сфере деятельности и функции по контролю и надзору, кроме случаев, устанавливаемых указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

Агентство создает и организует работу Совета главных конструкторов информатизации регионов Российской Федерации. Данный Совет осуществляет свою деятельность в соответствии с Положением, утвержденным приказом агентства от 25 марта 2005 года № 11. Последний состав Совета утвержден приказом агентства от 21 декабря 2006 года № 83. В состав Совета входят представители органов исполнительной власти субъектов Российской Федерации,

в должностные обязанности которых входят вопросы информатизации и обеспечения информационной безопасности регионов.

Сайт агентства: <http://www.minsvyaz.ru>.

2.11. Федеральная служба по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия

Федеральная служба по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия создана Указом Президента Российской Федерации от 12 марта 2007 года № 320 «О Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия». В соответствии с Указом данная служба образована путем слияния двух служб: Федеральной службы по надзору в сфере связи (Россвязьнадзор) и Федеральной службы по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия (Росохранкультура).

Руководство Федеральной Службой осуществляет Правительство Российской Федерации.

Вышеназванным Указом определено, что «указанная Служба является уполномоченным федеральным органом исполнительной власти, осуществляющим функции по нормативно-правовому регулированию, контролю и надзору в сфере средств массовой информации и массовых коммуникаций, информационных технологий, связи и охраны культурного наследия, авторского права и смежных прав, а также организации деятельности радиочастотной службы».

Более подробно функции Службы будут определены в соответствующем Положении, разработка которого поручена Правительству Российской Федерации.

Указом Президента Российской Федерации от 12 мая 2008 года № 724 служба вновь преобразована в федеральную службу по надзору в сфере связи и массовых коммуникаций и входит в состав Министерства связи и массовых коммуникаций.

2.12. Федеральная служба по интеллектуальной собственности, патентам и товарным знакам

Федеральная служба по интеллектуальной собственности, патентам и товарным знакам создана Постановлением Правительства Российской Федерации от 7 апреля 2004 года № 178 «Вопросы Федеральной службы по интеллектуальной собственности, патентам и товарным знакам» в ведении Министерства образования и науки Российской Федерации.

Постановлением Правительства от 16 июня 2004 года N 299 утверждено Положение о службе (с изменениями в соответствии с Постановлением Правительства от 22.04.2005 № 247).

Служба является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере правовой охраны и использования объектов интеллектуальной собственности, патентов и товарных знаков и результатов интеллектуальной деятельности, вовлекаемых в экономический и гражданско-правовой оборот, соблюдения интересов Российской Федерации, российских физических и юридических лиц при распределении прав на результаты интеллектуальной деятельности, в том числе создаваемые в рамках международного научно-технического сотрудничества.

Она осуществляет свою деятельность во взаимодействии с другими федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, общественными объединениями и иными организациями.

Федеральная служба по интеллектуальной собственности, патентам и товарным знакам осуществляет следующие полномочия в установленной сфере деятельности:

- организует прием заявок на объекты интеллектуальной собственности, их регистрацию и экспертизу;
- выдает в установленном порядке патенты Российской Федерации на изобретение, полезную модель, промышленный образец, свидетельства Российской Федерации на товарный знак, знак обслуживания, на право пользования наименованием места происхождения товара, на общеизвестный в

Российской Федерации товарный знак, свидетельства об официальной регистрации программ для ЭВМ, баз данных, топологий интегральных микросхем;

- осуществляет регистрацию договоров о предоставлении права на изобретения, полезные модели, промышленные образцы, товарные знаки, знаки обслуживания, охраняемые программы для ЭВМ, базы данных, топологии интегральных микросхем, а также договоров коммерческой концессии на использование объектов интеллектуальной собственности, охраняемых в соответствии с патентным законодательством Российской Федерации;

- осуществляет в установленном порядке проверку деятельности организаций, распоряжающихся правами Российской Федерации на объекты интеллектуальной собственности и результаты интеллектуальной деятельности;

- обеспечивает в пределах своей компетенции защиту сведений, составляющих государственную тайну;

- осуществляет информационно-методическое обеспечение деятельности органов исполнительной власти, осуществляющих правоприменительные функции в сфере гражданского оборота объектов интеллектуальной собственности;

- на основании и во исполнение Конституции Российской Федерации, федеральных конституционных Законов, федеральных Законов, актов Президента Российской Федерации и Правительства Российской Федерации, нормативных правовых актов Министерства образования и науки Российской Федерации издает индивидуальные правовые акты по вопросам, отнесенным к сфере деятельности Службы.

Служба имеет право пресекать факты нарушения законодательства Российской Федерации в установленной сфере деятельности, а также применять предусмотренные законодательством Российской Федерации меры ограничительного, предупредительного и профилактического характера, направленные на недопущение и (или) ликвидацию последствий нарушений юридическими лицами и гражданами обязательных требований в установленной сфере деятельности.

Федеральная служба по интеллектуальной собственности, патентам и товарным знакам не вправе осуществлять в установленной сфере деятельности нормативно-правовое регулирование.

Сайт службы: <http://www.fips.ru>.

2.13. Федеральное агентство по техническому регулированию и метрологии

В соответствии с постановлением Правительства Российской Федерации от 2 июня 2003 года № 316 Государственный комитет Российской Федерации по стандартизации и метрологии (Госстандарт) определен органом, уполномоченным исполнять функции национального органа Российской Федерации по стандартизации, а также функции федерального органа исполнительной власти по техническому регулированию.

Указом Президента Российской Федерации от 9 марта 2004 года № 314 Государственный комитет Российской Федерации по стандартизации и метрологии преобразован в Федеральную службу по техническому регулированию и метрологии, его функции по принятию нормативных правовых актов в установленной сфере деятельности переданы Министерству промышленности и энергетики Российской Федерации.

В соответствии с Указом Президента Российской Федерации от 20 мая 2004 года № 649 служба преобразована в Федеральное агентство по техническому регулированию и метрологии, входящее в состав Министерства промышленности и энергетики. Постановлением Правительства РФ от 17 июня 2004 года № 294 "О Федеральном агентстве по техническому регулированию и метрологии" (с изменениями от 27 октября 2004 года) утверждено Положение об агентстве и отменено ранее принятое Постановление от 8 апреля 2004 года № 194 "Вопросы Федеральной службы по техническому регулированию и метрологии".

Агентство организует:

- экспертизу и подготовку заключений по проектам федеральных целевых программ, а также межотраслевых и межгосударственных научно-технических и инновационных программ;

- экспертизу проектов национальных стандартов;
- проведение в установленном порядке испытаний средств измерений в целях утверждения их типа и утверждение типа средств измерений;
- проведение в установленном порядке поверки средств измерений в Российской Федерации;
- сбор и обработку информации о случаях причинения вреда вследствие нарушения требований технических регламентов, а также информирование приобретателей, изготовителей и продавцов по вопросам соблюдения требований технических регламентов.

Агентство обеспечивает в пределах своей компетенции защиту сведений, составляющих государственную тайну. Осуществляет утверждение и учет национальных стандартов, ведение федерального информационного фонда технических регламентов и стандартов, единой информационной системы по техническому регулированию, общероссийских классификаторов технико-экономической и социальной информации.

Сайт агентства: <http://www.gost.ru>.

На сайте <http://www.technormativ.ru/> содержится информация о всех стандартах и классификаторах Российской Федерации.

Постановлением Правительства Российской Федерации от 1 марта 2005 года № 97 “О правительственной комиссии по техническому регулированию» (в ред. распоряжений Правительства РФ от 28.07.2005 № 1063-р, от 24.03.2006 № 414-р, от 28.04.2006 № 599-р, от 15.08.2006 № 1135-р, Постановления Правительства РФ от 18.01.2007 № 26, распоряжения Правительства РФ от 31.03.2007 № 386-р) создана соответствующая комиссия, утверждено Положение и персональный состав.

Комиссия является координационным органом, обеспечивающим согласованные действия заинтересованных федеральных органов исполнительной власти при решении вопросов в области технического регулирования.

Основными задачами Комиссии являются:

а) обеспечение согласованных действий федеральных органов исполнительной власти по реализации государственной политики в сфере технического регулирования;

б) рассмотрение вопросов, связанных с оценкой состояния и путей совершенствования технического регулирования;

в) координация деятельности федеральных органов исполнительной власти по обеспечению соответствия технического регулирования интересам российской экономики, уровню развития материально-технической базы и уровню научно-технического развития, а также международным нормам и правилам;

г) рассмотрение вопросов о состоянии дел в области учета случаев причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда вследствие нарушения требований технических регламентов;

д) рассмотрение и подготовка предложений по вопросам совершенствования законодательных и иных нормативных правовых актов в области технического регулирования;

е) обеспечение согласованных действий федеральных органов исполнительной власти при подготовке концепций технических регламентов, программы разработки технических регламентов и других документов по техническому регулированию;

ж) организация подготовки аналитических материалов в сфере технического регулирования;

з) рассмотрение и подготовка предложений по уточнению утвержденной Правительством Российской Федерации Программы разработки технических регламентов;

и) рассмотрение проектов технических регламентов, разногласий по ним между федеральными органами исполнительной власти и принятие соответствующих решений по снятию разногласий и внесению проектов технических регламентов в установленном порядке в Правительство Российской Федерации.

Организационно-техническое обеспечение деятельности Комиссии осуществляет Министерство промышленности и энергетики Российской Федерации. Председателем комиссии назначен министр промышленности и энергетики.

3. МЕЖДУНАРОДНЫЕ ПРОФЕССИОНАЛЬНЫЕ ОБЪЕДИНЕНИЯ

Работа крупных международных профессиональных (отраслевых) организаций (объединений), как правило, имеет следующие отличительные особенности: как правило, не направлена только на решение задач информационной безопасности – задачи информационной безопасности решаются в комплексе со множеством других проблем (развития информационных технологий, построения телекоммуникационных систем и т.п.); в определенной мере может опираться на поддержку со стороны различных государственных структур; объединяет большое количество специалистов из различных исследовательских, учебных, коммерческих организаций, но при этом большинство участников (членов) может не иметь конкретных обязательств, обязывающих вносить вклад в работу и достигать определенных целей.

Основными наиболее крупными и известными международными профессиональными объединениями, связанными с вопросами информационной безопасности, являются:

- ITU – International Telecommunication Union;
- IEEE – Institute of Electrical and Electronics Engineers;
- ACM – Association for Computing Machinery;
- W3 Consortium;
- ISSA – Information Systems Security Association;
- ISO – International Organization for Standardization;
- IETF – Internet Engineering Task Force;
- ICISA – International Computer Security Association;
- Information Systems Audit and Control Association (ISACA);
- Internet Security Alliance.

3.1. Международная организация по стандартизации (ИСО) - International Organization for Standardization (ISO)

Международная организация по стандартизации, ИСО (International Organization for Standardization, ISO) – международная организация, занимающаяся выпуском стандартов.

Международная организация по стандартизации создана в 1946 году двадцатью пятью национальными организациями по стандартизации, на основе двух организаций: ISA (International Federation of the National Standardizing Associations), учреждённой в Нью-Йорке в 1926 году (расформирована в 1942) и UNSCC (United Nations Standards Coordinating Committee), учреждённой в 1944 году. Фактически её работа началась с 1947 года. СССР был одним из основателей организации, постоянным членом руководящих органов, дважды представитель Госстандарта избирался председателем организации. Россия стала членом ИСО как правопреемник СССР. 23 сентября 2005 года Россия вошла в Совет ИСО.

При создании организации и выборе её названия учитывалась необходимость того, чтобы аббревиатура наименования звучала одинаково на всех языках. Для этого было решено использовать греческое слово ίσος (исос) – равный, вот почему на всех языках мира Международная организация по стандартизации имеет краткое название «исо».

Сфера деятельности ИСО касается стандартизации во всех областях, кроме электротехники и электроники, относящихся к компетенции Международной электротехнической комиссии (МЭК, IEC). Некоторые виды работ выполняются совместными усилиями этих организаций. Кроме стандартизации, ИСО занимается проблемами сертификации.

ИСО определяет свои задачи следующим образом: содействие развитию стандартизации и смежных видов деятельности в мире с целью обеспечения международного обмена товарами и услугами, а также развития сотрудничества в интеллектуальной, научно-технической и экономической областях.

Официальными языками являются: английский, французский и русский. На сегодняшний день в состав ИСО входит 165 стран своими национальными

организациями по стандартизации. Россию представляет Федеральное агентство по техническому регулированию и метрологии в качестве комитета — члена ИСО. Всего в составе ИСО более 100 комитетов-членов. Кроме комитетов-членов, членство в ИСО может иметь статус членов-корреспондентов, которыми являются организации по стандартизации развивающихся государств. Категория член-абонент введена для развивающихся стран.

Комитеты-члены имеют право принимать участие в работе любого технического комитета ИСО, голосовать по проектам стандартов, избираться в состав Совета ИСО и быть представленными на заседаниях Генеральной ассамблеи. Члены-корреспонденты (их 42) не ведут активной работы в ИСО, но имеют право на получение информации о разрабатываемых стандартах. Члены-абоненты уплачивают льготные взносы, имеют возможность быть в курсе международной стандартизации.

3.2.Международная электротехническая комиссия (МЭК) - International Electrotechnical Commission (IEC)

Международная электротехническая комиссия (МЭК; англ. International Electrotechnical Commission, IEC; фр. Commission électrotechnique internationale, CEI) — международная некоммерческая организация по стандартизации в области электрических, электронных и смежных технологий. Некоторые из стандартов МЭК разрабатываются совместно с Международной организацией по стандартизации (ISO).

МЭК составлена из представителей национальных служб стандартов. МЭК была основана в 1906 году и в настоящее время в её состав на правах полноправных и ассоциированных членов входят 83 страны. Первоначально комиссия располагалась в Лондоне, с 1948 года по настоящее время штаб-квартира находится в Женеве, Швейцария. В настоящее время имеет региональные центры в Юго-восточной Азии (Сингапур), Латинской Америке (Сан-Пауло, Бразилия) и Северной Америке (Бостон, США).

МЭК способствовала развитию и распространению стандартов для единиц измерения, особенно гаусса, герца, и вебера. Также МЭК предложила систему стандартов, которая, в конечном счёте, вошла в систему единиц СИ. В 1938 году был издан международный словарь с целью унифицировать терминологию в области электротехники. Эти усилия продолжаются и в подготовке Международного электротехнического словаря (известного также как Electropedia), способствующего совместной работе в электротехнических областях промышленности.

Стандарты МЭК имеют номера в диапазоне 60 000 — 79 999, и их названия имеют вид типа МЭК 60411 Графические символы. Номера старых стандартов МЭК были преобразованы в 1997 году путём добавления числа 60 000, например, стандарт МЭК 27 получил номер МЭК 60027. Стандарты, развитые совместно с Международной организацией по стандартизации, имеют названия вида ISO/IEC 7498-1:1994 Open Systems Interconnection: Basic Reference Model.

3.3. Британский институт стандартов – British Standards Institution (BSI)

Группа BSI начала свою деятельность в 1901 г. как комитет инженеров, которые устанавливали стандарты на сталь. Эти стандарты использовались британскими промышленниками для производства более качественной и конкурентоспособной продукции. BSI — член Международной организации по стандартизации (ISO).

BSI Group уже более 100 лет является лидером в предоставлении бизнес решений в области Систем Менеджмента организациям по всему миру. BSI Group предлагает наиболее полный набор услуг по Сертификации Систем Менеджмента и продукции, стандартизации и всем видам обучения.

Группа BSI насчитывает в своём штате 2274 сотрудника. Каждый год публикуется более 2000 стандартов BSI.

Деятельность группы BSI:

- Услуги и решения по системам менеджмента;
- Услуги по оценке и сертификации;
- Сертификация продукции;

- Обучение системам менеджмента;
- Стандарты и публикации;
- Маркировка CE

Британский институт стандартов — крупнейший мировой провайдер стандартов, покрывающий все аспекты современной экономики от защиты интеллектуальной собственности до технических спецификаций систем индивидуальной защиты. Центр Британских стандартов базируется в Лондоне и имеет широкие связи с национальными институтами стандартизации других стран.

3.4. Институт инженеров по электронике и электротехнике – Institute of Electrical and Electronics Engineers (IEEE)

IEEE является одной из наиболее известных профессиональных организаций, существует с 1884 года и в настоящее время насчитывает около 380000 членов из 150 стран мира. В сферу ее интересов входит множество вопросов, связанных с электротехникой, радиоэлектроникой, вычислительной техникой, информатикой, а также некоторыми разделами физики и математики. Основные направления работы этой организации:

- проведение специализированных профессиональных конференций;
- публикация специализированных изданий;
- поддержка образовательной деятельности;
- поддержка инновационных технических и методических разработок в различных сферах;
- разработка и распространение технических стандартов.

В состав IEEE входят 10 региональных отделений, 38 профессиональных обществ, 4 совета и 1450 студенческих отделений. Текущее управление деятельностью на верхнем уровне осуществляется Советом директоров и Исполнительным комитетом, работу которых возглавляют Президент и Исполнительный директор.

Одним из основных подразделений IEEE, специализирующихся на вопросах информационной безопасности, является Технический комитет по безопасности и

защите частной информации – "IEEE Computer Society Technical Committee on Security and Privacy" (<http://www.ieee-security.org/>). В его составе функционируют три подкомитета:

- Подкомитет по стандартам (Subcommittee on Standards);
- Подкомитет по академической работе (Subcommittee on Academic Affairs);
- Подкомитет по специализированным конференциям (Subcommittee on Security Conferences).

Основными мероприятиями, которые проводит этот комитет, являются:

- Ежегодный симпозиум по безопасности и защите частной информации (IEEE CS Symposium on Security and Privacy);
- Ежегодный семинар по основам информационной безопасности (Computer Security Foundations Workshop).

Также комитет ведет работу по сбору и обобщению актуальной информации о событиях в сообществе специалистов по информационной безопасности: объявления о планируемых конференциях, отчеты о прошедших конференциях и семинарах, обзоры литературы и периодики, ссылки на ресурсы в сети Интернет и т.п. Специальный информационный бюллетень с этой информацией – "Cipher" – рассылается подписчикам в среднем один раз в два месяца.

3.5. Ассоциация вычислительной техники – Association for Computing Machinery (ACM)

ACM является одной из старейших организаций, связанных с информационными технологиями, – она была основана в 1947 году, на заре развития компьютерной техники. Основные задачи ACM - поддержка образовательных проектов в сфере информационных технологий, организация научно-практических конференций, симпозиумов и семинаров, общественно-политическая работа, связанная с информационными технологиями, публикация периодических изданий и сборников научных трудов, посвященных проблемам современных информационных технологий, поддержка электронного архива таких публикаций, а также другая подобная деятельность. Основным

управляющим органом этой организации является Совет АСМ, в который входит 16 человек, в том числе президент и вице-президент. Управление текущими делами Ассоциации осуществляют четыре профильных комитета. Штаб-квартира АСМ, в которой работают основные исполнительные органы, располагается в Нью-Йорке, начиная с 1960 года.

Одной из основ организации работы АСМ является разделение всего сообщества членов ассоциации на так называемые группы специальных интересов (*Special Interests Group – SIG*) – подразделения, специализирующиеся на отдельных относительно узких проблемах развития информационных технологий. Всего АСМ объединяет 34 группы, специализирующиеся на различных вопросах разработки и использования программного обеспечения, аппаратных средств и телекоммуникаций. Каждая из групп самостоятельно определяет для себя границы своей деятельности, а их политика и финансовые вопросы координируются одним из комитетов.

Одна из этих групп – **Special Interest Group on Security, Audit and Control (SIGSAC)**, Группа специальных интересов по вопросам безопасности, аудита и контроля, (<http://www.acm.org/sigs/sigsac/>) – специализируется на вопросах информационной безопасности. Основной задачей данной группы является организация работы специализированных научно-практических конференций, таких как:

- Симпозиум по технологиям и моделям управления доступом (SACMAT: ACM Symposium on Access Control Models and Technologies), проводимый ежегодно начиная с 1995 года;
- Конференция по безопасности компьютеров и коммуникаций (CCS: ACM Conference on Computer and Communications Security), проводимая ежегодно начиная с 1993 года.

Кроме того, вопросы информационной безопасности прямо или косвенно затрагиваются в работе других специализированных групп Ассоциации, таких как, например, *Special Interest Group on Electronic Commerce* (Группа по проблемам электронной коммерции).

3.6.Консорциум Всемирной Паутины – World Wide Web Consortium (W3C)

Создание W3C было инициировано в 1989 году с целью разработки единых, согласованных стандартов обмена информацией в глобальных сетях передачи данных, а официально создание консорциума было оформлено в 1994г. Его основными задачами являются:

- обеспечение возможности доступа к сети Интернет для как можно большего числа людей вне зависимости от знания иностранных языков, культурной принадлежности, географического положения и доступных им технических средств и технической инфраструктуры;
- обеспечение возможности подключения к Интернет различных технических устройств;
- обеспечение возможности структурирования и формализации информации, доступной через Интернет, с целью сделать ее как можно более пригодной для автоматизированной обработки;
- обеспечение надежности и безопасности обмена информацией, а также возможности участвовать в информационном обмене с тем уровнем защищенности, который отдельные пользователи считают для себя подходящим.

К настоящему времени консорциум объединяет более четырехсот ведущих технологических и телекоммуникационных компаний, правительственных организаций, исследовательских центров, институтов и университетов по всему миру. Кроме того, в штате консорциума состоят около 70 независимых технических экспертов, обеспечивающих его работу. Финансирование деятельности осуществляется за счет членских взносов, а основные административные функции и повседневная деятельность выполняются на базе трех организаций:

1. Массачусетский технологический институт (США);
2. Европейский консорциум по исследованиям в области информатики и математики (Франция);
3. Университет Кейо (Япония).

Помимо формирования стандартов ("рекомендаций"), эта организация также занимается образовательной деятельностью и предоставляет возможности для обсуждения различных вопросов, связанных с функционированием Интернет.

Деятельность консорциума организована в виде групп: Рабочие группы (занимаются проработкой технических вопросов), Группы специальных интересов и Координационные группы (обеспечивают взаимодействие между другими группами). В каждую группу входят представители организаций-участников консорциума и приглашенные эксперты. Сферы работы консорциума ("домены", Domain), разделены на направления (Activities). Работа по двадцати четырем направлениям выполняется в общей сложности шестьюдесятью группами.

Вопросами информационной безопасности занимается сфера "Технология и общество" (Technology and Society Domain) в рамках специального направления "Безопасность" (W3C Security Activity), состоящего из двух рабочих групп. Также до 2006 года в составе Консорциума функционировало направление "Защита частной информации" (Privacy).

К работам консорциума в сфере информационной безопасности относятся:

- разработка стандарта цифровых подписей для информационных ресурсов (PICS Signed Labels 1.0 Specification);
- разработка системы электронной подписи для документов XML;
- разработка стандартов передачи зашифрованных данных с использованием языка XML.

3.7. Международный союз электросвязи – International Telecommunication Union (ITU)

ITU является старейшей международной организацией, связанной с информационными технологиями. Она была основана в 1885 году как Международный телеграфный союз и получила свое новое название в 1934 году. В настоящее время ITU объединяет 189 государств. Как понятно из названия, основной ее задачей изначально было управление и координация деятельности в сфере передачи информации и, в частности, в радиосвязи и телеграфной связи.

Однако по мере развития глобальных компьютерных сетей и интеграции компьютерных и телекоммуникационных систем, область деятельности ИТУ была значительно расширена и в настоящее время включает в себя множество вопросов, связанных с построением компьютерных сетей, передачей цифровых данных, обработкой информации и т.п.

Членами ИТУ-Т являются:

- государственные органы власти (министерства и ведомства связи отдельных стран);
- научные организации и компании – производители телекоммуникационного оборудования;
- региональные и международные телекоммуникационные организации.

Функциональными органами ИТУ-Т являются:

- Всемирная ассамблея по стандартизации телекоммуникаций (*World Telecommunication Standardization Assembly*), проводимая каждые четыре года, – основной руководящий орган сектора стандартизации;
- Бюро по стандартизации телекоммуникаций (*Telecommunication Standardization Bureau*) – исполнительное подразделение сектора стандартизации;
- Исследовательские группы (всего их 14);
- Консультативная группа по стандартизации телекоммуникаций (*Telecommunication Standardization Advisory Group*) – вспомогательное подразделение, осуществляющее координационную работу.

Высшим органом власти Союза является Полномочная Конференция (*Plenipotentiary Conference*), собрание делегаций государств – членов Союза, проходящее раз в четыре года. Основные исполнительные органы — Совет и Генеральный секретариат ИТУ. Основные рабочие подразделения разделены на три сектора:

- сектор стандартизации связи, ИТУ-Т;
- сектор радиосвязи, ИТУ-R;
- сектор развития электросвязи ИТУ-D.

ИТУ-R и ИТУ-D выполняют отдельные исследовательские, координационные и технические функции (такие как, например, регистрация радиочастот или

координация работы космических телекоммуникационных спутников), тогда как Сектор стандартизации связи – ITU-T в большей степени отвечает за решение стратегических задач развития информационных технологий и инфраструктуры и, в частности, за разработку методик и стандартов, необходимых для всего мирового сообщества.

Основной целью работы ITU-T является разработка универсальных рекомендаций и международных стандартов, относящихся к различным сферам телекоммуникационных технологий и управления телекоммуникациями. Разрабатываемые рекомендации обеспечивают основу для развития рынка услуг связи, создания совместимых технических и организационных систем и т.п. С точки зрения обеспечения информационной безопасности наиболее значимыми стали рекомендации, относящиеся к серии "X – Сети передачи данных и связь открытых систем" и, в частности, к серии "X.8xx – Безопасность".

В соответствии с Резолюцией 1 Всемирной ассамблеи по стандартизации телекоммуникаций 2000-го года, была введена практика назначения Ведущих исследовательских групп (*Lead Study Groups, LSGs*) по определенным вопросам, требующим одновременной координации усилий нескольких исследовательских групп, которые работают в различных областях. Начиная с сентября 2001 года функционирует "Исследовательская группа 17: Сети передачи данных и телекоммуникационное программное обеспечение" ("*Study Group 17: Data Networks and Telecommunication Software*"), образованная на основе существовавших до этого "Исследовательской группы 7" и "Исследовательской группы 10". С момента своего образования она является Ведущей исследовательской группой по вопросам безопасности коммуникационных систем (*Communication Systems Security, CSS*) и, соответственно, не только работает над обеспечением безопасности технологий, напрямую относящихся к ее компетенции, но и курирует вопросы обеспечения безопасности различных коммуникационных технологий, разрабатываемых другими исследовательскими группами.

Одной из наиболее значимых разработок этой группы в сфере информационной безопасности считается Стандарт X.509, заложивший основы

развития инфраструктуры публичных ключей. Наиболее актуальными проблемами, над которыми в настоящее время работает Ведущая исследовательская группа по вопросам безопасности коммуникационных систем, являются:

- управление безопасностью;
- безопасность мобильных систем;
- безопасность систем связи служб реагирования на чрезвычайные ситуации;
- телебиометрия.

В целом же работа этой исследовательской группы охватывает следующие основные сферы:

- безопасность управления сетями (включает в себя работу над следующими рекомендациями: М.3010 – Принципы сетей управления телекоммуникациями, М.3016 – Обзор безопасности сетей управления телекоммуникациями и некоторые другие);
- аутентификация и службы каталогов (Х.500 – Обзор концептуальных моделей и сервисов, Х.509 – Основы технологии публичных ключей и сертификатов и некоторые другие);
- управление системами (Х.733 – Функция отчета о происшествии, Х.740 – Функция проведения аудита безопасности и некоторые другие);
- основы *архитектуры безопасности* (Х.800 – *Архитектура безопасности* инфраструктуры открытых систем для приложений ITU; Х.802 – Модель безопасности нижних уровней, Х.803 – Модель безопасности верхних уровней и некоторые другие);
- факсимильная связь (Т.36 – Возможности обеспечения безопасности при использовании факсимильных аппаратов третьей группы; Т.563 – Характеристики терминалов для использования с факсимильными аппаратами четвертой группы и некоторые другие);
- телевизионные и кабельные системы (J.170 – Спецификация безопасности IPCabelcom и некоторые другие);

- техника обеспечения безопасности (X.841 – Объекты информационной безопасности для контроля доступа и некоторые другие);
- мультимедийные коммуникации (H.233 – Система обеспечения конфиденциальности для аудиовизуальных сервисов, H.234 – Управление ключами шифрования и *системой аутентификации* в аудиовизуальных сервисах и некоторые другие).

Помимо разработки рекомендаций и стандартов, одним из важных направлений работы ITU также стало обеспечение информационного обмена в различных формах: распространение методических материалов, касающихся обеспечения информационной безопасности, проведение семинаров и конференций. Одним из наиболее масштабных таких мероприятий является Всемирный саммит по *информационному обществу* (WSIS: The World Summit On The Information Society).

3.8. Организация Объединенных Наций

Организация Объединённых Наций – международная организация, созданная для поддержания и укрепления международного мира и безопасности, развития сотрудничества между государствами.

ООН считается универсальным форумом, наделённым уникальной легитимностью, несущей конструкцией международной системы коллективной безопасности, главным элементом современной многосторонней дипломатии.

Основы её деятельности и структура разрабатывались в годы Второй мировой войны ведущими участниками антигитлеровской коалиции. Название «Объединённые Нации» было впервые использовано в Декларации Объединённых Наций, подписанной 1 января 1942 года.

Устав ООН был утверждён на Сан-Францисской конференции, проходившей с апреля по июнь 1945 года, и подписан 26 июня 1945 года представителями 50 государств. 15 октября 1945 года Польша также подписала Устав, вступив, таким образом, в число первоначальных членов Организации. Дата вступления Устава в силу (24 октября) отмечается как День Организации Объединённых Наций.

Генеральная Ассамблея ООН занимает центральное место в качестве главного совещательного, директивного и представительного органа. Генеральная Ассамблея рассматривает принципы сотрудничества в области обеспечения международного мира и безопасности; избирает непостоянных членов Совета Безопасности ООН, членов Экономического и Социального Совета; по рекомендации Совета Безопасности назначает Генерального секретаря ООН; совместно с Советом Безопасности избирает членов Международного Суда ООН; координирует международное сотрудничество в экономической, социальной, культурной и гуманитарной сферах; осуществляет иные полномочия, предусмотренные в Уставе ООН.

У Генеральной Ассамблеи сессионный порядок работы. Она может проводить регулярные, специальные и чрезвычайные специальные сессии.

Ежегодная очередная сессия Ассамблеи открывается в третий вторник сентября и работает под руководством Председателя Генеральной Ассамблеи (или одного из его 21 заместителя) на пленарных заседаниях и в главных комитетах до полного исчерпания повестки дня.

Генеральная Ассамблея, согласно её решению от 17 декабря 1993 года, имеет в своем составе 6 Главных комитетов:

- Комитет по вопросам разоружения и международной безопасности (Первый комитет);
 - Комитет по экономическим и финансовым вопросам (Второй комитет);
 - Комитет по социальным и гуманитарным вопросам и вопросам культуры (Третий комитет);
 - Комитет по специальным политическим вопросам и вопросам деколонизации (Четвёртый комитет);
 - Комитет по административным и бюджетным вопросам (Пятый комитет);
 - Комитет по правовым вопросам (Шестой комитет).
- Кроме того, Генеральной Ассамблеей учреждены комитеты:

– Генеральный комитет — выносит рекомендации Ассамблее относительно утверждения повестки дня, распределения пунктов повестки дня и организации работы;

– Комитет по проверке полномочий — представляет Ассамблее доклады о полномочиях представителей.

В состав Генерального комитета входят: Председатель Генеральной Ассамблеи; заместители Председателя, председатели главных комитетов, избираемые с учётом принципа справедливого географического представительства пяти регионов (районов): Азии, Африки, Латинской Америки, Западной Европы (включая Канаду, Австралию и Новую Зеландию) и Восточной Европы.

Специальные сессии Генеральной Ассамблеи ООН могут созываться по любому вопросу по требованию Совета Безопасности в течение 15 дней со дня получения такого требования Генеральным секретарём ООН или большинства членов ООН. На начало 2014 года было созвано 28 специальных сессий по вопросам, касающимся большинства государств мира: по правам человека, охране окружающей среды, борьбе с наркотиками и др.

Чрезвычайные специальные сессии могут созываться по требованию Совета Безопасности ООН или большинства государств-членов ООН в течение 24 часов после получения такого требования Генеральным секретарём ООН.

Совет Безопасности несёт главную ответственность за поддержание международного мира и безопасности, его решениям обязаны подчиняться все члены ООН. Пять постоянных членов Совета Безопасности (Российская Федерация, США, Великобритания, Франция, Китай) обладают правом вето.

Совет Безопасности состоит из 15 членов: пять членов Совета — постоянные (Россия, США, Великобритания, Франция и Китай), остальные десять членов (по терминологии Устава — «непостоянные») избираются в Совет в соответствии с процедурой, предусмотренной Уставом (пункт 2 статьи 23).

3.9. Совет Европы (комитет министров)

Совет Европы — международная организация, содействующая сотрудничеству между её членами, странами Европы, в области стандартов права, прав человека, демократического развития, законности и культурного взаимодействия. Будучи основанным в 1949 году, Совет Европы является старейшей в Европе международной организацией. В его состав входят 47 государств, в которых проживают более 800 млн человек. Совет Европы является полностью самостоятельной организацией, не входящей в систему Европейского союза, объединяющего только 28 государств. В отличие от Евросоюза, Совет Европы не может издавать обязательные законы, однако эти две международные организации имеют некоторые общие символические атрибуты, например, гимн и флаг.

Одним из самых значительных достижений Совета Европы считается разработка и принятие Европейской конвенции о защите прав человека и основных свобод.

Совет Европы был создан на волне призывов к единению Европы и построения своего рода «Соединённых Штатов Европы» после Второй мировой войны. Одним из наиболее активных сторонников этой идеи считается Уинстон Черчилль.

Свое знаменитое обращение к созданию «Соединённых Штатов Европы» и Совету Европы Уинстон Черчилль произнёс 19 сентября 1946 года в Цюрихском университете. Ранее в 1943 году он по радио обращался к нации с идеей создания Совета Европы. В дальнейшем структура Совета Европы длительно обсуждалась ведущими политическими лидерами. Было две основных школы, предлагавшие различные структуры организации: согласно первой предлагалось построить классическую международную организацию с представителями стран-участниц, тогда как согласно второй предлагалось создание политического форума с парламентариями. В итоге оба принципа были взяты в основу учрежденных Комитета министров и Парламентской ассамблеи. Аналогичная двойная структура была впоследствии скопирована Европейским сообществом, НАТО и ОБСЕ.

Официально Совет был создан 5 мая 1949 г. Устав Совета Европы был подписан в Лондоне десятью государствами: Королевством Бельгии, Королевством Дании, Республикой Ирландией, Итальянской Республикой, Великим Герцогством Люксембург, Королевством Нидерландов, Королевством Норвегии, Соединённым Королевством Великобритании и Северной Ирландии, Французской Республикой и Королевством Швеции. Штаб-квартира СЕ расположилась в Страсбурге — городе на границе Франции и Германии, в качестве символа примирения двух стран.

4. ОСНОВНЫЕ НОРМАТИВНО-ПРАВОВЫЕ ДОКУМЕНТЫ В ОБЛАСТИ ИБ

Система нормативных правовых актов Российской Федерации состоит из нескольких уровней, от международного до уровня предприятия. К числу международных актов относятся документы, которые подписаны от имени Российской Федерации. Ниже приведен список основных нормативных правовых документов, касающихся информационной безопасности.

Международные документы

1. **«Конвенция, учреждающая Всемирную организацию интеллектуальной собственности»** (Стокгольм, 14.07.1967, в редакции от 2.10.1979. Вступила в силу для СССР 26.04.1970).
2. **«Всемирная конвенция об авторском праве»** (Женева, 6.09.1952. Пересмотрена в Париже 24.07.1971. Вступила в силу для СССР 27.05.1973).
3. **«Брюссельская конвенция о распространении несущих программы сигналов, передаваемых через спутники. (Конвенция по спутникам)»**. 1974 год. Российская Федерация присоединилась 20.01.1989.
4. **«Бернская конвенция об охране литературных и художественных произведений в редакции 1971 года»**. Российская Федерация присоединилась 13.03.1995.

5. **«Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».** Страсбург, 28.01.1998. Ратифицирована Законом РФ от 19.12.2005 № 160-ФЗ.

6. **«Окинавская Хартия глобального информационного общества»**

Окинава. 22 июля 2000 года.

7. **Декларация принципов. «Построение информационного общества – глобальная задача в новом тысячелетии».** Всемирная встреча на высшем уровне по вопросам информационного общества. Женева. 10.12.2003.

8. **«Международная конвенция об охране прав исполнителей, изготовителей фонограмм и вещательных организаций»** (Рим, 26.10.1961. Вступила в силу для Российской Федерации 26.05.2003).

9. **«Конвенция об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм»** (Женева, 29.10.1971; вступила в силу для Российской Федерации 13.03.1995).

10. **Конвенция Совета Европы о компьютерных преступлениях. СДСЕ № 185.** (Будапешт. Открыта для подписания 23.11.2001).

Концептуальные документы Российской Федерации

1. **«Конституция Российской Федерации»** от 12.12.1993.

2. **«Доктрина информационной безопасности Российской Федерации».** Утверждена Указом Президента Российской Федерации от 06.12.2016 № 646.

3. **«Концепция национальной безопасности Российской Федерации»** Утверждена Указом Президента Российской Федерации от 10.01.2000 № 24

4. **«Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года».** Распоряжение Правительства РФ от 27.09.2004 № 1244-р. (ред. от 10.03.2009)

5. **«Концепции создания системы персонального учета населения Российской Федерации».** Утверждена Распоряжением Правительства РФ от 9.06.2005 № 748-р.

6. **«Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от**

несанкционированного доступа к информации». Утвержден решением Государственной технической комиссии от 30.03.1992.

7. Стратегия развития информационного общества в России. (Указ Президента РФ от 09.05.2017 N 203.

Федеральные Законы Российской Федерации

1. **«О средствах массовой информации»** от 27.12.1991 № 2124-1 (ред. от 18.04.2018, с изм. от 17.01.2019).

2. **«О безопасности»** от 5.03.1992 № 2446-I (ред. от 05.10.2015).

3. **«О правовой охране программ для электронных вычислительных машин и баз данных»** от 23.09.1992 № 3523-1. *Закон утратил силу с 01.01.2008 г. в связи с принятием Закона № 231-ФЗ от 18.12.2006 г.*

4. **«О государственной тайне»** от 21.07.1993 № 5485-I (ред. от 29.07.2018)

5. **«Гражданский кодекс Российской Федерации»** от 30.11.1994 № 51-ФЗ. (часть 1 с изм. от 29.12.2006 № 258-ФЗ, часть 2 с изм. от 18.12.2006 № 231-ФЗ, часть 3 с изм. от 18.12.2006 № 231-ФЗ, от 29.12.2006 № 258-ФЗ, часть 4 в соответствии с Федеральным законом от 18.12.2006 № 231-ФЗ вступила в силу с 1 января 2008 года.) (ред. от 03.08.2018) (с изм. и доп., вступ. в силу с 01.01.2019).

6. **«Об информации, информатизации и защите информации»** от 20.02.1995 № 24-ФЗ. *(ред. от 18.12.2018).*

7. **«О Федеральной службе безопасности»** от 3.04.1995 № 40-ФЗ (ред. от 07.03.2018).

8. **«Об оперативно-розыскной деятельности»** от 12.08.1995 № 144-ФЗ (ред. от 06.07.2016).

9. **«О государственной охране»** от 7.05.1996 № 57-ФЗ (ред. от 07.03.2018)

10. **«Об участии в международном информационном обмене»** от 4.06.1996 № 85-ФЗ. *Закон утратил силу в связи с принятием Закона № 149-ФЗ.*

11. **«Уголовный кодекс Российской Федерации»** от 13.06.1996 № 63-ФЗ (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019).

12. **«О внешней разведке»** от 10.01.1996 № 5-ФЗ(ред. от 07.03.2018).

13. **«О лицензировании отдельных видов деятельности»** от 8.08.2001 № 128-ФЗ (с последними изменениями и дополнениями от 05.02.2007 № 13-ФЗ).
14. **«Кодекс Российской Федерации об административных правонарушениях»** от 30.12.2001 № 195-ФЗ (ред. от 07.04.2025).
15. **«Трудовой Кодекс Российской Федерации»** от 30.12.2001 № 197-ФЗ (ред. от 07.04.2025).
16. **«Об электронной цифровой подписи»** от 10.01.2002 № 1-ФЗ. (с изм. и доп., вступ. в силу с 31.12.2017).
17. **«О техническом регулировании»** от 27.12.2002 № 184-ФЗ (ред. от 29.07.2017).
18. **«О государственной автоматизированной системе Российской Федерации «Выборы»** от 10.01.2003 № 20-ФЗ.
19. **«Таможенный кодекс Российской Федерации»** от 28.05.2003 № 61-ФЗ (с последними изменениями от 19.12.2006 № 238-ФЗ).
20. **«О связи»** от 7.07.2003 № 126-ФЗ (ред. от 27.12.2018).
21. **«О коммерческой тайне»** от 29.07.2004 № 98-ФЗ (ред. от 18.04.2018)
22. **«Об архивном деле в Российской Федерации»** от 22.10.2004 № 125-ФЗ (с изменениями и дополнениями от 04.12.2006 № 202-ФЗ).
23. **«О ратификации конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»** от 19.12.2005 № 160-ФЗ.
24. **«О рекламе»** от 13.03.2006 № 38-ФЗ (ред. от 30.10.2018).
25. **«О персональных данных»** от 27.07.2006 № 152-ФЗ. (ред. от 08.08.2024) .
26. **«Об информации, информационных технологиях и о защите информации»** от 27.07.2006 № 149-ФЗ. (ред. от 18.12.2018).
27. **«О транспортной безопасности»** от 9.02.2007 № 16-ФЗ. (ред. от 03.08.2018)
28. **«О внесении изменений в статьи 146 и 180 Уголовного кодекса Российской Федерации»** от 9.04.2007 № 42-ФЗ.

29. **«О безопасности критической информационной инфраструктуры Российской Федерации»** от 26.07.2017 № 187-ФЗ (ред. От 10.07.2023).

30. **«О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»»** от 26.07.2017 № 193-ФЗ.

31. **«О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»** от 26.07.2017 № 194-ФЗ.

32. **«О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»** от 28.05.2022 № 141-ФЗ.

33. **«О контроле за деятельностью лиц, находящихся под иностранным влиянием»** от 14.07.2022 № 255-ФЗ (ред. От 28.12.2024).

34. **«О внесении изменения в статью 104.1 Уголовного кодекса Российской Федерации»** от 13.06.2023 № 214-ФЗ.

35. **“Об информации, информационных технологиях о защите информации”** от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024, с изм. и доп., вступ. в силу с 01.01.2025).

36. **"О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации"** от 29.12.2022 № 584-ФЗ.

37. **"О внесении изменений в Кодекс Российской Федерации об административных правонарушениях"** от 24.06.2023 № 277-ФЗ.

38. **"О внесении изменений в Федеральный закон "О персональных данных", отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона "О банках и банковской деятельности"** от 14.07.2022 № 266-ФЗ.

39. **"Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о**

внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации" от 29.12.2022 № 572-ФЗ.

Указы Президента Российской Федерации

1. От 31.12.1993 № 2334 «О дополнительных гарантиях прав граждан на информацию».
2. От 20.01.1994 № 170 «Об основах государственной политики в сфере информатизации».
3. От 30.11.1995 № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне».
4. От 3.04.1995 № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».
5. От 8.11.1995 № 1108 «О создании Межведомственной комиссии по защите государственной тайны».
6. От 9.01.1996 № 21 «О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации».
7. От 6.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».
8. От 10.01.2000 № 24 «Об утверждении концепции национальной безопасности Российской Федерации».
9. От 11.03.2003 № 308 «О мерах по совершенствованию государственного управления в области безопасности Российской Федерации».
10. От 11.08.2003 № 960 «Вопросы Федеральной службы безопасности Российской Федерации».
11. От 12.05.2004 № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена».

12. От 20.05.2004 № 649 «Структура федеральных органов исполнительной власти».

13. От 7.06.2004 № 726 «Об утверждении Положений о Совете Безопасности Российской Федерации и аппарате Совета Безопасности...».

14. От 7.08.2004 № 1013 «Вопросы Федеральной службы охраны Российской Федерации».

15. От 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

16. От 6.10.2004 № 1286 «Вопросы Межведомственной комиссии по защите государственной тайны»

17. Распоряжение от 16.04.2005 № 151-рп «О перечне должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне».

18. От 28.10.2005 № 1244 «Об утверждении Положения о Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности».

19. От 12.03.2007 № 320 «О Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия».

20. От 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

21. От 03.02.2012 № 803 Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации.

22. От 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации».

23. От 14.04.2022 № 203 «О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации».

24. От 02.03.2018 № 98 «О внесении изменений в перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента Российской Федерации».

25. От 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".

26. От 12.04.2021 № 213 "Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности".

27. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации, утверждены Секретарем Совета Безопасности Российской Федерации 31.08.2017.

Постановления Правительства Российской Федерации

1. От 5.12.1991 № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

2. От 3.11.1994 № 1224 «О присоединении Российской Федерации к Бернской Конвенции об охране литературных и художественных произведений в редакции 1971 года и дополнительным протоколам 1 и 2, Конвенции 1971 года об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм».

3. От 3.11.1994 № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в Федеральных органах исполнительной власти».

4. От 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны».

5. От 4.09.1995 № 870 «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».

6. От 26.06.1995 № 608 «О сертификации средств защиты информации».

7. От 28.10.1995 № 1050 «Об утверждении инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне».

8. От 28.02.1996 № 226 «О государственном учете и регистрации баз и банков данных».

9. От 1.07.1996 № 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно – розыскной деятельности.

10. От 3.06.1998 № 564 «Об утверждении Положения о лицензировании деятельности по международному информационному обмену».

11. От 22.08.1998 № 1003 «Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне».

12. От 10.03.2000 № 214 «Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежит лицензированию».

13. От 15.07.2002 № 526 «Об утверждении Положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность».

14. От 23.09.2002 № 691 «Об утверждении Положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».

15. От 12.02.2003 № 95 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

16. От 12.02.2003 № 98 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти».

17. От 15.08.2003 № 500 «О Федеральном информационном фонде технических регламентов и стандартов и единой информационной системе по техническому регулированию».

18. От 7.04.2004 № 178 «Вопросы Федеральной службы по интеллектуальной собственности, патентам и товарным знакам».

19. От 16.06.2004 № 299 «Об утверждении Положения о Федеральной службе по интеллектуальной собственности, патентам и товарным знакам».

20. От 17.06.2004 № 294 «О Федеральном агентстве по техническому регулированию и метрологии».

21. От 30.06.2004 № 319 «Об утверждении Положения о федеральном агентстве по информационным технологиям».

22. Распоряжение от 27.09.2004 № 1244-р "Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года".

23. От 3.12.2004 № 728 «О персональном составе Межведомственной комиссии по защите государственной тайны».

24. От 31.12.2004 № 896 «Об утверждении перечня средств связи, подлежащих обязательной сертификации».

25. Распоряжение от 9.06.2005 № 748-р об утверждении «Концепции создания системы персонального учета населения Российской Федерации».

26. От 27.08.2005 № 538 «Об утверждении правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно- розыскную деятельность».

27. От 17.11.2005 № 685 «О порядке распоряжения правами на результаты научно- технической деятельности».

28. От 23.01.2006 № 32 «Об утверждении правил оказания услуг связи по передаче данных».

29. От 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности».

30. От 13.04.2006 № 213 «О правительственной комиссии по федеральной связи».

31. Распоряжение от 17.07.2006 № 1024-р об одобрении «Концепции региональной информатизации до 2010 года».

32. От 15.08.2006 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».

33. От 31.08.2006 № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

34. От 14.02.2007 № 94 «О государственной информационной системе миграционного учета».

35. От 10.03.2007 № 147 «Об утверждении Положения о пользовании официальными сайтами в сети Интернет для размещения информации о размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд и о требованиях к технологическим, программным, лингвистическим, правовым и организационным средствам обеспечения пользования указанными сайтами».

36. От 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

37. От 15.01.2008 № 8 «О внесении изменений в пункт 5 Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».

38. От 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации».

39. От 13.04.2019 № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127».

40. От 24.12.2021 № 2431 «О внесении изменений в Правила категорирования объектов критической информационной инфраструктуры Российской Федерации».

41. От 19.08.2022 № 1463 «О внесении изменений в Правила категорирования объектов критической информационной инфраструктуры Российской Федерации».

42. От 20.12.2022 № 2360 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127».

43. От 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

44. От 08.06.2019 № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры».

45. От 21.12.2019 № 1746 «Об установлении запрета на допуск отдельных видов товаров, происходящих из иностранных государств, и внесении изменений в некоторые акты Правительства Российской Федерации».

46. От 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о

структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)».

47. От 22.08.2022 № 1478 «Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, Правил согласования закупок иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, а также закупок услуг, необходимых для использования этого программного обеспечения на таких объектах, и Правил перехода на преимущественное использование российского программного обеспечения, в том числе в составе программно-аппаратных комплексов, органов государственной власти, заказчиков, осуществляющих закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации».

48. От 24.05.2010 № 365 «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов».

49. От 06.07.2017 № 803 "О внесении изменений в постановление Правительства Российской Федерации от 24 мая 2010 г. № 365".

50. От 06.07.2015 № 676 "О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных

информационных систем и дальнейшего хранения содержащейся в их базах данных информации".

51. От 12.02.2020 № 126 "Об установке, эксплуатации и о модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования"

52. От 12.02.2020 № 127 "Об утверждении Правил централизованного управления сетью связи общего пользования".

53. От 06.05.2016 № 399 "Об организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса".

54. От 11.07.2018 № 808 "О внесении изменения в Правила организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с государственным участием и организациях оборонно-промышленного комплекса".

55. От 13.05.2022 № 860 "О проведении эксперимента по повышению уровня защищенности государственных информационных систем федеральных органов исполнительной власти и подведомственных им учреждений".

56. От 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

57. От 21.03.2012 № 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".

58. От 18.09.2012 № 940 “Об утверждении Правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определённых видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю”.

59. От 01.11.2012 № 1119 “Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных”.

60. От 29.06.2021 № 1046 "О федеральном государственном контроле (надзоре) за обработкой персональных данных".

61. От 29.12.2022 № 2526 "Об утверждении перечня случаев, при которых к операторам, осуществляющим трансграничную передачу персональных данных в целях выполнения возложенных международным договором Российской Федерации, законодательством Российской Федерации на государственные органы, муниципальные органы функций, полномочий и обязанностей, не применяются требования частей 3 - 6, 8 - 11 статьи 12 Федерального закона "О персональных данных".

62. От 10.01.2023 № 6 "Об утверждении Правил принятия решения о запрещении или об ограничении трансграничной передачи персональных данных уполномоченным органом по защите прав субъектов персональных данных и информирования операторов о принятом решении".

63. От 16.01.2023 № 24 "Об утверждении Правил принятия решения уполномоченным органом по защите прав субъектов персональных данных о запрещении или об ограничении трансграничной передачи персональных данных в целях защиты нравственности, здоровья, прав и законных интересов граждан"

64. От 01.06.2023 № 906 "Об аккредитации юридических лиц для обработки персональных данных отдельных категорий лиц, принимаемых на работу, непосредственно связанную с обеспечением транспортной безопасности, или

осуществляющих такую работу, в целях проверки субъектом транспортной инфраструктуры сведений, предусмотренных пунктами 1 - 6 и 9 части 1 статьи 10 Федерального закона "О транспортной безопасности", а также для принятия органами аттестации решения об аттестации сил обеспечения транспортной безопасности".

65. От 09.10.2021 № 1723 "Об утверждении Правил предоставления сведений, содержащихся в едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации, в том числе перечня указанных сведений и сроков их предоставления, и перечня обезличенных персональных данных, содержащихся в едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации".

66. От 30.09.2021 № 1657 "Об утверждении Правил осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, контроля и надзора за выполнением органами, организациями, индивидуальными предпринимателями и нотариусами, указанными в части 18.2 статьи 14.1 Федерального закона "Об информации, информационных технологиях и о защите информации", организационных и технических мер по обеспечению безопасности персональных данных и использованием средств защиты информации, указанных в части 18.3 статьи 14.1 Федерального закона "Об информации, информационных технологиях и о защите информации".

67. От 14.09.2021 № 1555 "О представлении Президенту Российской Федерации для внесения на ратификацию Соглашения о взаимной правовой помощи по административным вопросам в сфере обмена персональными данными".

68. От 24.05.2021 № 776 "Об утверждении Правил предоставления субсидии из федерального бюджета автономной некоммерческой организации "Университет Национальной технологической инициативы 2035" на проведение мероприятий по формированию школьниками и студентами проектов в сфере

искусственного интеллекта, обеспечению получения гражданами дополнительного профессионального образования в области искусственного интеллекта и в смежных областях с использованием механизма персональных цифровых сертификатов, разработке и актуализации цифрового решения для учета и развития участников сообществ в сфере искусственного интеллекта".

69. От 13.11.2019 № 1443 "О внесении изменения в Правила создания, формирования и ведения автоматизированной информационной системы "Реестр нарушителей прав субъектов персональных данных".

70. От 03.06.2019 № 705 "О внесении изменений в приложение № 2 к Правилам аккредитации юридических лиц для проведения оценки уязвимости объектов транспортной инфраструктуры и транспортных средств и в приложение № 2 к Правилам аккредитации юридических лиц для проведения проверки в целях принятия органами аттестации решения об аттестации сил обеспечения транспортной безопасности, а также для обработки персональных данных отдельных категорий лиц, принимаемых на работу, непосредственно связанную с обеспечением транспортной безопасности, или осуществляющих такую работу".

71. От 15.04.2019 № 454 "О внесении изменения в перечень 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".

72. От 13.02.2019 № 146 "Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных".

73. От 6.07.2008 № 512 "Об утверждении Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных".

74. От 31.05.2023 № 883 "Об утверждении Положения о единой биометрической системе, в том числе о ее региональных сегментах, и о признании утратившим силу постановления Правительства Российской Федерации от 16 июня 2022 г. № 1089".

75. От 25.05.2023 № 815 "Об утверждении перечня случаев, при которых аутентификация с использованием информационных систем организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, не допускается, и перечня случаев, при которых допускается использование биометрических персональных данных, согласие физического лица на обработку которых подписано простой электронной подписью, правом создания (замены) и выдачи ключа которой в порядке, предусмотренном законодательством Российской Федерации в области использования электронных подписей, обладает организация, осуществляющая аутентификацию на основе биометрических персональных данных физических лиц".

76. От 22.05.2023 № 810 "Об утверждении Правил аккредитации организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, оснований ее приостановления и прекращения и признании утратившим силу постановления Правительства Российской Федерации от 20 октября 2021 г. № 1799".

77. От 28.04.2023 № 670 "Об аккредитации государственных органов, Центрального банка Российской Федерации для осуществления аутентификации, о требованиях к организациям, привлекаемым государственными органами, Центральным банком Российской Федерации для осуществления функций операторов информационных систем, обеспечивающих аутентификацию физических лиц с использованием векторов единой биометрической системы, и о признании утратившим силу постановления Правительства Российской Федерации от 26 августа 2022 г. № 1498".

78. От 06.04.2023 № 552 "Об утверждении Правил рассмотрения обращения высшего исполнительного органа субъекта Российской Федерации об образовании регионального сегмента в составе единой биометрической системы, а также предложений уполномоченного органа в сфере идентификации и аутентификации физических лиц на основе биометрических персональных данных об образовании регионального сегмента в составе единой биометрической

системы и об исключении регионального сегмента из состава единой биометрической системы".

79. От 27.03.2023 № 478 "Об утверждении Правил представления физическим лицом отказа от сбора и размещения биометрических персональных данных в целях проведения идентификации и (или) аутентификации, отзыва такого отказа и письменного подтверждения многофункциональным центром предоставления государственных и муниципальных услуг представления физическим лицом указанных отказа и отзыва отказа, а также форм указанных отказа, отзыва отказа и письменного подтверждения их представления".

80. От 24.03.2023 № 451 "Об утверждении Правил направления оператором регионального сегмента единой биометрической системы, аккредитованным государственным органом, Центральным банком Российской Федерации в случае прохождения им аккредитации, организацией, осуществляющей аутентификацию на основе биометрических персональных данных физических лиц, мотивированного запроса оператору единой биометрической системы о предоставлении информации о результатах проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в единой биометрической системе, и предоставления оператором единой биометрической системы такой информации".

81. От 17.03.2023 № 405 "Об утверждении Правил получения согласия, указанного в пункте 6 части 5 статьи 26 Федерального закона "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации", и формы согласия физического лица на размещение его биометрических персональных данных в региональном сегменте единой биометрической системы".

82. От 29.12.2022 № 2511 "О Координационном совете по развитию цифровых технологий идентификации и аутентификации на основе биометрических персональных данных".

83. От 12.07.2022 № 1237 "О внесении изменения в состав сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, включая вид биометрических персональных данных".

84. От 16.06.2022 № 1089 "Об утверждении Положения о единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица".

85. От 15.06.2022 № 1066 "О размещении физическими лицами своих биометрических персональных данных в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица".

86. От 15.06.2022 № 1067 "О случаях и сроках использования биометрических персональных данных, размещенных физическими лицами в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица".

87. От 23.10.2021 № 1815 "Об утверждении перечня случаев осуществления сбора и обработки используемых для идентификации либо идентификации и аутентификации биометрических персональных данных в информационных системах организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также случаев использования организациями, за исключением кредитных организаций, некредитных финансовых организаций, которые осуществляют указанные в части первой статьи 761 Федерального закона "О

Центральном банке Российской Федерации (Банке России)" виды деятельности, субъектами национальной платежной системы, индивидуальными предпринимателями указанных информационных систем для идентификации либо идентификации и аутентификации физического лица, выразившего согласие на их проведение".

88. От 20.10.2021 № 1799 "Об аккредитации организаций, владеющих информационными системами, обеспечивающими идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, и (или) оказывающих услуги по идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц".

89. От 15.10.2021 № 1754 "Об утверждении требований к проверке простой электронной подписи, которой в соответствии с частями 5 и 23 статьи 14.1 Федерального закона "Об информации, информационных технологиях и о защите информации" подписаны согласия на обработку персональных данных и биометрических персональных данных, при хранении указанных согласий".

90. От 15.10.2021 № 1753 "Об утверждении требований к организационным и техническим условиям осуществления многофункциональными центрами предоставления государственных и муниципальных услуг размещения или обновления в единой системе идентификации и аутентификации сведений, необходимых для регистрации физических лиц в данной системе, размещения биометрических персональных данных в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, с использованием программно-технических комплексов".

91. От 13.09.2019 № 1197 "О внесении изменения в состав сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их

соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных".

92. От 28.12.2018 № 1703 "Об утверждении Правил предоставления оператором единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, в Министерство внутренних дел Российской Федерации и Федеральную службу безопасности Российской Федерации сведений, содержащихся в указанной системе".

93. От 14.07.2018 № 820 "Об установлении требований к проведению идентификации гражданина Российской Федерации государственными органами и иными организациями, осуществляющими размещение в электронной форме в единой системе идентификации и аутентификации сведений, необходимых для регистрации гражданина Российской Федерации в указанной системе, и иных сведений, предусмотренных федеральными законами, а также размещающими сведения в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации".

94. От 30.06.2018 № 772 "Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации".

95. От 29.06.2018 № 747 "Об установлении требований к фиксированию действий при размещении в электронной форме в единой системе идентификации

и аутентификации сведений, необходимых для регистрации гражданина Российской Федерации в указанной системе, и иных сведений, предусмотренных федеральными законами, а также при размещении биометрических персональных данных гражданина Российской Федерации в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации".

96. От 28.03.2018 № 335 "Об определении федерального органа исполнительной власти, осуществляющего регулирование в сфере идентификации граждан Российской Федерации на основе биометрических персональных данных".

97. От 29.05.2023 № 851 "О внесении изменений в постановление Правительства Российской Федерации от 15 июня 2022 г. № 1066".

Распоряжение Правительства Российской Федерации

1. От 22.12.2022 № 4088-р «Об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации».

Постановления Федеральных органов

1. Приказ ФСБ от 13.11.1999 № 564 «Об утверждении Положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия».

2. Положение о порядке регистрации сетевых электронных научных изданий, публикации в которых учитываются при защите диссертационных работ. Утверждено заместителем министра связи и информатизации 18.04.2002.

3. Приказ Федеральной налоговой службы от 3.03.2003 № БГ-3-28/96

«Об утверждении порядка доступа к конфиденциальной информации налоговых органов».

4. Приказ Государственного таможенного комитета Российской Федерации от 13.05.2004 № 564 «Об утверждении Положения об организации проверок информационных систем, информационных технологий и средств их обеспечения, используемых участниками внешнеэкономической деятельности».

5. Приказ ФСБ от 9.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

6. Стандарт Банка России СТО БР ИББС-1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». Введен в действие с 01.01.2006 распоряжением Банка России от 26.01.2006 № Р-27.

7. Постановление пленума Верховного суда Российской Федерации от 19.06.2006 № 15 «О вопросах, возникших у судов при рассмотрении гражданских дел, связанных с применением законодательства об авторском праве и смежных правах».

8. Постановление Центральной избирательной комиссии от 28.02.2007 № 200/1254- 4 «О внесении изменений в Положение об обеспечении безопасности информации в государственной автоматизированной системе Российской Федерации "ВЫБОРЫ".

9. Постановление Центральной избирательной комиссии от 28.02.2007 № 200/1255-4 «Об инструкции по размещению данных государственной автоматизированной системы Российской Федерации "ВЫБОРЫ" в сети Интернет».

10. Решение Совета главных конструкторов информатизации регионов Российской Федерации от 2.11.2006 № СГК-2/2-2006.

11. Приказ министерства информационных технологий и связи Российской Федерации от 9.01.2008 № 1 «Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации».

12. Приказ ФСТЭК, ФСБ, министерства информационных технологий и связи Российской Федерации от 13.02.2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».

13. Приказ ФСБ от 01.11.2022 №543 «Об определении переходного периода, предусмотренного подпунктом «б» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. № 50» (Зарегистрирован 01.12.2022 № 71291).

14. Приказ ФСБ от 11.05.2023 № 213 «Об утверждении порядка осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими» (Зарегистрирован 02.06.2023 № 73701).

15. Приказ ФСТЭК от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрирован 08.02.2017 № 49966).

16. Приказ ФСТЭК от 10.02.2022 № 26 «О внесении изменений в Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом Федерации службы по техническому и экспертному контролю от 6 декабря 2017 г. № 227» (Зарегистрирован 01.04.2022 № 68031).

17. Приказ ФСТЭК от 11.12.2017 № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрирован 28.12.2017 № 49500).

18. Приказ ФСТЭК от 26.04.2017 № 72 «О внесении изменений в Регламент Федеральной службы по техническому и экспортному контролю, утвержденный приказом ФСТЭК России от 12 мая 2005 г. № 167» (Зарегистрирован 18.05.2018 № 51127).

19. Приказ ФСТЭК от 28.05.2020 № 75 «Об утверждении Порядка согласования субъектом критической информационной инфраструктуры Российской Федерации с Федеральной службой по техническому и экспортному контролю подключения значимого объекта критической информационной инфраструктуры Российской Федерации к сети связи общего пользования» (Зарегистрирован 15.09.2020 № 59866).

20. Приказ ФСТЭК от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (Зарегистрирован 22.02.2018 № 50118).

21. Приказ ФСТЭК от 27.03.2019 № 64 «О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235» (Зарегистрирован 13.06.2019 № 54920).

22. Приказ ФСТЭК от 20.04.2023 № 69 «О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом ФСТЭК России от 21 декабря 2017 г. № 235» (Зарегистрирован 23.06.2023 № 73969).

23. Приказ ФСТЭК от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» (Зарегистрирован 13.04.2017 № 50753).

24. Приказ ФСТЭК от 21.03.2019 № 59 «О внесении изменений в форму направления сведений о результатах присвоения объекту критической

информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденную приказом Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 г. № 236» (Зарегистрирован 18.04.2019 № 54436).

25. Приказ ФСТЭК от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрирован 26.03.2018 № 50524).

26. Приказ ФСТЭК от 09.08.2018 № 138 «О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31, и в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239" (Зарегистрирован 05.09.2018 № 52071)».

27. Приказ ФСТЭК от 26.03.2019 № 60 "О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239" (Зарегистрирован 18.04.2019 № 54443).

28. Приказ ФСТЭК от 20.02.2020 № 35 "О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239" (Зарегистрирован 11.09.2020 № 59793).

29. Приказ ФСБ России и ФСТЭК России от 31.08.2010 № «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

30. Приказ ФСТЭК от 11.02.2013 № 17 “Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах”.

31. Приказ ФСТЭК от 28.05.2019 № 106 "О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17" (Зарегистрирован 13.09.2019 № 55924).

32. Приказ ФСТЭК от 15.02.2017 № 27 "О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17" (Зарегистрирован 14.03.2017 № 45933).

33. Приказ ФСТЭК от 29.04.2021 № 77 "Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну" (Зарегистрирован 10.08.2021 № 64589).

34. Информационное сообщение ФСТЭК России от 22.06.2017 № 240/22/3031 “О порядке рассмотрения и согласования моделей угроз безопасности информации и технических заданий на создание государственных информационных систем”.

35. Информационное сообщение ФСТЭК России от 4.05.2018 № 240/22/2339 “О методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации”.

36. Информационное сообщение ФСТЭК России от 17.12.2018 № 240/11/5453 “О разработанной ФСТЭК России примерной программе повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры”.

37. Информационное сообщение ФСТЭК России от 17.04.2020 № 240/84/611 “По вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления

сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий”.

38. Информационное сообщение ФСТЭК России от 24.03.2022 № 240/22/1549 “О мерах по повышению защищенности информационной инфраструктуры”.

39. Информационное сообщение ФСТЭК России от 28.06.2022 № 240/83/1698 “О порядке представления субъектами критической информационной инфраструктуры сведений о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий”.

40. Методический документ “Меры защиты информации в государственных информационных системах”, утвержден ФСТЭК России 11 февраля 2014 г.

41. Методический документ “Методика оценки угроз безопасности информации”, утвержден ФСТЭК России 5 февраля 2021 г.

42. Методический документ “Методика тестирования обновлений безопасности программных, программно-аппаратных средств”, утвержден ФСТЭК России 28 октября 2022 г.

43. Методический документ “Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств”, утвержден ФСТЭК России 28 октября 2022 г.

44. Методический документ “Рекомендации по безопасной настройке операционных систем Linux”, утвержден ФСТЭК России 25 декабря 2022 г.

45. Методический документ “Руководство по организации процесса управления уязвимостями в органе (организации)”, утвержден ФСТЭК России 17 мая 2023 г.

46. Приказ ФСБ Российской Федерации от 10.07.2014 № 378 “Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения

установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

47. Приказ ФСБ Российской Федерации от 13.02.2023 № 77 "Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных" (Зарегистрирован 20.02.2023 № 72404).

48. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утверждены руководством 8 Центра ФСБ России (от 31 марта 2015 г. № 149/7/2/6-432).

49. Приказ ФСТЭК от 18.02.2013 № 21 "Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

50. Информационное сообщение ФСТЭК России от 15.06.2013 № 240/22/2637 "По вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»".

51. Информационное сообщение ФСТЭК России от 06.06.2018 № 240/13/2549 "О некоторых вопросах по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

52. Информационное сообщение ФСТЭК России от 31.07.2018 № 240/13/3330 “О необходимости получения лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации в случаях, связанных с обработкой персональных данных”.

Приказы Минцифры, Минэнерго, Минздрава России

1. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 17.03.2020 № 114 "Об утверждении Порядка и Технических условий установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации" (Зарегистрирован 25.06.2020 № 58753).

2. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28.12.2020 № 777 “Об утверждении Рекомендаций по проведению сертификации оборудования связи, используемого в составе сетей связи общего пользования, обеспечивающей функционирование значимых объектов критической информационной инфраструктуры”.

3. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28.12.2020 № 779 “Об утверждении организационно-технических мер по обеспечению информационной безопасности ресурсов сети связи общего пользования, используемых значимыми объектами критической информационной инфраструктуры”.

4. Документ Минэнерго России от 31.07.2019 “Методические рекомендации определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса, согласованные Минэнерго России и ФСТЭК России”.

5. Документ Минздрава России от 5.04.2021 “Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения”.

6. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 18.02.2022 № 132 «Об утверждении Требований к порядку ввода сетей связи в эксплуатацию» (Зарегистрирован 31.05.2022 № 68652).

7. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 12.09.2022 № 659 «Об утверждении требований к линиям связи, пересекающим Государственную границу Российской Федерации, и к средствам связи, к которым подключаются указанные линии связи» (Зарегистрирован 29.11.2022 № 71191).

8. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 8.10.2022 № 766 «О перечне видов деятельности в области информационных технологий».

9. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 31.01.2023 № 62 «Об утверждении классификатора программно-аппаратных комплексов и Правил применения классификатора программно-аппаратных комплексов» (Зарегистрирован 13.04.2023 № 72994).

10. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы Российской Федерации от 29.03.2023 № 321/147 «Об утверждении Типовых требований к плану мероприятий по внедрению собственниками или иными владельцами технологических сетей связи, имеющих уникальный идентификатор совокупности средств связи и иных технических средств в информационнотелекоммуникационной сети "Интернет", технических средств, обеспечивающих выполнение установленных действий при проведении оперативно-разыскных мероприятий» (Зарегистрирован 25.05.2023 № 73467).

11. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 18.01.2023 № 21 «Об утверждении Методических рекомендаций по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры Российской Федерации, и о реализации мер,

направленных на ускоренный переход органов государственной власти и организаций на использование российского программного обеспечения в Российской Федерации».

12. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28.03.2019 № 108 "Об утверждении форм запроса и ответа на запрос на подтверждение соответствия персональных данных фактических пользователей сведениям, заявленным в абонентских договорах оператора связи" (Зарегистрирован 07.06.2019 № 54878).

13. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 21.12.2020 № 734 "Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации" (Зарегистрирова 01.06.2021 № 63735).

14. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 29.09.2021 № 1015 "Об утверждении порядка уничтожения персональных данных, полученных в результате обезличивания, субъектом экспериментального правового режима в сфере цифровых инноваций в случае прекращения статуса субъекта экспериментального правового режима" (Зарегистрирован 29.11.2021 № 66042).

15. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 15.11.2021 № 1187 "Об утверждении перечня индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных" (Зарегистрирован 14.01.2022 № 66870).

16. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 27.04.2023 № 432 "О направлении оператором единой биометрической системы оператору регионального сегмента единой биометрической системы, аккредитованному государственному органу, Центральному банку Российской Федерации в случае прохождения им

аккредитации, организации, осуществляющей аутентификацию на основе биометрических персональных данных физических лиц, запроса о блокировании, об удалении, уничтожении векторов единой биометрической системы и подтверждении осуществления таких блокирования, удаления, уничтожения векторов единой биометрической системы" (Зарегистрирован 29.05.2023 № 73566).

17. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 12.05.2023 № 453 "О порядке обработки биометрических персональных данных и векторов единой биометрической системы в единой биометрической системе и в информационных системах аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации, организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц" (Зарегистрирован 30.05.2023 № 73620).

18. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 31.03.2023 № 334 "Об утверждении методики расчета взимания платы за использование государственной информационной системы "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных", в том числе ее региональных сегментов" (Зарегистрирован 19.05.2023 № 73370).

19. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 17.04.2023 № 378 "Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица соответствующим векторам единой биометрической системы и определении степени взаимного соответствия биометрических персональных данных и векторов единой биометрической системы, достаточной для проведения идентификации и (или) аутентификации" (Зарегистрирован 23.05.2023 № 73396).

20. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 20.04.2023 № 387 "Об утверждении требований к деловой репутации единоличного исполнительного органа, а также

членов коллегиального исполнительного органа и (или) физических лиц - учредителей (участников), имеющих право распоряжаться более 10 процентами акций (долей), составляющих уставный капитал организации, осуществляющей аутентификацию на основе биометрических персональных данных физических лиц, и о признании утратившим силу приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 27 августа 2021 г. № 896" (Зарегистрирован 19.05.2023 № 73366).

21. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 05.05.2023 № 446 "Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в информационных системах организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, за исключением организаций финансового рынка, и единой биометрической системы, а также актуальных при взаимодействии информационных систем государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с указанными информационными системами, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных" (Зарегистрирован 26.05.2023 № 73487).

22. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 05.05.2023 № 445 "Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица в единой биометрической системе, а также актуальных при взаимодействии информационных систем государственных органов, органов местного

самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка, индивидуальных предпринимателей, нотариусов с единой биометрической системой, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных" (Зарегистрирован 26.05.2023 № 73486).

23. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 12.05.2023 № 453 "О порядке обработки биометрических персональных данных и векторов единой биометрической системы в единой биометрической системе и в информационных системах аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации, организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц" (Зарегистрирован 30.05.2023 № 73620).

24. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 31.01.2022 № 71 "О внесении изменений в пункт 1.4 перечня угроз безопасности, актуальных при идентификации заявителя - физического лица в аккредитованном удостоверяющем центре, выдаче квалифицированного сертификата без его личного присутствия с применением информационных технологий путем предоставления сведений из единой системы идентификации и аутентификации и единой информационной системы персональных данных, обеспечивающей обработку, сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации а также хранении и использовании ключа электронной подписи в аккредитованном удостоверяющем центре, утвержденного приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 26 ноября 2020 г. № 624" (Зарегистрирован 14.03.2022 № 67725).

25. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 01.09.2021 № 902 "Об утверждении

перечня угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в информационных системах организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, за исключением единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, а также актуальных при взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей, нотариусов и организаций, за исключением организаций финансового рынка, с указанными информационными системами, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных, и учетом вида аккредитации организации из числа организаций, указанных в частях 18.28 и 18.31 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Зарегистрирован 03.11.2021 № 65692).

26. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 10.09.2021 № 930 "Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации" (Зарегистрирован 28.10.2021 № 65621).

27. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 25.05.2021 № 494 "Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, а также актуальных при взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей, нотариусов и организаций, за исключением организаций финансового рынка, с указанной системой, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных" (Зарегистрирован 15.09.2021 № 65009).

28. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 06.08.2021 № 816 "Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, а также об определении степени взаимного соответствия указанных биометрических персональных данных, достаточной для проведения идентификации, предусмотренной Федеральным законом от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Зарегистрирован 08.09.2021 № 64922).

29. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 29.03.2021 № 187 "Об утверждении Порядка ведения перечня государственных органов, органов местного самоуправления, организаций финансового рынка, иных организаций, индивидуальных предпринимателей, нотариусов, использующих единую

информационную систему персональных данных, обеспечивающую обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица" (Зарегистрирован 06.09.2021 № 64900).

30. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 07.07.2021 № 685 "Об определении форм подтверждения соответствия информационных технологий и технических средств, предназначенных для обработки биометрических персональных данных, требованиям, определенным в соответствии с пунктом 1 части 13 статьи 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Зарегистрирован 03.09.2021 № 64868).

31. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 26.11.2020 № 624 "Об утверждении перечня угроз безопасности, актуальных при идентификации заявителя - физического лица в аккредитованном удостоверяющем центре, выдаче квалифицированного сертификата без его личного присутствия с применением информационных технологий путем предоставления сведений из единой системы идентификации и аутентификации и единой информационной системы персональных данных, обеспечивающей обработку, сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, а также хранении и использовании ключа электронной подписи в аккредитованном удостоверяющем центре" (Зарегистрирован 22.12.2020 № 61689).

32. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 04.07.2019 № 369 "О внесении изменений в приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 25 июня 2018 г. № 321 "Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических

персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации" (Зарегистрирован 25.09.2019 № 56059).

33. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 25.06.2018 № 321 "Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации" (Зарегистрирован 04.07.2018 № 51532).

34. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 25.06.2018 № 323 "Об утверждении форм подтверждения соответствия информационных технологий и технических средств, предназначенных для обработки биометрических персональных данных в целях проведения идентификации, требованиям к информационным технологиям и техническим средствам, предназначенным для указанных целей" (Зарегистрирован 29.06.2018 № 51497).

35. Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 21.06.2018 № 307 "Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, а также об определении степени взаимного соответствия указанных биометрических персональных данных, достаточной для проведения идентификации, предусмотренной Федеральным законом от 27 июля

2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Зарегистрирован 29.06.2018 № 51496).

Приказы Роскомнадзора России

1. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 22.10.2020 № 137 "О внесении изменения в Положение об обработке и защите персональных данных в центральном аппарате Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденное приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 3 декабря 2012 г. № 1255" (Зарегистрирован 24.11.2020 № 61086).

2. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.02.2021 № 18 "Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения" (Зарегистрирован 21.04.2021 № 63204).

3. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 21.06.2021 № 106 "Об утверждении Правил использования информационной системы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, в том числе порядка взаимодействия субъекта персональных данных с оператором" (Зарегистрирован 11.08.2021 № 64602).

4. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14.09.2021 № 183 "О внесении изменений в перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных, утвержденный приказом Федеральной службы по надзору в сфере связи, информационных

технологий и массовых коммуникаций от 15 марта 2013 г. № 274" (Зарегистрирован 21.10.2021 № 65514).

5. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24.12.2021 № 253 "Об утверждении формы проверочного листа (списка контрольных вопросов, ответы на которые свидетельствуют о соблюдении или несоблюдении контролируемым лицом обязательных требований), применяемого при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальными органами» (Зарегистрирован 25.02.2022 № 67486).

6. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.08.2022 № 128 "Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных" (Зарегистрирован 20.09.2022 № 70152).

7. 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" (Зарегистрирован 28.11.2022 № 71166).

8. 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" (Зарегистрирован 28.11.2022 № 71167).

9. 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" (Зарегистрирован 15.12.2022 № 71532).

10. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14.11.2022 № 187 "Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных" (Зарегистрирован 28.12.2022 № 71851).

11. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 21.02.2023 № 22 "Об утверждении Порядка формирования и размещения на официальном сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в информационно-телекоммуникационной сети "Интернет" перечня информационных систем и (или) программ для электронных вычислительных машин, указанных в части 8 статьи 10 Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Зарегистрирован 07.04.2023 № 72921).

12. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 10.01.2023 № 1 "О внесении изменений в форму проверочного листа (списка контрольных вопросов, ответы на которые свидетельствуют о соблюдении или несоблюдении контролируемым лицом обязательных требований), применяемого при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальными органами, утвержденную приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24 декабря 2021 г. № 253" (Зарегистрирован 05.04.2023 № 72886).

13. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.02.2023 № 25 "Об утверждении Критериев оценки материалов и (или) информации, необходимых для принятия Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций решений, являющихся основаниями для

включения доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет", а также сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", в единую автоматизированную информационную систему "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено" (Зарегистрирован 17.04.2023 № 73053).

14. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 02.02.2023 № 13 "Об утверждении порядка проведения мониторинга информационно-телекоммуникационных сетей, в том числе сети "Интернет", а также определении видов информации и (или) информационных ресурсов, в отношении которых проводится мониторинг" (Зарегистрирован 31.03.2023 № 72824).

15. Рекомендации Роскомнадзора по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

16. Методические рекомендации по применению приказа Роскомнадзора от 05.09.2013 № 966 «Об утверждении требований и методов по обезличиванию персональных данных», утверждены руководителем Роскомнадзора 13.12.2013.

17. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 15.03.2013 № 274 "Об утверждении Перечня иностранных государств, не являющихся сторонами конвенции совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных» (Зарегистрирован 19.04.2013 № 28212).

18. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 "Об утверждении Требований и методов по обезличиванию персональных данных".

19. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 22.07.2015 № 84 "Об утверждении Порядка взаимодействия оператора реестра нарушителей прав субъектов персональных данных с провайдером хостинга и Порядка получения доступа к информации, содержащейся в реестре нарушителей прав субъектов персональных данных, оператором связи" (Зарегистрирован 14.08.2015 № 38532).

20. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 22.07.2015 № 85 "Об утверждении формы заявления субъекта персональных данных принятия мер по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных" (Зарегистрирован 17.08.2015 № 38544).

21. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30.05.2017 № 94.

Дополнительные документы

1. Методические рекомендации по организационной защите физическим лицом своих персональных данных (данный документ рекомендуется к ознакомлению в рамках исполнения п. 6. ч. 1 ст. 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»).

Кроме приведенных выше документов в области ИКТ действует несколько десятков государственных стандартов, информацию о которых можно получить на сайте информационной системы «Технорматив» <http://www.technormativ.ru>, <http://www.consultant.ru>. На сайте ФСТЭК (<http://www.fstec.ru>) приведены руководящие документы Гостехкомиссии по вопросам технической защиты информации.

ВОПРОСЫ

1. Государственные органы РФ, контролирующие деятельность в области защиты информации и международные организации в области информационной безопасности.
2. Комитет Государственной думы по безопасности.
3. Совет безопасности России.
4. Федеральная служба по техническому и экспортному контролю (ФСТЭК России).
5. Федеральная служба безопасности Российской Федерации (ФСБ России).
6. Федеральная служба охраны Российской Федерации (ФСО России).
7. Служба внешней разведки Российской Федерации (СВР России).
8. Министерство обороны Российской Федерации (Минобороны России).
9. Министерство внутренних дел Российской Федерации (МВД России).
10. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).
11. Организация объединенных наций.
12. Совет Европы (комитет министров).
13. Европейский комитет по проблемам преступности.
14. Комитет экспертов по преступности в киберпространстве (КЭ-ПК).
15. Международная электротехническая комиссия (МЭК/IEC).
16. Международная организация по стандартизации (ИСО/ISO).
17. Британский институт стандартов (BSI).
18. Американский институт AICPA.
19. Нормы международного права в информационной сфере.
20. Всеобщая декларация прав человека.

21. Международно-правовые проблемы противодействия правонарушениям в сфере компьютерной информации.

22. Стандартизация систем и процессов управления информационной безопасностью.

23. Признаки компьютерных правонарушений по версии Генерального секретариата Интерпола в сфере компьютерной информации.

24. Киберпреступность как вид преступной деятельности в сфере компьютерной информации.

25. Международный опыт уголовно-правового обеспечения информационной безопасности.

26. Обеспечение информационной безопасности в уголовном праве европейских стран.

27. Модельный уголовный кодекс стран – участниц СНГ.

28. Проблемы нормативного обеспечения международной информационной безопасности.

29. Международные и национальные стандарты в информационной сфере.

30. Международные нормы регулирования общественных отношений в информационной сфере как основа международных и национальных стандартов.

31. Опыт применения международных стандартов в информационной сфере. Эволюция международных и национальных стандартов.

32. Международный пакт о гражданских и политических правах.

33. Международные нормы охраны информационной инфраструктуры.

34. Интернет: авторское или пиратское право?

35. Основные нормы гуманитарного права в информационной сфере.

36. Спам и антиспамовое законодательство. Распространение спама.

37. Компьютерное мошенничество.

38. Распространение вирусов.

39. Хакерство.

40. Кодификатор Генерального секретариата Интерпола.
41. Политика работы с конфиденциальной информацией.
42. Политика отправки электронной почты за пределы интранета.
43. Политика хранения сообщений электронной почты.
44. Политика использования паролей.
45. Проблемы уязвимости пользователей WI-Fi соединений.
46. Политика использования алгоритмов шифрования.
47. Политика антивирусной защиты.
48. Политика оценки рисков ИБ
49. Политика аудита ИБ.
50. Политика подключения новых устройств к интранету.
51. Политика удаленного доступа к интранету.
52. Политика подключения подразделений к интранету.
53. Политика для пограничных маршрутизаторов интранета.
54. Политика для экстранета.
55. Политика для пограничной демилитаризованной зоны.
56. Серия стандартов ИСО/МЭК 27000 «Информационные технологии.

Методы обеспечения безопасности».

57. Стандарт ИСО/МЭК 27000:2009. СУИБ: определения и основные принципы.

58. Стандарт ИСО/МЭК 27001:2005. СУИБ: требования.
59. Стандарт ИСО/МЭК 27003:2010. Руководство по внедрению СУИБ.
60. Стандарт ИСО/МЭК 27004:2009. Оценка функционирования СУИБ.
61. Стандарт ИСО/МЭК 27005:2008. Управление рисками ИБ.
62. Стандарт ИСО/МЭК 18044. Управление инцидентами ИБ.
63. Стандарт ИСО/МЭК 27006:2011. Требования к органам, обеспечивающим аудит и сертификацию СУИБ.

64. Стандарты ИСО/МЭК 27007 и ИСО/МЭК 27008. Руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ.

65. Стандарт ИСО/МЭК 27011:2008. Руководство по управлению ИБ для телекоммуникационных компаний на основе ИСО/МЭК 27002.

66. Стандарт ИСО/МЭК 27013. Руководство по интегрированному внедрению стандартов ИСО/МЭК 20000 и ИСО/МЭК 27001.

67. Стандарт ИСО/МЭК 27014. Инфраструктура руководства ИБ.

68. Стандарт ИСО/МЭК 27015. Руководство по управлению ИБ для финансовых сервисов.

69. Стандарт ИСО/МЭК 27031:2011. Руководство по готовности информационных и телекоммуникационных технологий для обеспечения непрерывности бизнеса.

70. Стандарты ИСО/МЭК 15408 и ИСО/МЭК 18045. Общие критерии и методология оценки безопасности информационных технологий.

71. Стандарт ИСО/МЭК 27037. Руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме.

72. Стандарт ИСО/МЭК 13335. Методы и средства обеспечения безопасности для информационных технологий.

73. Стандарт ИСО/МЭК 27033. Управление безопасностью сетей.

74. Стандарт ИСО/МЭК 27035. Управление инцидентами ИБ.

75. Серия стандартов по СУИБ агентства BSI Федеральное агентство по ИБ немецкого правительства.

76. Стандарт BS 7799-3:2006. Руководство по управлению рисками ИБ.

77. Стандарт ИСО 19011:2002. Рекомендации по аудиту систем менеджмента качества и/или окружающей среды.

78. Стандарт BS 25999. Управление непрерывностью бизнеса.

ВЫВОДЫ

Многие исследователи к числу важнейших факторов относят недостаточную нормативно-правовую базу в области регулирования информационных отношений и обеспечения информационной безопасности. В последние годы законодательная база России в области регулирования информационной безопасности существенно изменена. Принят ряд новых законодательных актов, изменены и даже отменены некоторые ранее принятые.

Анализ изменений нормативно-правовой базы в области ИБ дает основание утверждать, что Россия уверенно движется по пути построения и развития гражданского общества. Наряду с совершенствованием государственной правовой базы Россия подписала ряд международных концептуальных документов и конвенций в области охраны интеллектуальной собственности и защиты интересов личности в информационном обществе. Одновременно совершенствуется государственная организационная система управления процессами информатизации и правоприменительная практика при раскрытии компьютерных преступлений. Укрепляется международное сотрудничество по борьбе с компьютерным пиратством в глобальных телекоммуникационных системах.

В настоящее время все учреждения должны создавать свою нормативную базу в сфере обеспечения информационной безопасности.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Домарев В.В. Безопасность информационных технологий. Системный подход – К.: ООО ТИД Диа Софт, 2004. – 992 с.
2. Лапина М.А., Ревин А.Г., Лапин В.И. Информационное право. М.: ЮНИТИ-ДАНА, Закон и право, 2004.
3. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник. / Под ред. акад. РАН Б.Н. Топорнина. СПб.: Изд-во "Юридический центр Пресс", 2001.
4. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов. М.: Горячая линия – Телеком, 2006. – 544 с.: ил.
5. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. – М.: Горячая линия – Телеком, 2005. – 416 с.:ил.
6. Галатенко В.А. Стандарты информационной безопасности: курс лекций. Учебное пособие /Второе издание / М.: ИНТУИТ.РУ «Интернет-университет информационных технологий», 2006.- 264 с.
7. Галатенко В.А. Основы информационной безопасности. Под ред. В.Б. Бетелина М.: ИНТУИТ.РУ «Интернет-университет информационных технологий», 2006.- 208 с.
8. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений. М.: ДМК Пресс, 2004. – 616 с.
9. Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. Автореферат диссертации на соискание ученой степени кандидата юридических наук. 2007, г. Москва
10. Курило А.П., и др. Обеспечение информационной безопасности бизнеса. М.: БДЦ – пресс, 2005. – 512 с.
11. Котухов М.М. Основные положения и нормативно-правовое обеспечение информационной безопасности автоматизированных систем. Учебное пособие. – М.: издание ИПКИР, 2006, - 67 с.

12. Крылов Г.О. Международный опыт правового регулирования информационной безопасности и его применение в Российской Федерации. Автореферат диссертации на соискание ученой степени кандидата юридических наук. 2007, г. Москва.
13. Малюк А.А. Информационная безопасность: концептуальные и методические основы защиты информации. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2004. – 280 с.: ил.
14. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. Учебное пособие для вузов. – 2-е изд. – М.: Горячая линия – Телеком, 2004. – 147 с.: ил.
15. Минков А.М. Международная охрана интеллектуальной собственности. – СПб: Питер, 2001. – 720 с.: ил.
16. Ожиганова М.И., Мордвинова А.Ю. Международные и российские нормативные акты и стандарты по информационной безопасности: учебно-методическое пособие / Сост. М.И. Ожиганова,. – Севастополь: СевГУ, 2019. – 112 с.
17. Родичев А.Ю., Родичев Ю.А. Системная модель защиты информации информационных систем распределенного типа. Вестник Самарского гос. ун-та. 2003., № 2, с.15-20
18. Родичев Ю.А. Компьютерные сети. Нормативно-правовые аспекты информационной безопасности. Часть 1. Учеб. пособие для вузов. – Самара : изд-во «Универс-групп», 2007. – 344 с.
19. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты. «Питер», 2008. - 272 с.
20. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.
21. Титоренко Г.А. Методы и средства построения систем информационной безопасности. Их структура. 2-е издание, дополненное. – М., 2003. – 205 с.

22. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, организационные и технические аспекты: Учебное пособие. – М.: Гелиос АРВ, 2006. – 528 с., ил.

23. Шамраев А.В. Правовое регулирование информационных технологий (анализ проблем и основные документы). Версия 1.0. М.: «Статут», «Интертех», «БЦД-пресс», 2003. – 1013 с.

24. A Guide to Developing Computing Policy Documents (SAGE Short Topics in System Administration). Edited by Barbara L. Dijker. 1996.

25. BS 7799-3:2006 «Information security management systems. Guidelines for information security risk management».

26. BS 25777:2008 «Information and communications technology continuity management. Code of practice».

27. BS 25999-1:2006 «Business continuity management. Code of practice».

28. BS 25999-2:2007 «Business continuity management. Specification».

29. Business Conyinuity Management, BSI Standard 100-4, Version 1.0, November 2008, <http://www.bsi.bund.de>.

30. Department of Defense Trusted Compute System Evaluation Criteria, DoD 5200.28STD, 1985.

31. Guttman, B.; Roback, E. An Introduction to Computer Security: The NIST Handbook. NIST Special Publication 800-12. 1995.

32. Information Security Management Systems (ISMS), BSI Standard 100-1, Version 1.5, Mai 2008, <http://www.bsi.bund.de>.

33. ISO/IEC 9001:2008 «Quality management systems. Requirements».

34. ISO/IEC 13335-1:2004 «Information technology. Security techniques. Management of information and communications technology security...».

35. ISO/IEC 13335-3:1998 «Information technology. Security techniques. Management of information and communications technology security...».

36. ISO/IEC 13335-4:2000 «Information technology. Security techniques. Management of information and communications technology security...».

37. ISO/IEC 13335-5:2001 «Information technology. Security techniques. Management of information and communications technology security...».
38. ISO/IEC 15408-1:2009 «The Common Criteria for Information Technology Security Evaluation. 1: Introduction and general model».
39. ISO/IEC 15408-2:2008 «The Common Criteria for Information Technology Security Evaluation. Security functional components».
40. ISO/IEC 15408-3:2008 «The Common Criteria for Information Technology Security Evaluation. Security assurance components».
41. ISO/IEC 19011:2002 «Guidelines for quality and/or environmental management systems auditing».
42. ISO/IEC 20000-1:2005 «Information technology service management. Specification for Service Management».
43. ISO/IEC 20000-2:2005 «Information technology service management. Code of Practice for Service Management».
44. ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements».
45. ISO/IEC 27002:2005 «Information technology. Security techniques. Code of practice for information security management».
46. ISO/IEC 27003:2010 «Information Technology. Security Techniques. Information Security Management Systems Implementation Guidance».
47. ISO/IEC 27004:2009 «Information technology. Security techniques. Information security management. Measurement».
48. ISO/IEC 27005:2008 «Information technology. Security techniques. Information security risk management».
49. ISO/IEC 27006:2011 «Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems».
50. ISO/IEC 27007 «Information technology. Security techniques. Guidelines for Information Security Management Systems auditing (FCD)».

51. ISO/IEC 27008 «Information technology. Security techniques. Guidance for auditors on ISMS controls».

52. ISO/IEC 27011:2008 «Information technology. Security techniques. Information security management guidelines for telecommunications organizations based on ISO/IEC 27002».

53. ISO/IEC 27013 «Information technology. Security techniques. Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001».

54. ISO/IEC 27014 «Information technology. Security techniques. Information security governance framework».

55. ISO/IEC 27031:2011 «Information technology. Security techniques. Guidelines for information and communications technology readiness for business continuity».

56. ISO/IEC 27033-1:2009 «Information technology. Security techniques. Network security....».

57. ISO/IEC 27033-3:2010 «Information technology. Security techniques. Network security....».

58. ISO/IEC TR 18044:2004 «Information technology. Security techniques. Information security incident management».

59. IT-Grundschutz Methodology, BSI Standard 100-2, Version 2.0, Mai 2008, <http://www.bsi.bund.de>

60. ITU-T Recommendation X.509 «Information Technology. Open Systems Interconnection. The Directory: Public Key and Attribute Certificate Frameworks». June 2000.

61. ITU-T Recommendation X.1051 «Information security management system. Requirements for telecommunications (ISMS-T)».

62. Mui L., Mohtashemi M., Halberstadt A. A computational model of trust and reputation // System Sciences. 2002. P. 2431-2439.

63. PAS 77:2006 «IT Service Continuity Management. Code of practice».

64. Risk Analysis on the Basis of IT-Grundschutz, BSI Standard 100-3, Version 2.5, Mai 2008, <http://www.bsi.bund.de>

65. Tipton H.F., Krause M. Information Security Management Handbook. 6th edition. Taylor & Francis Group, USA, 2007. – 3231 p.

66. «Underlying Technical Models for Information Technology Security» (NIST Special Publication 800-33). U.S. Government Printing Office. Washington, 2001.

Интернет-ресурсы

1. <http://www.fstec.ru> – сервер ФСТЭК
2. <http://www.itsec.ru/> – информационная безопасность
3. <http://microsoft.com/rus/security/> – сервер корпорации Microsoft
4. <http://www.citforum.ru/internet/infsecure/> – сайт по ИТ-технологиям
5. <http://www.infosec.ru/> – компания «Информзащита»
6. <http://www.iis.ru> – сайт института развития информационного общества
7. <http://www.gov.ru/> – сервер органов государственной власти Российской Федерации
8. <http://www.fsb.ru/> – сайт ФСБ
9. <http://www.svr.gov.ru/> – сайт службы внешней разведки
10. <http://www.fso.gov.ru/> – сайт федеральной службы охраны
11. <http://www.minsvyaz.ru/ministry/> – сайт министерства информационных технологий и связи
12. <http://www.minsvyaz.ru/departments/rosinformtehnologii/news/> – сайт
13. федерального агентства по информационным технологиям
14. <http://www.scrf.gov.ru/> – сайт Совета Безопасности
15. <http://www.securitylab.ru> – информационный портал в области защиты информации
16. <http://www.elspa.ru> – Ассоциация по борьбе с компьютерным пиратством
17. <http://www.bsa.org> – BSA (международная ассоциация производителей программного обеспечения)
18. <http://www.cyberpol.ru/> – Cyberpol.ru — компьютерная преступность и борьба с нею

Приложение 1

Основные виды конфиденциальной информации принятые в законодательстве Российской Федерации <i>Виды информации с ограниченным доступом</i>	Правовая регламентация защиты
I. Сведения, составляющие государственную тайну	
Государственная тайна.	Закон РФ "О государственной тайне". Закон РФ "Об информации, информации – онных технологиях и защите информа – ции". Уголовный кодекс РФ.
II. Сведения конфиденциального характера	
Сведения о фактах, событиях и обстоя – тельствах частной жизни граж – данина, позволяющие идентифици – ровать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации (СМИ) в установленных федераль – ными законами случаях.	Закон РФ "Об информации, информации – онных технологиях и защите информа – ции". Закон РФ "О персональных данных". Уголовный кодекс РФ. Трудовой кодекс РФ. Гражданский кодекс РФ. Семейный кодекс РФ. Кодекс РФ об административных право – нарушениях.
Сведения, составляющие тайну следствия и судопроизводства.	Уголовно – процессуальный Кодекс РФ. Уголовный кодекс РФ. Кодекс РФ об административных право – нарушениях.
Служебные сведения, доступ к ко – торым ограничен органами государ – ственной власти в соответствии с Гражданским кодексом РФ и феде – ральными законами (служебная тайна).	Закон РФ "О государственной граждан – ской службе в РФ". Уголовный кодекс РФ. Гражданский кодекс РФ. Трудовой кодекс РФ. "Перечень сведений конфиденциального характера." "Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти".
III. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами	
Банковская тайна.	Закон РСФСР "О банках и банковской деятельности". Уголовный кодекс РФ. Гражданский кодекс РФ.

ГОСУДАРСТВЕННЫЕ СТАНДАРТЫ РФ В СФЕРЕ ИБ

	Обозначение	Наименование на русском языке
1.	ГОСТ Р 50739-95	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования
2.	ГОСТ Р 50922-2006	Защита информации. Основные термины и определения
3.	ГОСТ Р 51188-98	Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство
4.	ГОСТ Р 51275-2006	Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения
5.	ГОСТ Р 51583-2014	Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения
6.	ГОСТ Р 52069.0-2013	Защита информации. Система стандартов. Основные положения
7.	ГОСТ Р 52447-2005	Защита информации. Техника защиты информации. Номенклатура показателей качества
8.	ГОСТ Р 52448-2005	Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения
9.	ГОСТ Р 52633.0-2006	Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации
10.	ГОСТ Р 52633.1-2009	Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
11.	ГОСТ Р 52633.2-2010	Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
12.	ГОСТ Р 52633.3-2011	Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора

	Обозначение	Наименование на русском языке
13	ГОСТ Р 52633.4-2011	Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия - код доступа
14	ГОСТ Р 52633.5-2011	Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа
15	ГОСТ Р 52633.6-2012	Защита информации. Техника защиты информации. Требования к индикации близости предъявленных биометрических данных образу «Свой»
16	ГОСТ Р 52863-2007	Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования
17	ГОСТ Р 53109-2008	Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности
18	ГОСТ Р 53110-2008	Система обеспечения информационной безопасности сети связи общего пользования. Общие положения
19	ГОСТ Р 53111-2008	Устойчивость функционирования сети связи общего пользования. Требования и методы проверки
20	ГОСТ Р 53112-2008	Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний
21	ГОСТ Р 53113.1-2008	Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения
22	ГОСТ Р 53113.2-2009	Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов

	Обозначение	Наименование на русском языке
23	ГОСТ Р 53114-2008	Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения
24	ГОСТ Р 53115-2008	Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства
25	ГОСТ Р 53131-2008	Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения
26	ГОСТ Р 54581-2011 / ISO/IEC TR 15443-1:2005	Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы
27	ГОСТ Р 54582-2011 / ISO/IEC TR 15443-2:2005	Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия
28	ГОСТ Р 54583-2011 / ISO/IEC TR 15443-3:2007	Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия
29	ГОСТ Р 56045-2014	Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью
30	ГОСТ Р 56093-2014	Защита информации. Автоматизированные системы в защищенном исполнении. Средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования
31	ГОСТ Р 56103-2014	Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения
32	ГОСТ Р 56115-2014	Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования

	Обозначение	Наименование на русском языке
33	ГОСТ Р ИСО/МЭК 13335-1-2006	Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
34	ГОСТ Р ИСО 7498-1-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель
35	ГОСТ Р ИСО 7498-2-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации
36	ГОСТ Р ИСО/МЭК ТО 13335-5-2006	Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
37	ГОСТ Р ИСО/МЭК 15408-1-2012	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
38	ГОСТ Р ИСО/МЭК 15408-2-2013	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности
39	ГОСТ Р ИСО/МЭК 15408-3-2013	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности
40	ГОСТ Р ИСО/МЭК ТО 15446-2008	Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности
41	ГОСТ Р ИСО/МЭК ТО 18044-2007	Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности
42	ГОСТ Р ИСО/МЭК 18045-2013	Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий
43	ГОСТ Р ИСО/МЭК ТО 19791-2008	Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем
44	ГОСТ Р ИСО/МЭК 21827-2010	Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса

	Обозначение	Наименование на русском языке
45	ГОСТ Р ИСО/МЭК 27000-2012	Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
46	ГОСТ Р ИСО/МЭК 27001-2006	Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
47	ГОСТ Р ИСО/МЭК 27002-2012	Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента безопасности
48	ГОСТ Р ИСО/МЭК 27003-2012	Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности
49	ГОСТ Р ИСО/МЭК 27004-2011	Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения
50	ГОСТ Р ИСО/МЭК 27005-2010	Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности
51	ГОСТ Р ИСО/МЭК 27006-2008	Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности
52	ГОСТ Р ИСО/МЭК 27007-2014	Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности
53	ГОСТ Р ИСО/МЭК 27013-2014	Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1
54	ГОСТ Р ИСО/МЭК 27033-1-2011	Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции
55	ГОСТ Р ИСО/МЭК 27033-3-2014	Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления

	Обозначение	Наименование на русском языке
56	ГОСТ Р ИСО/МЭК 27034-1-2014	Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия
57	ГОСТ Р ИСО/МЭК 27037-2014	Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме
58	ГОСТ Р ИСО/МЭК 29100-2013	Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности
59	Рекомендации по стандартизации Р 50.1.050-2004	Защита информации. Система обеспечения качества техники защиты информации. Общие положения
60	Рекомендации по стандартизации Р 50.1.053-2005	Информационные технологии. Основные термины и определения в области технической защиты информации
61	Рекомендации по стандартизации Р 50.1.056-2005	Техническая защита информации. Основные термины и определения

ПЕРЕЧЕНЬ ОСНОВНЫХ ДЕЙСТВУЮЩИХ ДОКУМЕНТОВ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

№ п/п	Документы	Реквизиты
Основные нормативные правовые документы		
Законы Российской Федерации (федеральные законы)		
1.	Конституция Российской Федерации	Конституция Российской Федерации от 12 декабря 1993 г.
2.	"О безопасности"	Закон Российской Федерации от 5.03.1992 года №2446-1
3.	"О государственной тайне"	Закон Российской Федерации от 21.07.1993 г. № 5485-1
4.	"Об информации, информационных технологиях и о защите информации"	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ
5.	"О персональных данных"	Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ
6.	"О лицензировании отдельных видов деятельности"	Федеральный Закон Российской Федерации от 8.08.2001 г. №128-ФЗ
7.	Кодекс Российской Федерации об административных правонарушениях	Кодекс Российской Федерации от 30.12.2001 г. № 195-ФЗ (выписка в части вопросов защиты информации)
8.	Уголовный кодекс Российской Федерации	Кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (выписка в части вопросов защиты информации)
9.	"Об электронной цифровой подписи"	Федеральный Закон Российской Федерации от 10.01.2002 г. №1-ФЗ
10.	"О техническом регулировании"	Федеральный Закон Российской Федерации от 27.12.2002 г. № 184-ФЗ
Указы и распоряжения Президента Российской Федерации		
11.	О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена	Указ Президента Российской Федерации 17 марта 2008 года № 351
12.	Об утверждении Перечня должностных лиц органов государственной власти Российской Федерации, наделенных полномочиями по отнесению сведений к государственной тайне	Распоряжение Президента Российской Федерации от 17.01.2000 г. № 6-рп ч.
13.	Об утверждении Перечня сведений конфиденциального характера	от 6.03.1997 г. №188
14.	Об утверждении Перечня сведений, отнесенных к государственной тайне	Указ Президента Российской Федерации от 30.11.1995 Г. № 1203
15.	О мерах по упорядочению разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы, а также использования специальных технических средств, предназначенных для негласного получения информации	Указ Президента Российской Федерации от 9.01.1996 г. №21
16.	Вопросы Федеральной службы по техническому и экспортному контролю	Указ Президента Российской Федерации от 16.08.2004 г. № 1085
17.	Вопросы Межведомственной комиссии по защите государственной тайны	Указ Президента Российской Федерации от 6.10.2004 г. № 1286

№ п/п	Документы	Реквизиты
18.	О некоторых мерах государственного регулирования размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров Российской Федерации и иных программ и проектов на территории Российской Федерации, на континентальном шельфе и в исключительной	Указ Президента Российской Федерации от 23.04.2001 г. №458
19.	Об утверждении Концепции национальной безопасности Российской Федерации	Указ Президента Российской Федерации от 17.12.1997 г. № 1300
Постановления Правительства Российской Федерации		
20.	О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны	Постановление Правительства Российской Федерации от 18.09.2006 г. № 573
21.	О лицензировании отдельных видов деятельности	Постановление Правительства Российской Федерации от 11.02.2002 г. № 135
22.	Об утверждении Положения об участии российских организаций в проведении выставок и показов продукции	Постановление правительства Российской Федерации от 13.12.99 г. № 1384
23.	О порядке согласования вопросов размещения дипломатических представительств и консульских учреждений в Российской Федерации, а также международных организаций и их представительств, аккредитованных при Министерстве иностранных дел Российской Федерации	Постановление Правительства Российской Федерации от 6.03.96 г. №233-18
24.	Об утверждении перечня территорий Российской Федерации с регламентированным посещением иностранных граждан	Постановление Правительства Российской Федерации от 4.07.92 г. № 470
25.	О порядке приема и передвижения иностранных граждан в Российской Федерации	Постановление Правительства Российской Федерации от 14.10.1992 г. № 790
26.	Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации о государственной тайне	Постановление Правительство Российской Федерации от 28.10.1995 г. № 1050
27.	Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности	Постановление Правительства Российской Федерации от 4.09.1995 г. № 870
28.	Об утверждении Положения о подготовке к передаче сведений, составляющих государственную тайну, другим государствам	Постановление Правительства Российской Федерации от 2.08.1997 г. № 973
29.	Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне	Постановление Правительства Российской Федерации от 22.08.1998 г. № 1003
30.	О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны	Постановление Правительства Российской Федерации от 15.04.1995 г. № 333
31.	Об утверждении Положения о лицензировании образовательной деятельности	Постановление Правительства Российской Федерации от 18.10.2000 г. № 796
32.	Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации	Постановление Правительства Российской Федерации от 30.04.2002 г. № 290
33.	Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации	Постановление Правительства Российской Федерации от 27.05.2002 г. № 348
34.	Об утверждении Положения о лицензировании деятельности по международному информационному обмену	Постановление Правительства Российской Федерации от 3.06.1998 г. № 564

№ п/п	Документы	Реквизиты
35.	Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами	Постановление Правительства Российской Федерации от 23.09.2002 г. № 691
36.	О порядке размещения и использования на территории Российской Федерации, на континентальном шельфе и в исключительной экономической зоне Российской Федерации иностранных технических средств наблюдения и	Постановление Правительства Российской Федерации от 29.08.2001 г. № 633
37.	Об утверждении Положения о сертификации средств защиты информации	Постановление Правительства Российской Федерации от 26.06.1995 г. № 608
Основные организационно-распорядительные документы		
Положения		
38.	Положение о государственной системе защиты информации в Российской Федерации от иностранной технической разведки и от ее утечки по техническим каналам	Утверждено Постановлением Совета Министров Правительства Российской Федерации от 15.09.93 г. №912-51
39.	Положение о Федеральной службе по техническому и экспортному контролю	Утверждено Указом Президента Российской Федерации от 16.08.2004 г. №
40.	Положение о Межведомственной комиссии по защите государственной тайны	Утверждено Указом Президента Российской Федерации от 6.10.2004 г. № 1286
41.	Положение о порядке предоставления организациям Российской Федерации права на осуществление внешнеторговой деятельности в отношении продукции военного назначения	Утверждено Указом Президента Российской Федерации от 1.12.2000 г. № 1953
42.	Положения об управлениях Федеральной службы по техническому и экспортному контролю по федеральным округам	Утверждены приказом ФСТЭК России от 18.10.2004 г. №3
43.	Положение о формировании, использовании и защите государственных информационных ресурсов Российской Федерации	Одобрено решением Государственной комиссии по информатизации от 21.04.1998 г. № 18
44.	Положение об участии российских организаций в проведении выставок и показов продукции военного назначения	Утверждено постановлением Правительства Российской Федерации от 13.12.1999 г. № 1384
45.	Положение о подготовке к передаче сведений, составляющих государственную тайну, другим государствам	Утверждено постановлением Правительства Российской Федерации от 2.08.1997 г. № 973
46.	Положение о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц, из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне	Утверждено постановлением Правительства Российской Федерации от 22.08.1998 г. № 1003
47.	Положение о порядке согласования совместной с иностранными фирмами деятельности предприятий связи, направленной на обеспечение живучести и устойчивости магистральных сетей электрической и почтовой связи	Утверждено постановлением Правительства Российской Федерации от 7.03.1995 г. № 220-8
48.	Типовое положение о Совете (Технической комиссии) министерства, ведомства, органа государственной власти субъекта Российской Федерации по защите информации от иностранных технических разведок и от ее утечки по техническим каналам	Решение Гостехкомиссии России от 14.03.1995 г. №32
49.	Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в министерствах и ведомствах, в органах государственной власти субъектов Российской Федерации	Решение Гостехкомиссии России от 14.03.1995 г. №32

№ п/п	Документы	Реквизиты
50.	Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам на предприятии (в учреждении, организации)	Решение Гостехкомиссии России от 14.03.1995 г. №32
51.	Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны	Утверждено постановлением Правительства Российской Федерации от 15.04.1995 г. №333
52.	Положение о государственном лицензировании деятельности в области защиты информации	Решение Гостехкомиссии России и ФАПСИ от 27.04.1994 г. № 10
53.	Положение о лицензировании образовательной деятельности	Утверждено постановлением Правительства Российской Федерации от
54.	Положение о лицензировании деятельности по технической защите конфиденциальной информации	Утверждено постановлением Правительства Российской Федерации от
55.	Положение о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации	Утверждено постановлением Правительства Российской Федерации от 27 мая 2002 г. №348
56.	Положение о лицензировании деятельности по международному информационному обмену	Утверждено постановлением Правительства Российской Федерации от 3.06.1998 г. № 564
57.	Положение о лицензировании деятельности по распространению шифровальных (криптографических) средств	Утверждено постановлением Правительства Российской Федерации от 23.09.2002 г. № 691
58.	Положение о лицензировании деятельности по техническому обслуживанию шифровальных (криптографических) средств	Утверждено постановлением Правительства Российской Федерации от 23.09.2002 г. № 691
59.	Положение о лицензировании предоставления услуг в области шифрования информации	Утверждено постановлением Правительства Российской Федерации от 23.09.2002 г. № 691
60.	Положение о лицензировании разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем	Утверждено постановлением Правительства Российской Федерации от 23.09.2002 г. № 691
61.	Положение о сертификации средств защиты информации	Утверждено постановлением Правительства Российской Федерации от
62.	Положение о системе сертификации средств защиты информации по требованиям безопасности информации (система сертификации Гостехкомиссии России)	Утверждено приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 15.08.2000 г. №328
63.	Положение о размещении и использовании на территории Российской Федерации, на континентальном шельфе и в исключительной экономической зоне Российской Федерации иностранных технических средств наблюдения и контроля	Утверждено постановлением Правительства Российской Федерации от 29.08.2001 г. № 633
64.	Положение о сертификации средств защиты информации по требованиям безопасности информации	Утверждено Приказом председателя Гостехкомиссии России от 27.10.1995 г. №
65.	Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации	Утверждено Приказом председателя Гостехкомиссии России от 5.01.1996 г. № 3
66.	Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации	Утверждено решением председателя Гостехкомиссии России от 25.11.1994 г.
67.	Положение по аттестации объектов информатизации по требованиям безопасности информации	Утверждено Приказом председателя Гостехкомиссии России от 5.01.1996 г. №

№ п/п	Документы	Реквизиты
68.	Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации	Утверждено Приказом председателя Гостехкомиссии России от 5.01.1996 г. № 3
69.	Типовое положение об испытательной лаборатории	Утверждено Приказом председателя Гостехкомиссии России от 5.01.1996 г. №
70.	Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти	Утверждено постановлением Правительства Российской Федерации от 3.11.1994 г. № 1233
Руководства, инструкции и др.		
71.	Типовые требования к содержанию и порядку разработки руководств по защите информации на объектах	Утверждены Решением Гостехкомиссии России от 3.10.1995 г. № 42
72.	Инструкция о порядке допуска должностных лиц и граждан к сведениям, составляющим государственную тайну)	Утверждена постановлением Правительства Российской Федерации от 28.10.1995 г. № 1050
73.	Инструкция о порядке проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну	Утверждена Директором ФСБ России 23.08.1995 г. №28. Согласована с Гостехко-миссией России 5.07.1995 г. и ФАПСИ 31.07.1995 г.
74.	Инструкция о порядке проведения государственной аттестации руководителей предприятий, учреждений и организаций, ответственных за защиту сведений, составляющих государственную тайну	Утверждена председателем Гостехкомиссии России 17.10.1995 г.
75.	Инструкция о порядке проведения специальных экспертиз предприятий, учреждений и организаций на право осуществления мероприятий и (или) оказания услуг в области противодействия иностранной технической	Утверждена председателем Гостехкомиссии России 17.10.1995 г.
76.	Инструкция о порядке проведения экспертиз предприятий и организаций на право получения лицензии в области защиты информации	Утверждена председателем Гостехкомиссии России 16.02.1998 г.
77.	Методические рекомендации по организации и проведению государственной аттестации руководителей предприятий, учреждений и организаций, ответственных за защиту сведений, составляющих государственную тайну	Решение Межведомственной комиссии по защите государственной тайны от 13.03.1996 г. №3
78.	Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности	Утверждены постановлением Правительства Российской Федерации от 4.09.1995 г. № 870
79.	Перечень учебных заведений, осуществляющих подготовку специалистов по защите информации, составляющей государственную тайну, свидетельство об окончании которых дает руководителям предприятий, учреждений и организаций право на освобождение от государственной	Решение Межведомственной комиссии по защите государственной тайны от 12.09.2000 г. № 63
80.	Перечень территорий Российской Федерации с регламентированным посещением для иностранных граждан	Утвержден постановлением Правительства Российской Федерации от 4.07.1992 г. № 470
81.	Перечень должностных лиц органов государственной власти Российской Федерации, наделенных полномочиями по отнесению сведений к государственной тайне	Утвержден распоряжением Президента Российской Федерации от 17.01.2000 г. № 6-рп
82.	Перечень сведений конфиденциального характера	Утвержден Указом Президента Российской Федерации от 6.03.1997 г. №
83.	Перечень сведений, отнесенных к государственной тайне	Утвержден Указом Президента Российской Федерации от 30.11.1995 г. №
84.	Структура Межведомственной комиссии по защите государственной тайны	Утверждена Указом Президента Российской Федерации от 6.10.2004 г. №

№ п/п	Документы	Реквизиты
85.	Состав Межведомственной комиссии по защите государственной тайны по должностям	Утвержден Указом Президента Российской Федерации от 6.10.2004 г. №
Концепции		
86.	Доктрина информационной безопасности Российской Федерации	Утверждена Президентом Российской Федерации 9.09.2000 г. № Пр-1895
87.	Концепция национальной безопасности Российской Федерации	Утверждена Указом Президента Российской Федерации от 17.12.1997 г. №
88.	Концепция защиты государственной тайны в Российской Федерации	Решение Межведомственной комиссии по защите государственной тайны от 24.03.1998 г. №33
89.	Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации	Решение председателя Гостехкомиссии России от 30.03.1992 г.
Нормативные документы		
Нормативные документы национальной системы стандартизации		
90.	ГОСТ Р 52069-2003. Защита информации. Система стандартов. Общие положения	Госстандарт России
91.	ГОСТ 28147-89. Защита информации от утечки за счет побочных электромагнитных излучений и наводок. Общие технические требования	Госстандарт России
92.	ГОСТ 29339-92. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений и наводок при ее обработке средствами вычислительной техники. Общие технические требования	Госстандарт России
93.	ГОСТ 50752-95. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений и наводок при ее обработке средствами вычислительной техники. Методы испытаний	Госстандарт России
94.	ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая	Госстандарт России
95.	ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные	Госстандарт России
96.	ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия	Госстандарт России
97.	ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования	Госстандарт России
98.	ГОСТ Р 50922-96 ЗИ. Основные термины и определения	Госстандарт России
99.	ГОСТ Р 50972-96 ЗИ. Радиомикрофон. Технические требования к защите от утечки секретной информации	Госстандарт России
100.	ГОСТ Р 50.1.050-2004 ЗИ. Система обеспечения качества техники защиты информации. Общие положения	Госстандарт России
101.	ГОСТ Р 50.1.56-2005 ТЗИ. Термины и определения	Госстандарт России
102.	ГОСТ Р 52447-2005 ЗИ. Техника защиты информации. Номенклатура показателей качества	Госстандарт России
103.	ГОСТ Р 52448-2005 ЗИ. Обеспечение безопасности информации сетей электросвязи. Общие положения	Госстандарт России
104.	РД 50-715-92. Методические указания. Информационная технология. Защита информации от утечки за счет ПЭМИН при ее обработке средствами вычислительной техники. Порядок организации работ при разработке и изготовлении	Госстандарт России

№ п/п	Документы	Реквизиты
105.	РД 50-716-92. Методические указания. Информационная технология. Защита информации от утечки за счет ПЭМИН при ее обработке средствами вычислительной техники. Правила разработки, построения, изложения, оформления	Госстандарт России
106.	ГОСТ Р 51241-98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний	Госстандарт России
107.	ГОСТ 34.936-91. Информационная технология. Локальные вычислительные сети. Определение услуг уровня управления доступом	Госстандарт России
108.	ГОСТ Р ИСО/МЭК 17779-2005. Информационная технология. Практические правила управления информационной безопасностью	Госстандарт России
109.	ГОСТ (образовательный) Специальность 090102 (075200) «Компьютерная безопасность»	Госстандарт России
110.	ГОСТ (образовательный) Специальность 090103 (075300) «Организация и технология защиты»	Госстандарт России
111.	ГОСТ (образовательный) Специальность 090104 (075400) «Комплексная защита объектов информатизации»	Госстандарт России
112.	ГОСТ (образовательный) Специальность 090105 (075500) «Комплексное обеспечение информационной безопасности автоматизированных систем»	Госстандарт России
113.	ГОСТ (образовательный) Специальность 090106 (075600) «Информационная безопасность телекоммуникационных	Госстандарт России
114.	ГОСТ (образовательный) Специальность 090107 (075700) «Противодействие техническим разведкам»	Госстандарт России
115.	ГОСТ Р 50543-93. Конструкции базовые несущие средств вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования	Госстандарт России
116.	ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов.	Госстандарт России
117.	ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию.	Госстандарт России
118.	ГОСТ Р 51583-00. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения	Госстандарт России
119.	ГОСТ Р 51624-00. Защита информации. Автоматизированные системы в защищенном исполнении. Общие	Госстандарт России
Специальные нормативно-технические документы ФСТЭК России		
120.	СТР Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам	Решение Гостехкомиссии России от 23.05.1997 г. №55
121.	СТР-К. Специальные требования и рекомендации по технической защите конфиденциальной информации	Утверждены приказом Гостехкомиссии России от 30.08.2002 г. № 282
122.	Методика сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров	Гостехкомиссия России, 2000 г.
123.	Временные методики сертификационных и аттестационных испытаний сетевых помехоподавляющих фильтров по требованиям безопасности информации	Гостехкомиссия России, 2000 г.
124.	Временный порядок аттестации объектов информатизации по требованиям безопасности информации	Приказ председателя Гостехкомиссии России от 21.06.2002 г. №201
125.	Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения	Решение председателя Гостехкомиссии России от 30.03.1992 г.

№ п/п	Документы	Реквизиты
126.	Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации	Решение председателя Гостехкомиссии России от 30.03.1992 г.
127.	Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации	Решение председателя Гостехкомиссии России от 30.03.1992 г.
128.	Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники	Решение председателя Гостехкомиссии России от 30.03.1992 г.
129.	Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации	Решение председателя Гостехкомиссии России от 25.07.1997 г.
130.	Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования	Решение председателя Гостехкомиссии России от 25.07.1997 г.
131.	Руководящий документ. Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации	Решение председателя Гостехкомиссии России и Госстандарта России 01.04.1996 г.
132.	Руководящий документ Гостехкомиссии России. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей	Решение председателя Гостехкомиссии России от 4.06.1999 г. № 114
133.	Руководящий документ. Защита информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам	Гостехкомиссия России, 2000 г.
Информационные документы		
134.	Перечень лицензионных центров Гостехкомиссии (ФСТЭК) России	Периодически обновляется
135.	Перечень органов по сертификации средств защиты информации по требованиям безопасности информации	Периодически обновляется
136.	Перечень органов по аттестации объектов информатизации по требованиям безопасности информации	Периодически обновляется
137.	Перечень организаций, получивших лицензии Гостехкомиссии (ФСТЭК) России на деятельность в области	Периодически обновляется
138.	Перечень организаций, получивших лицензии Гостехкомиссии (ФСТЭК) России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны в части противодействия	Периодически обновляется
139.	Перечень организаций, получивших лицензии Гостехкомиссии (ФСТЭК) России на проведение специальных экспертиз организаций на право осуществления мероприятий и (или) оказания услуг в области защиты государственной тайны в части противодействия иностранным техническим разведкам	Периодически обновляется

Учебное издание

**МЕЖДУНАРОДНЫЕ И РОССИЙСКИЕ
НОРМАТИВНЫЕ АКТЫ И СТАНДАРТЫ
ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Учебно-методическое пособие

Составитель: **Контылева** Елена Александровна

В авторской редакции

Изд. № 118/2025. Объем 9 п. л. Усл. печ. л. 8,37. Уч.-изд. л. 8,82.
Издательский центр ФГАОУ ВО «Севастопольский государственный университет»