МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)

Ю Р И Д И Ч Е С К И Й И Н С Т И Т У Т

ГРУЗДЕВА Л. М.

Защита информации

Учебное пособие

МОСКВА—2019

УДК 004.056.57
ББК 32.973
Г—87
ISBN 978-5-7876-0326-2

Груздева, Л. М. Защита информации : учеб. пособие / Л. М. Груздева. — Москва : Юридический институт МИИТ, 2019. — 144 с.

В пособии представлен обзор основных национальных стандартов Российской Федерации в области защиты информации. Описывается структура специальных государственных органов, осуществляющих регулирование и контроль в области информационной безопасности и защиты информации. Особое внимание уделено рассмотрению вопросов технической защиты информации, в том числе при применении информационных технологий. Приведены классификации по различным признакам факторов, воздействующих на безопасность защищаемой информации, угроз безопасности информации, уязвимостей информационных систем.

Пособие включает девять практических работ, целью выполнения которых является изучение основных положений и норм законодательных актов в сфере защиты информации, а также знакомства с правовыми информационными системами и сайтами государственных органов. Широкий перечень контрольных вопросов и тестовых заданий может быть полезен преподавателям модуля «Основы информационной безопасности и защита информации», а также широкому кругу читателей, самостоятельно изучающих вопросы защиты информации.

При работе с изданием использовалась справочная правовая система КонсультантПлюс.

Изд. заказ 17	Подписано в печать 02.10.2019	Тираж 100 экз.
Усл.-печ. л. 6,5	Уч.-изд. л. 4,8	Формат $60\times90^{1}/_{16}$

127994, Москва, ул. Образцова, д. 9, стр. 9.

Содержание

Введение

Защита информации согласно Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» представляет собой принятие правовых, организационных и технических мер, направленных:

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

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства РФ об информации, информационных технологиях и о защите информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством РФ, обязаны обеспечить:

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

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

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

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

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории РФ баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

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

Таким образом изучение вопросов в сфере защиты информации является необходимым условием для обеспечения качества подготовки специалистов с учетом требований современной цифровой экономики.

Данное учебное пособие предназначено для подготовки студентов юридического профиля, обучающихся по программам специалитета 40.05.03 «Судебная экспертиза», 40.05.02 «Правоохранительная деятельность» и 40.05.01 «Правовое обеспечение национальной безопасности».

Тема 1. Система стандартов по защите информации

Система стандартов по защите информации (ССЗИ) является составной частью национальной системы стандартизации Российской Федерации и формируется в соответствии с программами разработки национальных стандартов.

ГОСТ Р 52069.0-2013 «Защита информации. Система стандартов. Основные положения» (взамен ГОСТ Р 52069.0-2003) является основополагающим национальным стандартом Российской Федерации в области защиты информации, устанавливает цель, задачи и структуру системы стандартов по защите (некриптографическими методами) информации, объекты (рис. 1.1) и аспекты стандартизации в данной области.

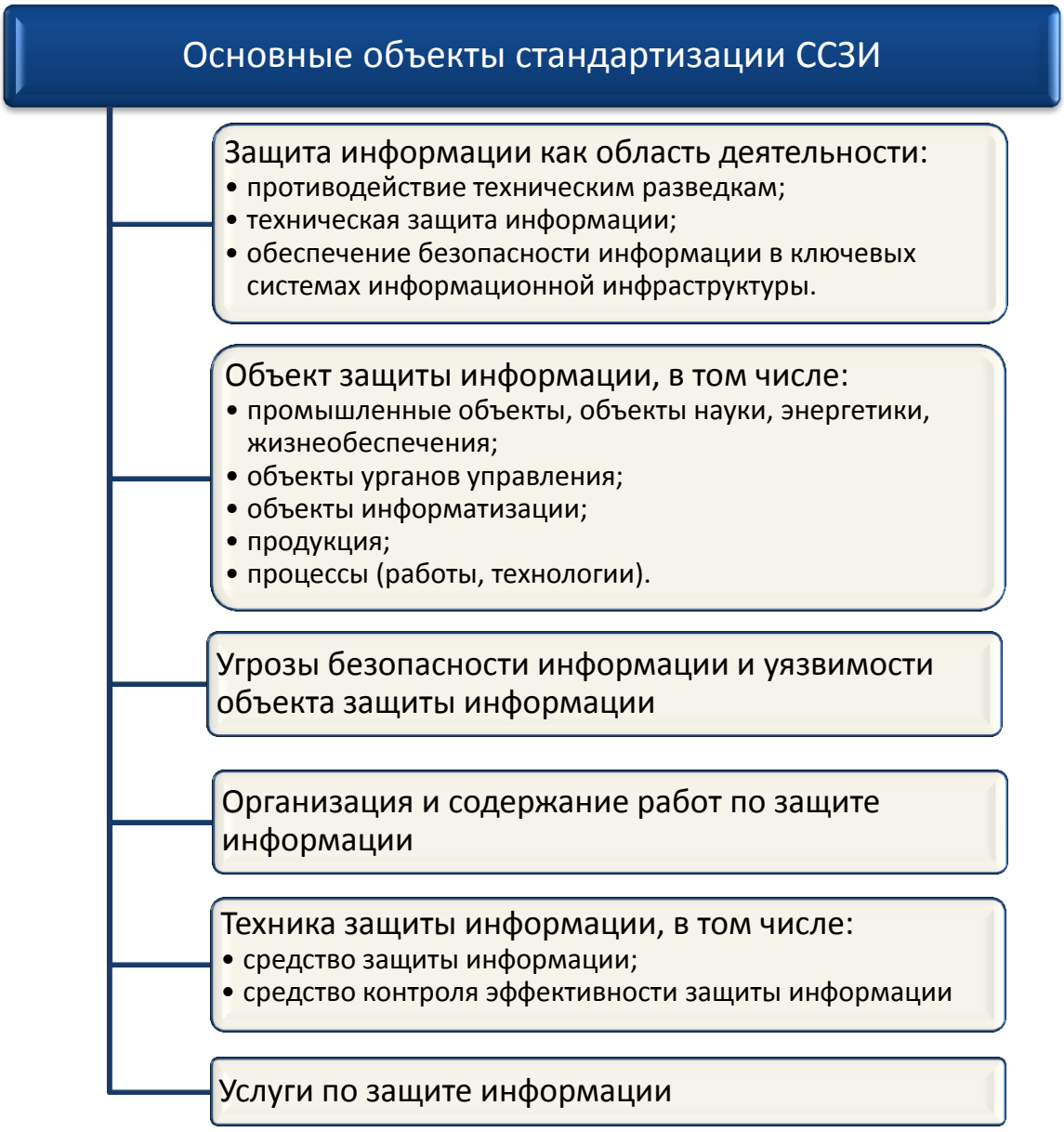


Рис. 1.1. **Основные объекты стандартизации ССЗИ**

Система стандартов по защите информации — совокупность взаимосвязанных стандартов, устанавливающих характеристики продукции, правила осуществления и характеристики процессов, выполнения работ или оказания услуг в области защиты информации.

Целью ССЗИ является достижение рациональной упорядоченности организации и содержания работ в области защиты информации (ЗИ), повышение эффективности ЗИ на основе установления общих правил и характеристик для их многократного использования, а также повышение эффективности работ по стандартизации за счет упорядочения структуры системы стандартов, процесса разработки стандартов, учета взаимосвязи стандартов различных систем.

Система стандартов по защите информации является составной частью общей системы документов в области ЗИ. Структура ССЗИ определяется объектами и аспектами стандартизации.

Основными *аспектами* стандартизации в ССЗИ являются: термины и определения в области ЗИ; классификация в области ЗИ (объектов защиты информации (ОЗИ), угроз безопасности информации, уязвимостей ОЗИ, работ и услуг по ЗИ, техники ЗИ); требования к системе документов в области ЗИ и ССЗИ и пр.

Система стандартов по защите информации включает подсистемы стандартов в области (рис. 1.2):

- противодействия техническим разведкам;
- технической защиты информации (ТЗИ);
- обеспечения безопасности информации в ключевых системах информационной инфраструктур (ОБИ в КСИИ).

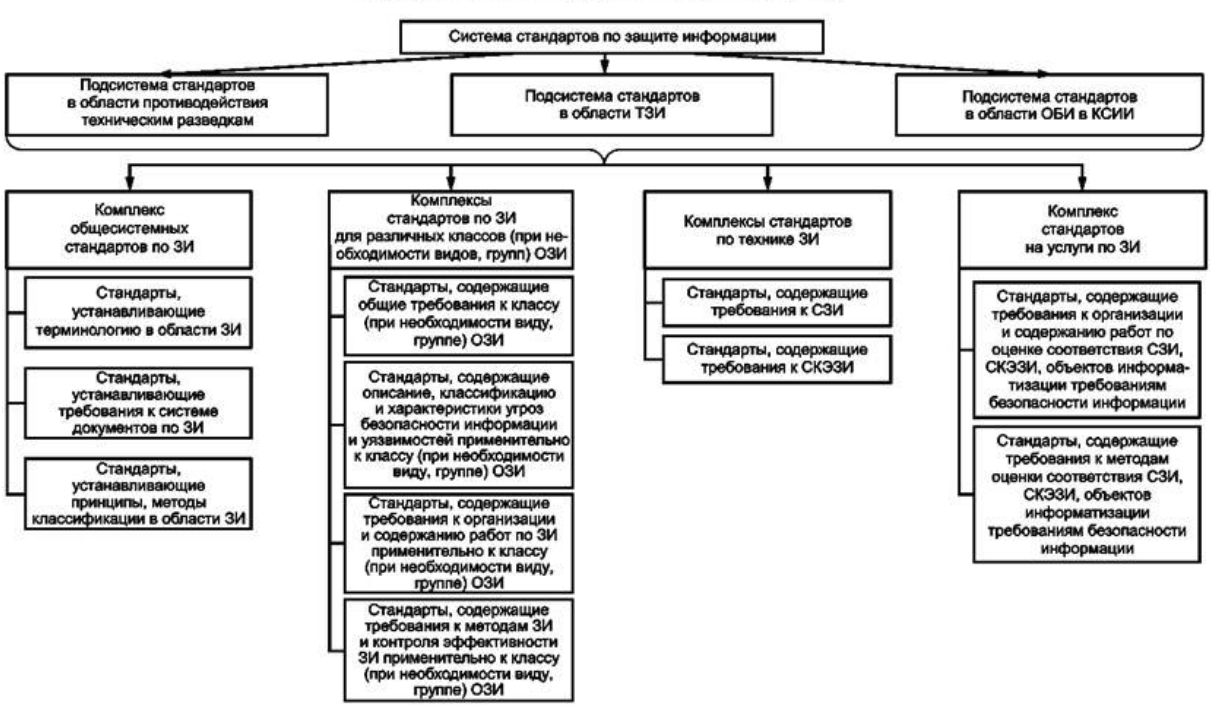


Рис. 1.2. **Структура системы стандартов по защите информации** (Приложение Б стандарта ГОСТ Р 52069.0-2013)

Перечень основных национальных стандартов Российской Федерации в области защиты информации:

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения (Protection of information. Basic terms and definitions): утвержден и введен (взамен ГОСТ Р 50922-96) в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст.

2. ГОСТ Р 52069.0-2013. Защита информации. Система стандартов. Основные положения (Safety of information. System of standards. Basic principles): утвержден и введен (взамен ГОСТ Р 52069.0-2003) в действие приказом Федерального агентства по техническому регулированию и метрологии от 28 февраля 2013 г. № 3-ст.

3. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения (Protection of information. Object of informatisation. Factors influencing the information. General): утвержден и введен (взамен ГОСТ Р 51275-99) в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст.

4. ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества (Information protection. Information protection technology. Nomenclature of quality indices): утвержден и введен (впервые) в действие приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 448-ст.

5. ГОСТ Р 52633.1-2009. Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации (Information protection. Information protection technology. Requirements for creation procedures for bases of natural biometric images, intended for high-reliability biometric authentication means testing): утвержден и введен (впервые) приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 839-ст.

6. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения (Information protection. Sequence of protected operational system formation. General): утвержден и введен (впервые) в действие приказом Федерального агентства по техническому регулированию и метрологии от 28 января 2014 г. № 3-ст.

7. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем (Information protection. Vulnerabilities in information systems. The classification of vulnerabilities in information systems): утвержден и введен (впервые) в действие приказом Федерального агентства по техническому регулированию и метрологии от 19 августа 2015 г. № 1181-ст.

8. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

(Protection of information. Information security provision in organization. Basic terms and definitions): утвержден и введен (впервые) в действие приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 532-ст.

9. ГОСТ Р 52863-2007. Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования (Protection of information. Protective automatically systems. Testing for stability to intentional power electromagnetic influence. General requirements): утвержден и введен (впервые) в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2007 г. № 515-ст.

10. ГОСТ Р 53112-2008. Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний (Information protection. Facilities for measuring side electromagnetic radiation and pickup parameters. Technical requirements and test methods): утвержден и введен (впервые) в действие приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 530-ст.

11. ГОСТ Р 53115-2008. Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства (Information protection. Conformance testing of technical information processing facilities to unauthorized access protection requirements. Methods and techniques): утвержден и введен (впервые) в действие приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 534-ст.

12. ГОСТ Р ИСО/МЭК 7498-1-99 Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель (Information technology. Open Systems Interconnection. Basic Reference Model. Part 1. The Basic Model): принят и введен (впервые) в действие постановлением Госстандарта России от 18 марта 1999 г. № 78.

13. ГОСТ Р ИСО 7498-2-99 Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации (Information technology. Open Systems Interconnection. Basic Reference Model. Part 2. Security Architecture): принят и введен (впервые) в действие постановлением Госстандарта России от 18 марта 1999 г. № 77.

14. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации: утверждены и введены (впервые) в действие приказом Федерального агентства по техническому регулированию и метрологии от 6 апреля 2005 г. № 77-ст.

15. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения: утверждены и введены (впервые) в действие приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 479-ст.

Контрольные вопросы и задания

1. Каковы правила применения национальных стандартов Российской Федерации, установленных в ГОСТ Р 1.0-2004 «Стандартизация в Российской Федерации. Основные положения»?
2. Каковы основные задачи международного сотрудничества в области стандартизации?
3. Что означают аббревиатуры: ЗИ, ОБИ в КСИ, ОЗИ, СЗИ, СКЭЗИ, ТЗИ, введенные в стандарте ГОСТ Р 52069.0-2013 «Защита информации. Система стандартов. Основные положения»?
4. Дайте определение понятию «система стандартов по защите информации» в соответствии со стандартом ГОСТ Р 52069.0-2013.
5. Каковы основные задачи по формированию и развитию ССЗИ?

Практическая работа 1.1. Основные положения и нормы Федерального закона «О техническом регулировании»

Цель работы: изучить основные положения Федерального закона от 27 декабря 2002 г. № 184-ФЗ, принципы технического регулирования.

Порядок выполнения работы

1. Изучить теоретический материал темы 1 «Система стандартов по защите информации» настоящего учебного пособия.
2. Выполнить задания, фиксируя каждый пункт работы в отчете.
3. Представить оформленный отчет преподавателю. Отчет должен содержать номера пунктов работы, их наименование и (в правой колонке) результат выполнения каждого пункта.

Задания

1. Запуск электронного фонда правовой и нормативно-технической документации АО «Кодекс».

1. Создайте файл отчета в MS Word по образцу, приведенному в приложении. Сохраните файл под именем «Ваша фамилия11» (например: Иванов11). Заполните его шапку.
2. Запустите электронную профессиональную справочную систему «Кодекс»/»Техэксперт», для чего:

— выйдите в Интернет на страницу http://docs.cntd.ru;

— откроется главная страница сайта (рис. 1.1.1), ознакомитесь с ее содержимым;

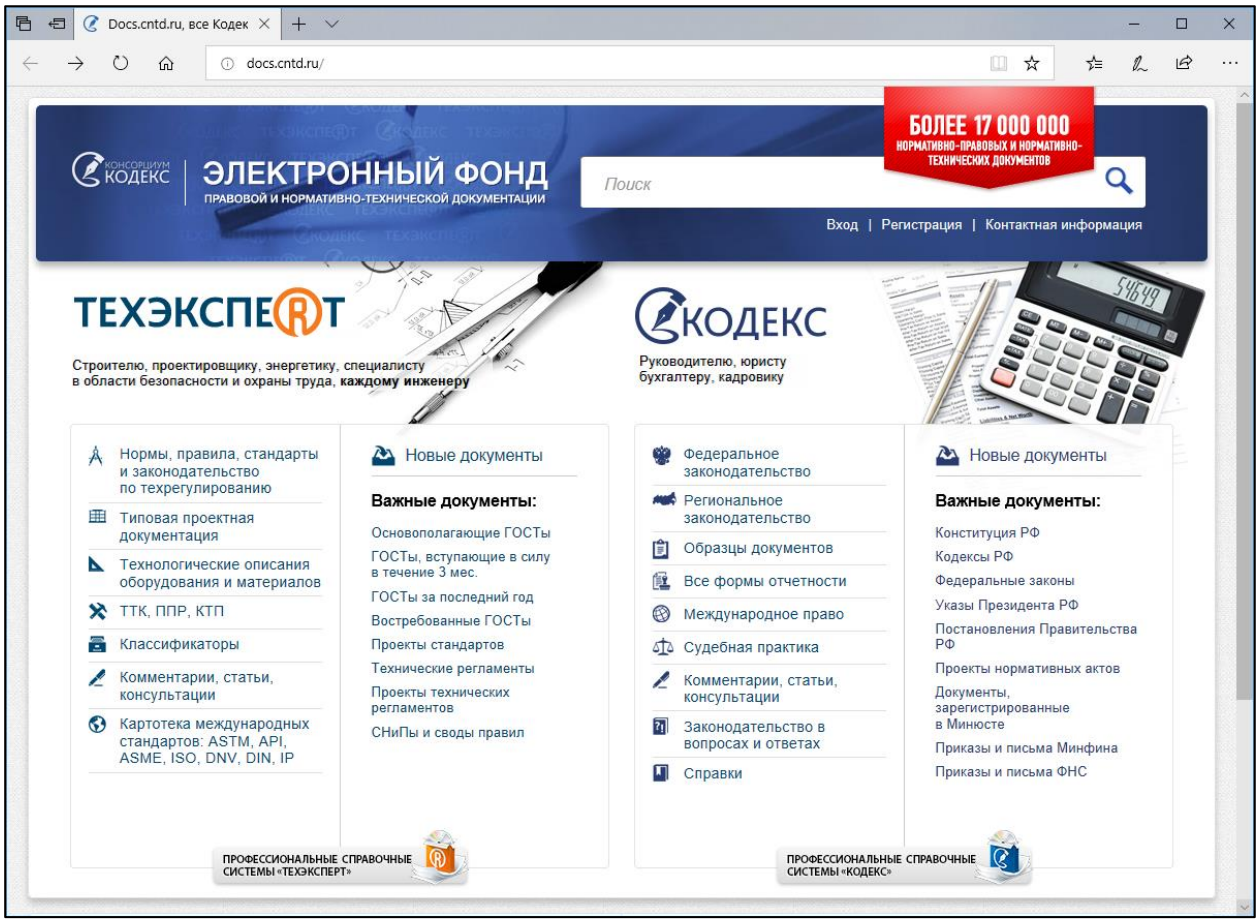


Рис. 2.1.1. **Сайт консорциума «Кодекс» http://docs.cntd.ru**

Зафиксируйте копию данной страницы в своем отчете.

2. Работа с Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

1. В строке быстрого поиска введите следующий текст: № 184-ФЗ и нажмите кнопку  .

2. Система сформирует список документов по введенному запросу (рис. 1.1.2). Каждый документ сопровождается символом  (означает, что документ действующий) или  (означает, что документ недействующий).

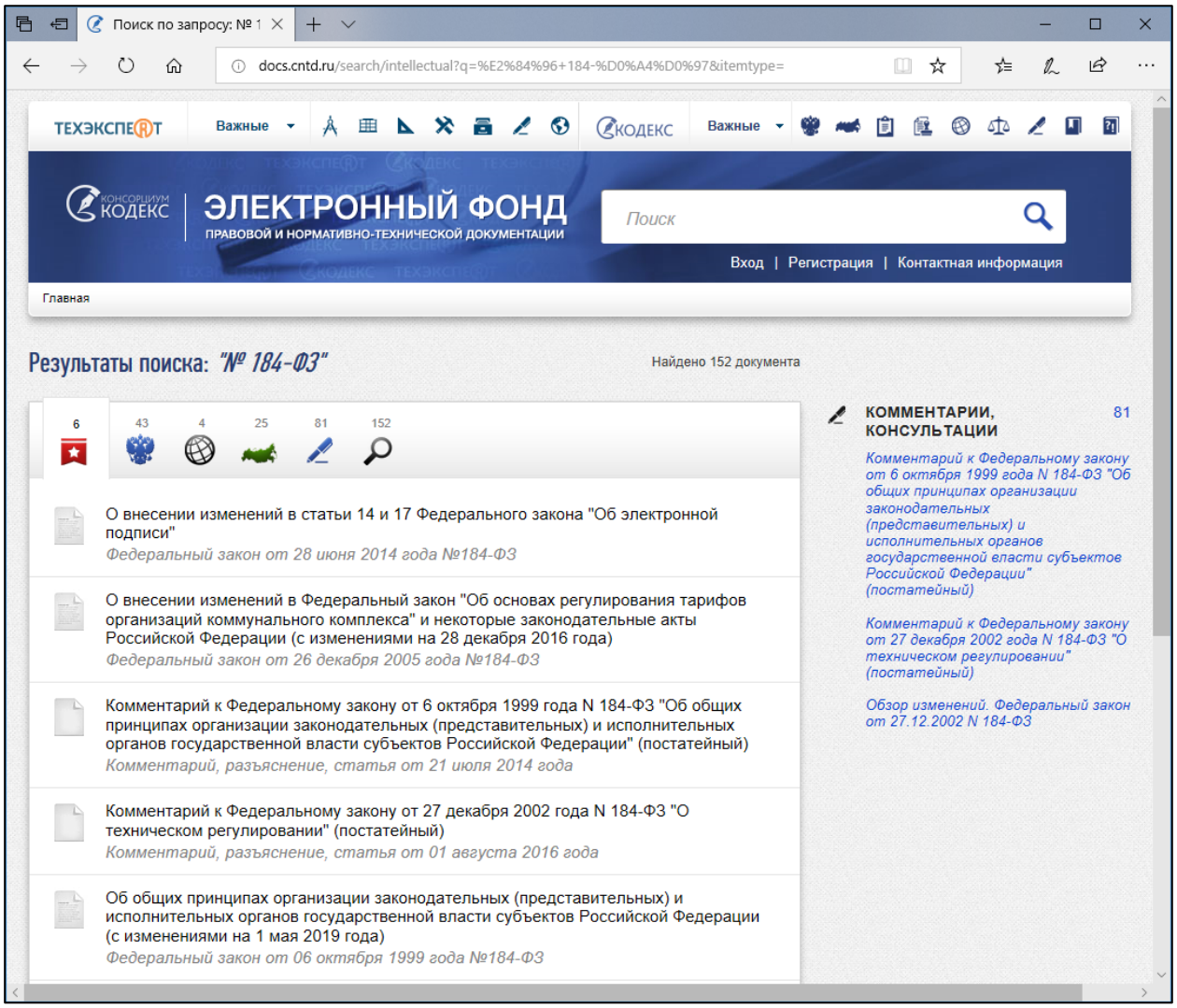


Рис. 1.1.2. **Сайт консорциума «Кодекс» http://docs.cntd.ru / результаты поиска по запросу «№ 184-ФЗ»**

Сохраните копию экрана со списком в отчете.

2. Откройте искомый Федеральный закон. *Копию экрана занесите в отчет.*

3. Откройте и *занесите в отчет копии* следующих разделов, связанных с выбранным документом (рис 1.1.3):

— Статус;

— Оперативная информация.

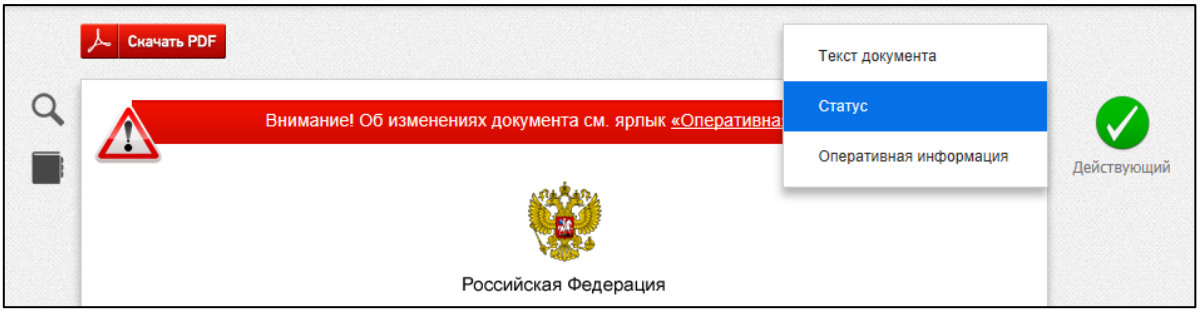


Рис. 1.1.3. **Сайт консорциума «Кодекс» http://docs.cntd.ru / разделы документа**

4. Вернитесь к тексту документа.

5. Откройте *Оглавление* документа с помощью кнопки  (рис 1.1.3), ознакомьтесь с ним и *скопируйте в отчет*.

6. С помощью *Оглавления* документа перейдите к Главе 2. Технические регламенты (статьи 6-10). *Копию экрана занесите в отчет*.

7. Изучите цели принятия технических регламентов. *Перенесите список целей в отчет*.

8. Внесите в отчет ответ на вопрос «Что обеспечивают минимально необходимые требования, устанавливаемые техническими регламентами с учетом степени риска причинения вреда?».

3. Изучить основные понятия и положения Закона.

1. Ответьте на вопросы для изучения в файле отчета. Номера вопросов определяются по начальной букве фамилии студента (табл. 1.1.1).

Таблица 1.1.1

Варианты к работе 1.1

Начальная буква фамилии студента	Номера вопросов	Начальная буква фамилии студента	Номера вопросов
А, И, С, Щ	1, 9, 17, 25, 33	Д, Н, Х	5, 13, 21, 29, 37
Б, К, Т	2, 10, 18, 26, 34	Е, О, Ц, Ю	6, 14, 22, 30, 38
В, Л, У, Э	3, 11, 19, 27, 35	Ж, П, Ч	7, 15, 23, 31, 39
Г, М, Ф	4, 12, 20, 28, 36	З, Р, Ш, Я	8, 16, 24, 32, 40

2. Представьте оформленный отчет по выполненной работе преподавателю на проверку.

Вопросы для изучения

1. Какие отношения регулирует Федеральный закон «О техническом регулировании»?

2. Какие отношения НЕ регулирует Федеральный закон «О техническом регулировании»?

3. Какой Федеральный закон «О техническом регулировании» устанавливает особенности технического регулирования в области обеспечения безопасности зданий и сооружений?

4. Какой Федеральный закон «О техническом регулировании» устанавливает особенности технического регулирования в области обеспечения безопасности продукции, а также процессов проектирования, производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, применяемых на территории инновационного центра «Сколково»?

5. Какой Федеральный закон «О техническом регулировании» устанавливает особенности технического регулирования в области обеспечения безопасности продукции, а также процессов проектирования, производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, применяемых на территории международного медицинского кластера?

6. Какой Федеральный закон «О техническом регулировании» устанавливает особенности технического регулирования в области обеспечения безопасности продукции, а также процессов проектирования, производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, применяемых на территориях инновационных научно-технологических центров?

7. Кем может принятия технического регламент?

8. Кто может быть разработчиком проекта технического регламента?

9. Дайте определение понятию «безопасность».

10. Дайте определение понятию «декларирование соответствия».

11. Дайте определение понятию «декларация о соответствии».

12. Дайте определение понятию «заявитель».

13. Дайте определение понятию «знак обращения на рынке».

14. Дайте определение понятию «знак соответствия».

15. Дайте определение понятию «контроль (надзор) за соблюдением требований технических регламентов».

16. Дайте определение понятию «международный стандарт».

17. Дайте определение понятию «орган по сертификации».

18. Дайте определение понятию «оценка соответствия».

19. Дайте определение понятию «подтверждение соответствия».

20. Дайте определение понятию «риск».

21. Дайте определение понятию «сертификация».

22. Дайте определение понятию «сертификат соответствия».

23. Дайте определение понятию «система сертификации».

24. Дайте определение понятию «техническое регулирование».

25. Дайте определение понятию «технический регламент».

26. Дайте определение понятию «форма подтверждения соответствия».

27. Дайте определение понятию «схема подтверждения соответствия».

28. Дайте определение понятию «региональная организация по стандартизации».

29. Дайте определение понятию «стандарт иностранного государства».

30. Дайте определение понятию «региональный стандарт».

31. Дайте определение понятию «свод правил иностранного государства».

32. Дайте определение понятию «региональный свод правил».

33. Что включает в себя сертификат соответствия?

34. Каковы функции органов по сертификации?

35. Каковы обязанности аккредитованных испытательных лабораторий?

36. Каковы права заявителя в области обязательного подтверждения соответствия?

37. Каковы обязанности заявителя в области обязательного подтверждения соответствия?

38. Каковы условия ввоза в Российскую Федерацию продукции, подлежащей обязательному подтверждению соответствия?

39. Каковы права органов государственного контроля (надзора)?

40. Каковы обязанности органов государственного контроля (надзора)?

Практическая работа 1.2. Классификация, построение и содержание стандартов в области защиты информации

Цель работы: изучить классификации, построения и содержания стандартов. Ознакомиться с объектами стандартизации в области защиты информации и с формированием обозначения стандарта.

Порядок выполнения работы

1. Изучить теоретическую часть.
2. Выполнить задания практической части.
3. Представить оформленный отчет преподавателю.

Стандарт (от англ. standard — норма, образец) в широком смысле слова — образец, эталон, модель, принимаемые за исходные для сопоставления с ними др. подобных объектов.

Международная организация по стандартизации (International Organization for Standardization, ISO, ИСО) определяет с*тандарт* как документ, устанавливающий требования, спецификации, руководящие принципы или характеристики, в соответствии с которыми могут использоваться материалы, продукты, процессы и услуги, которые подходят для этих целей.

Стандарт в Российской Федерации — документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг.

Категория стандарта — типологический признак стандарта, определяющий его принадлежность к стандартам определенного уровня принятия и применения (международного, регионального, межгосударственного, национального, корпоративного или уровня организации).

Различают следующие уровни стандартизации:

1) Международная стандартизация. Органом по стандартизации является ИСО (ISO). Нормативным документом ИСО являются стандарты ИСО.

2) Межрегиональная стандартизация. Охватывает ряд независимых государств (СНГ, ЕЭС и др.). Нормативным документом стран СНГ является межрегиональный стандарт.

3) Национальная стандартизация. Это — стандартизация в пределах одного государства. Нормативным документом по национальной стандартизации в России установлен государственный стандарт России — ГОСТ Р, в ФРГ — DIN, в Великобритании — BS, и т. д.

4) Правила, нормы и рекомендации в области стандартизации, общероссийские классификаторы технико-экономической и социальной информации.

5) Стандарты организаций — отраслевые стандарты (ОСТ[1]), стандарты предприятий (СТП), стандарты обществ и т. п. Это — низший уровень стандартизации.

В зависимости от специфики объекта стандартизации и содержания устанавливаемых к нему требований применяют следующие основные *виды* межгосударственных стандартов[2]:

- стандарты основополагающие;
- стандарты на продукцию;
- стандарты на услуги;
- стандарты на процессы;
- стандарты на методы контроля (испытаний, измерений, анализа);
- стандарты на термины и определения.

Правила оформления и обозначения национальных стандартов Российской Федерации, разрабатываемых на основе применения международных, региональных стандартов и национальных стандартов других стран.

Обозначение стандарта состоит из индекса «ГОСТ Р», регистрационного номера и отделенных от него тире четырех цифр года утверждения (принятия) стандарта (года его регистрации). Пример: ГОСТ Р 8724-2002.

Оформление национального стандарта Российской Федерации, идентичного международному (региональному) стандарту, осуществляют путем использования русской версии данного международного стандарта или аутентичного перевода на русский язык английской или французской версии международного (регионального) стандарта без изменения структуры и технического содержания.

В идентичном стандарте обязательному переоформлению относительно применяемого международного (регионального) стандарта для приведения в соответствие с правилами настоящего стандарта подлежат обозначение, титульный лист, предисловие, первая страница и библиографические данные, а

[1] *Отраслевой стандарт* (ОСТ) — устанавливается на те виды продукции, нормы, правила, требования, понятия и обозначения, регламентация которых необходима для обеспечения качества продукции данной отрасли. Обычно в виде ОСТов оформляются типовые ситуации, которые после дальнейшей практической проверки и подтверждения своей важности служат основой для выпуска соответствующего ГОСТа.

[2] ГОСТ 1.0-2015 Межгосударственная система стандартизации (МГСС). Основные положения.

при необходимости также наименование и/или разделы «Термины и определения» и/или «Обозначения и сокращения». Допускается также изменять стиль изложения отдельных формулировок (без изменения технического содержания) по отношению к русской версии (аутентичному переводу на русский язык) применяемого международного (регионального) стандарта.

Примеры:

национальный стандарт Российской Федерации, идентичный международному стандарту ИСО 7498-2-89, обозначают: ГОСТ Р ИСО 7498-2-99;

национальный стандарт Российской Федерации, идентичный международному стандарту ИСО/МЭК 7498-1-94, обозначают: ГОСТ Р ИСО/МЭК 7498-1-99.

Задания

1. Создайте файл отчета в MS Word. Сохраните файл под именем «Ваша фамилия12» (например: Иванов12).

2. Получите у преподавателя три стандарта в области защиты информации, изучите их, перенесите в отчет и заполните табл. 1.2.1.

Таблица 1.2.1

Характеристика стандартов

№	Обозначение и название стандарта	Категория стандарта	Вид стандарта	Структурные элементы (они совпадают с названиями разделов)	Область применения стандарта
1.					
2.					
3.					

3. Откройте текст национального стандарта Российской Федерации ГОСТ Р 52069.0-2013 «Защита информации. Система стандартов. Основные положения». Перенесите в отчет и заполните табл. 1.2.2.

Таблица 1.2.2

Характеристика стандарта ГОСТ Р 52069.0-2013

№	Структурные элементы	Содержание стандарта
1.	Объекты стандартизации ССЗИ	
2.	Аспекты стандартизации в	

	ССЗИ		
3.	Виды документов в области стандартизации по ЗИ, используемые на территории РФ, включает система стандартов по защите информации		
4.	Подсистемы стандартов, которые включает ССЗИ		
5.	Состав комплексов стандартов по технике ЗИ		
6.	Структура регистрационного номера стандартов ССЗИ		

4. Откройте текст национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Перенесите в отчет и заполните табл. 1.2.3.

Таблица 1.2.3

Основные термины ГОСТ Р ИСО/МЭК 27001-2006

№	Термин	Русский перевод термина	Первоисточник термина	Определение
1.	Asset			
2.	Availability			
3.	Confidentiality			
4.	Information security			
5.	Information security event			
6.	Information security incident			
7.	Information security management system			
8.	Integrity			
9.	Risk analysis			
10.	Risk assessment			

5. Перейдите на сайт Международной организация по стандартизации (https://www.iso.org/ru/home.html). Изучите структуру и руководящие органы ИСО. *Перенесите в свой отчет* организационную структуру управления ИСО. Укажите действующего президента ИСО.

6. Перенесите в отчет вопросы для изучения и ответьте на каждый из них.

7. Представьте оформленный отчет по выполненной работе преподавателю на проверку.

Вопросы для изучения

1. Что такое стандарт?
2. Что такое категория стандарта?
3. Перечислите известные вам категории стандартов.
4. Какие категории стандартов прописаны в Федеральном законе «О техническом регулировании»?
5. Что значит вид стандарта?
6. Назовите виды стандартов, применяемые в международной практике.
7. Какие виды стандартов используются в РФ?
8. Назовите основные международные организации по стандартизации.
9. Какие направления являются приоритетными при разработке международных стандартов?
10. Являются ли международные стандарты обязательными?

Тема 2. Основные понятия в области защиты информации

Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» устанавливает основные термины[1] с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации.

Правила применения национальных стандартов Российской Федерации установлены в ГОСТ Р 1.0-2004 «Стандартизация в Российской Федерации. Основные положения».

В стандарте ГОСТ Р 50922-2006 реализованы нормы Федеральных законов от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

[1] Термины, установленные настоящим стандартом, рекомендуется использовать в правовой, нормативной, технической и организационно-распорядительной документации, научной, учебной и справочной литературе.

Федеральный закон «Об информации, информационных технологиях и о защите информации» определяет понятие *информация*[1] и предусматривает ее разделение на *общедоступную информацию* и на информацию, доступ к которой ограничен федеральными законами (*информация ограниченного доступа*). В свою очередь информация ограниченного доступа подразделяется на информацию, отнесенную к *государственной тайне* (секретная информация) и *конфиденциальную*.

Безопасность информации — состояние защищенности информации, при котором обеспечены ее конфиденциальность[2], доступность[3] и целостность[4].

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

Объект защиты информации — информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

Защита информации (ЗИ) — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

К *правовым мерам защиты* относятся федеральные законы, указы Президента РФ и другие нормативные правовые акты. На законодательном уровне происходит регламентация правил обращения с информацией, определяются участники информационных отношений, их права и обязанности, а также ответственность в случае нарушения требований законодательства. Их основной функцией является упреждение потенциальных злоумышленников[5] и нарушителей[6].

---

[1] *Информация* — сведения (сообщения, данные) независимо от формы их представления [Федеральный закон «Об информации, информационных технологиях и о защите информации»].

[22] *Конфиденциальность информации* — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [Федеральный закон «Об информации, информационных технологиях и о защите информации»].

[3] *Доступность информации* — состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно [Р 50.1.053-2005].

[4] *Целостность* — состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право [Р 50.1.056-2005].

[5] *Злоумышленник* — лицо, заинтересованное в получении возможности несанкционированного доступа к конфиденциальной информации, представляющей промышленную и коммерческую тайну, предпринимающее попытку такого доступа или совершившее его [ГОСТ Р 52633.1-2009].

[6] *Нарушитель* (attacker) — любое лицо, преднамеренно использующее уязвимости технических и нетехнических мер и средств контроля и управления безопасностью с целью захвата или компрометации информационных систем и сетей, или снижения доступности ресурсов информационной системы и сетевых ресурсов для законных пользователей [ГОСТ Р ИСО/МЭК 27033-1-2011].

Меры организационного характера предназначены для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой, они должны работать в комплексе с физическими и техническими средствами защиты информации в части определения действий людей.

К *техническим мерам* относятся меры по защите от утечки информации по техническим каналам, защите от несанкционированного доступа, от программного воздействия, от вредоносных программ и т.п.

В стандарте ГОСТ Р 50922-2006 установлены следующие термины, относящиеся к замыслу защиты информации:

Замысел защиты информации — основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Цель защиты информации — заранее намеченный результат защиты информации.

Система защиты информации — совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

Техника защиты информации — средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

В стандарте ГОСТ Р 50922-2006 выделено четыре вида защиты информации (рис. 2.1). Организационные мероприятия по обеспечению физической защиты информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

К объектам защиты информации могут быть отнесены:

- охраняемая территория,
- здание (сооружение),
- выделенное помещение,
- информация и (или) информационные ресурсы объекта информатизации.

Объект информатизации (ОИ) — совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Рис. 2.1. **Виды защиты информации**

В стандарте ГОСТ Р 50922-2006 установлены следующие термины, относящиеся к способам защиты информации:

Способ защиты информации (рис. 2.2) — порядок и правила применения определенных принципов и средств защиты информации[1].

Защита информации от утечки — защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

[1] *Средство защиты информации* — техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации [ГОСТ Р 50922-2006].

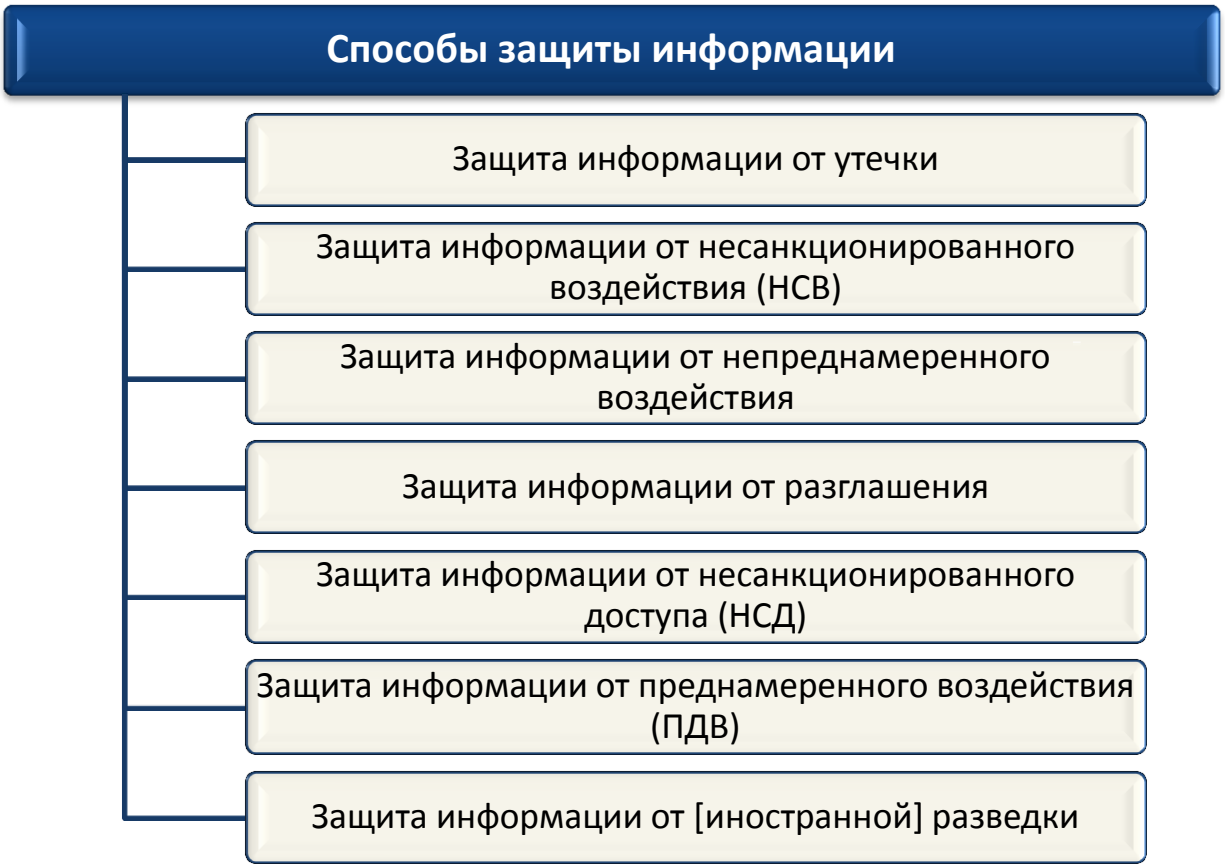


Рис. 2.2. **Способы защиты информации**

Защита информации от несанкционированного воздействия — защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия — защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения — защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа — защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями ин-

формации прав или правил разграничения доступа к защищаемой информации.

Защита информации от преднамеренного воздействия — защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного, и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

Защита информации от [иностранной] разведки — защита информации, направленная на предотвращение получения защищаемой информации [иностранной] разведкой.

Контрольные вопросы и задания

1. Как разделяется информация в зависимости от порядка ее предоставления или распространения в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»?
2. Как разделяется информация в зависимости от категории доступа в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации»?
3. Дайте определение понятию «информация».
4. Определите понятия «доступ к информации» и «конфиденциальность информации».
5. Как ГОСТ Р 50922-2006 определяет термин «защита информации»?
6. Дайте определение понятию «защищаемая информация».
7. Что относится к правовым мерам защиты информации?
8. Для чего предназначены меры организационного характера защиты информации?
9. Что относится к техническим мерам защиты информации?
10. Дайте определение понятию «безопасность информации»?
11. В чем заключается замысел и цель защиты информации в соответствии с ГОСТ Р 50922-2006?
12. Дайте определение понятию «система защиты информации»?
13. Дайте определение понятию «техника защиты информации»?
14. Дайте определение понятию «объект защиты информации»?
15. Какие виды защиты информации выделены в стандарте ГОСТ Р 50922-2006? Охарактеризуйте каждый из них.
16. Что может быть отнесено к объектам защиты информации?
17. Как определено понятие «злоумышленник» в стандарте ГОСТ Р 52633.1-2009?
18. Как определено понятие «нарушитель» в стандарте ГОСТ Р ИСО/МЭК 27033-1-2011?
19. Как определено понятие «доступность информации» в рекомендациях Р 50.1.053-2005?

20. Как определено понятие «целостность» в Р 50.1.056-2005?

21. Дайте определение понятию «способ защиты информации».

22. Дайте определение понятию «средство защиты информации».

23. Какие способы защиты информации выделены в стандарте ГОСТ Р 50922-2006?

24. Дайте определение понятию «защита информации от утечки».

25. Дайте определение понятию «защита информации от несанкционированного воздействия».

26. Дайте определение понятию «защита информации от непреднамеренного воздействия».

27. Дайте определение понятию «защита информации от разглашения».

28. Дайте определение понятию «защита информации от несанкционированного доступа».

29. Дайте определение понятию «защита информации от преднамеренного воздействия».

30. Дайте определение понятию «защита информации от [иностранной] разведки».

Практическая работа 2.1. Основные положения и нормы Федерального закона «Об информации, информационных технологиях и о защите информации»

Цель работы: изучить основные положения Федерального закона от 27 июля 2006 г. № 149-ФЗ, принципы правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации.

Порядок выполнения работы

1. Изучить теоретический материал темы 2 «Основные понятия в области защиты информации» настоящего учебного пособия.

2. Выполнить задания, фиксируя каждый пункт работы в отчете.

3. Представить оформленный отчет преподавателю. Отчет должен содержать номера пунктов работы, их наименование и (в правой колонке) результат выполнения каждого пункта.

Задания

1. Запуск on-line версии КонсультантПлюс.

1. Создайте файл отчета в MS Word по образцу, приведенному в приложении. Сохраните файл под именем «Ваша фамилия21» (например: Иванов21). Заполните его шапку.

2. Запустите интернет-версию КонсультантПлюс, для чего:

— выйдите в Интернет на страницу http://www.consultant.ru/online (рис. 2.1.1);

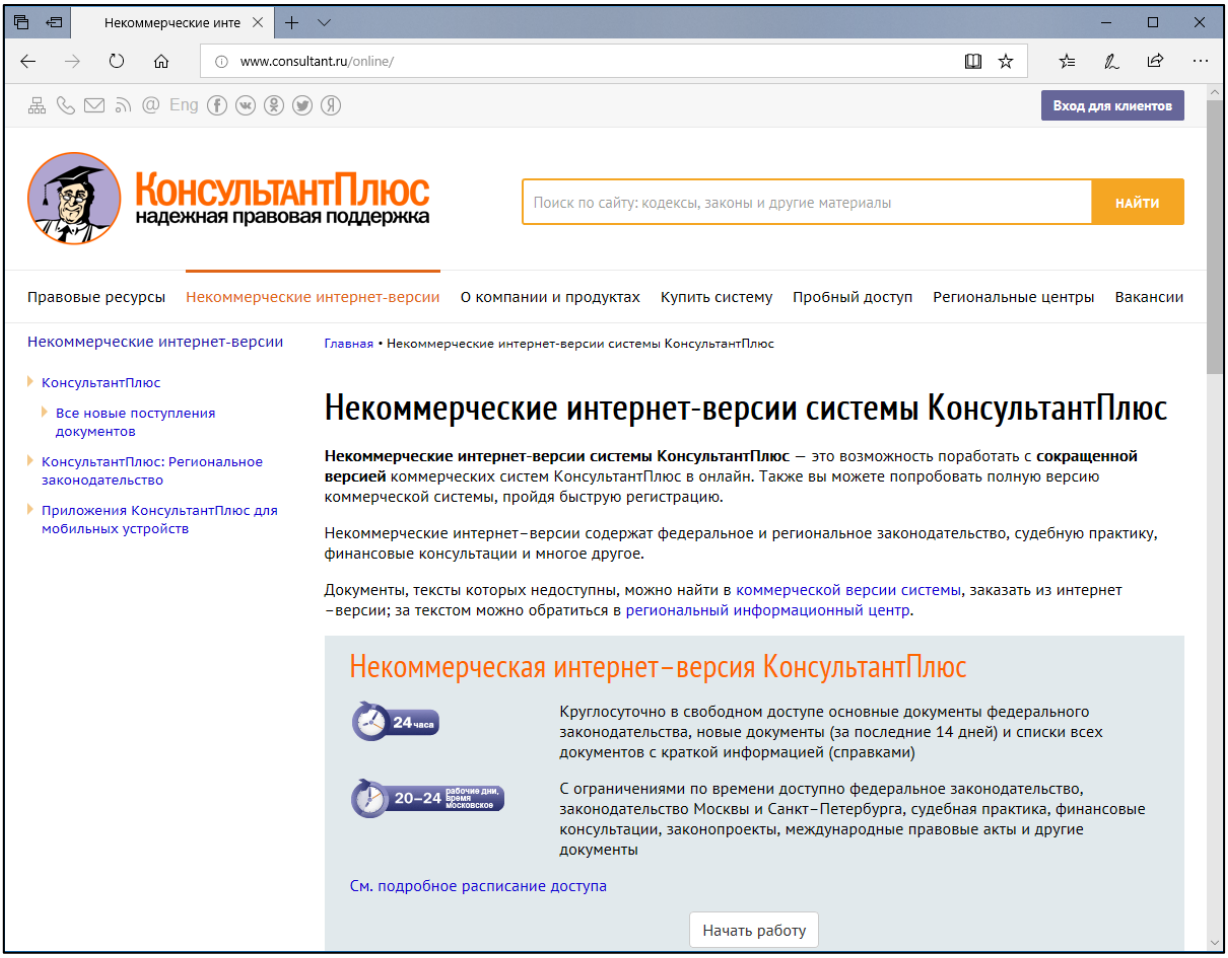


Рис. 2.1.1. **Интернет-страница КонсультантПлюс**

— перейдите на некоммерческую интернет-версию КонсультантПлюс по ссылке «Начать работу». Откроется первая страница системы (рис 2.1.2), ознакомитесь с ее содержимым;

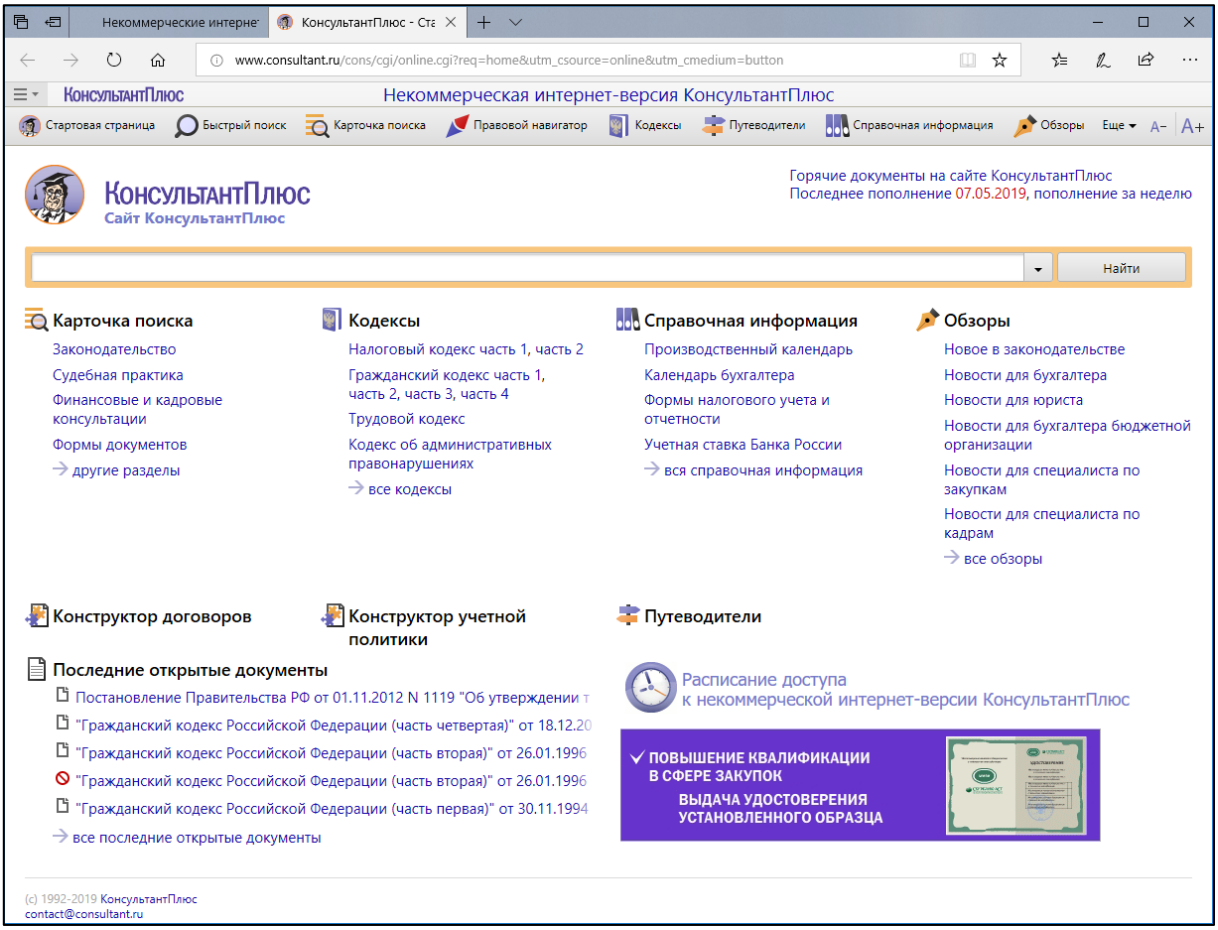


Рис. 2.1.2. **Некоммерческая интернет-версия КонсультантПлюс**

Зафиксируйте копию данной страницы в своем отчете.

3. Ознакомьтесь с расписанием доступа к некоммерческой версии КонсультантПлюс и *копию страницы с расписанием занесите в отчет.*

2. Работа с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1. В строке быстрого поиска введите следующий текст: № 149-ФЗ и нажмите кнопку Найти.

КонсультантПлюс сформирует перечень документов, наиболее соответствующих запросу. Каждый документ сопровождается символом (означает, что текст документа находится в свободном доступе) или (означает, что текст документа в некоммерческой интернет-версии КонсультантПлюс в данный момент недоступен.).

Сохраните копию экрана со списком в отчете.

2. Откройте искомый Федеральный закон. Скорее всего он будет первым по списку. *Копию экрана занесите в отчет.*

3. Откройте и *занесите в отчет копии* следующих разделов, связанных с выбранным документом (рис 2.1.3):

— Дополнительная информация к документу;

— Обзор изменений документа;
— Сравнить с предыдущей редакцией.

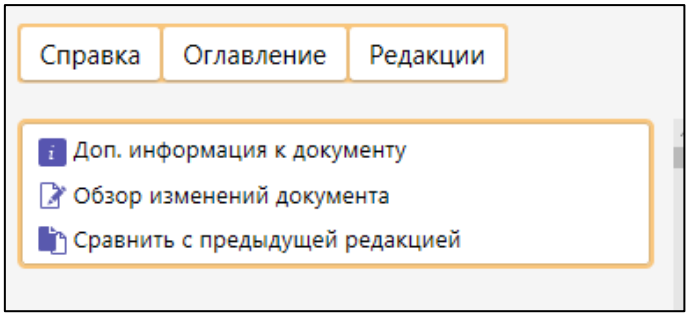


Рис. 2.1.3. **Разделы документа в КонсультантПлюс**

4. Используя кнопку *Редакции* (рис 2.1.3), определите действующую редакцию и редакции, еще не вступившие в силу. *Список редакций занесите в отчет*.

5. Откройте, ознакомьтесь и *скопируйте в отчет* для Федерального закона «Об информации, информационных технологиях и о защите информации» (рис 2.1.3):
— Справку;
— Оглавление.

6. Раскройте статью документа «Защита информации» и *копию экрана занесите в отчет*.

7. Изучите обязанности обладателей информации и операторов информационных систем, в случаях, установленных законодательством Российской Федерации. *Перенесите список обязанностей в отчет*.

8. Откройте Приказ ФСТЭК России от 11.02.2013 №7 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», для этого перейдите по ссылке Требования (рис. 2.1.4).

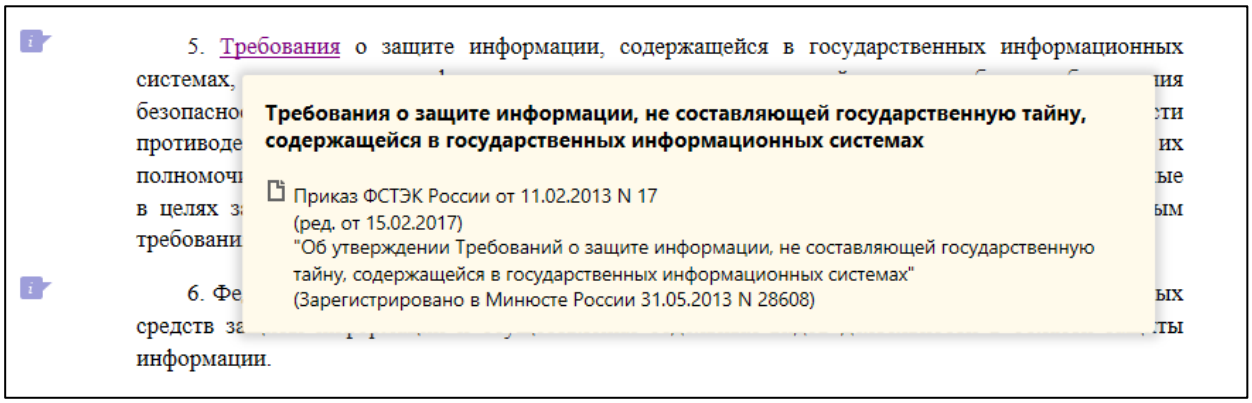


Рис. 2.1.4. **Статья 16. Защита информации, пункт 5**

9. Найдите в тексте Приказа ФСТЭК России от 11.02.2013 №7 мероприятия, которые должны проводиться для обеспечения защиты информации, содержащейся в информационной системе. Для этого:

— в строке поиска введите: *мероприятия*;

— нажмите кнопку Найти и убедитесь, что система нашла пункт 13;

— *перенесите список мероприятий в отчет*.

3. Изучить основные понятия и положения Закона.

1. Вернитесь к тексту Федерального закона «Об информации, информационных технологиях и о защите информации» на первую страницу системы.

2. Ответьте на вопросы для изучения в файле отчета. Номера вопросов определяются по начальной букве фамилии студента (табл. 2.1).

Таблица 2.1.1

Варианты к работе 2.1

Начальная буква фамилии студента	Номера вопросов	Начальная буква фамилии студента	Номера вопросов
А, И, С, Щ	1, 9, 17, 25, 33	Д, Н, Х	5, 13, 21, 29, 37
Б, К, Т	2, 10, 18, 26, 34	Е, О, Ц, Ю	6, 14, 22, 30, 38
В, Л, У, Э	3, 11, 19, 27, 35	Ж, П, Ч	7, 15, 23, 31, 39
Г, М, Ф	4, 12, 20, 28, 36	З, Р, Ш, Я	8, 16, 24, 32, 40

3. Представьте оформленный отчет по выполненной работе преподавателю на проверку.

Вопросы для изучения

1. Какие отношения регулирует Федеральный закон «Об информации, информационных технологиях и о защите информации»?
2. На каких принципах основывается правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации?
3. Когда информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу?
4. Дайте определение понятию «информация».
5. Дайте определение понятию «информационные технологии».
6. Дайте определение понятию «информационная система».
7. Дайте определение понятию «информационно-телекоммуникационная сеть».
8. Дайте определение понятию «обладатель информации».
9. Дайте определение понятию «доступ к информации».
10. Дайте определение понятию «конфиденциальность информации».
11. Дайте определение понятию «предоставление информации».
12. Дайте определение понятию «распространение информации».
13. Дайте определение понятию «электронное сообщение».

14. Дайте определение понятию «документированная информация».
15. Дайте определение понятию «электронный документ».
16. Дайте определение понятию «оператор информационной системы».
17. Дайте определение понятию «сайт в сети «Интернет»«.
18. Дайте определение понятию «страница сайта в сети «Интернет»«.
19. Дайте определение понятию «доменное имя».
20. Дайте определение понятию «сетевой адрес».
21. Дайте определение понятию «владелец сайта в сети «Интернет»«.
22. Дайте определение понятию «провайдер хостинга».
23. Дайте определение понятию «единая система идентификации и аутентификации».
24. Дайте определение понятию «поисковая система».
25. Как подразделяется информация в зависимости от категории доступа к ней?
26. Как подразделяется информация в зависимости от порядка ее предоставления или распространения?
27. Кто может являться обладателем информации?
28. Обязанности обладателя информации при осуществлении своих прав?
29. Что относится к общедоступной информации?
30. Какая информация является общедоступной, размещаемой в форме открытых данных?
31. При каких условиях граждане и организации вправе осуществлять поиск и получение любой информации в любых формах и из любых источников?
32. Когда гражданин и организация имеют право на получение информации от государственных органов и органов местного самоуправления?
33. К какой информации не может быть ограничен доступ?
34. Какую информацию запрещается требовать от гражданина?
35. Какую информацию обязан хранить на территории Российской Федерации организатор распространения информации в сети «Интернет»?
36. Что предусматривает государственное регулирование в сфере применения информационных технологий?
37. Что включают в себя информационные системы?
38. С какой целью создаются государственные информационные системы?
39. Каковы основания для включения в «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»?
40. Что представляет собой защита информации?

Тема 3. Государственные органы в области защиты информации

Система государственного регулирования и контроля в области информационной безопасности построена на деятельности специальных государственных органов, к которым относятся следующие.

Комитет Государственной Думы по безопасности и противодействию коррупции (Комитет) является постоянным действующим структурным подразделением Государственной Думы Федерального Собрания Российской Федерации[1]. Комитет образуется из числа депутатов Государственной Думы. Состав Комитета и изменения в нем определяются Государственной Думой.

В ведении Комитета находится предварительное рассмотрение и подготовка к рассмотрению Государственной Думой законопроектов и проектов постановлений палаты по различным вопросам, в том числе об информационной безопасности личности, общества и государства (защита информации, составляющей государственную, служебную и коммерческую тайну, защита персональных данных, информационно-психологическая безопасность человека).

Совет Безопасности Российской Федерации является конституционным совещательным органом, осуществляющим подготовку решений Президента РФ по вопросам обеспечения безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством РФ, организации обороны, военного строительства, оборонного производства, военного и военно-технического сотрудничества Российской Федерации с иностранными государствами, по иным вопросам, связанным с защитой конституционного строя, суверенитета, независимости и территориальной целостности Российской Федерации, а также по вопросам международного сотрудничества в области обеспечения безопасности[2].

[1] Положение о Комитете Государственной Думы Федерального Собрания Российской Федерации по безопасности и противодействию коррупции: утверждено решением Комитета Государственной Думы по безопасности и противодействию коррупции, протокол от 17 января 2017 г. № 15/8).

[2] Указ Президента РФ от 6 мая 2011 г. № 590 «Вопросы Совета Безопасности Российской Федерации».

Совет Безопасности в соответствии с Конституцией РФ формирует и возглавляет Президент РФ. Работой Совета Безопасности руководит Председатель Совета Безопасности.

Служба внешней разведки Российской Федерации (СВР России) является составной частью сил обеспечения безопасности и призвана защищать безопасность личности, общества и государства от внешних угроз. СВР России осуществляет разведывательную деятельность в целях[1]:

– обеспечения Президента РФ, Федерального Собрания и Правительства разведывательной информацией, необходимой им для принятия решений в политической, экономической, военно-стратегической, научно-технической и экологической областях;

– обеспечения условий, способствующих успешной реализации политики Российской Федерации в сфере безопасности;

– содействия экономическому развитию, научно-техническому прогрессу страны и военно-техническому обеспечению безопасности Российской Федерации.

Общее руководство органами внешней разведки Российской Федерации осуществляет Президент РФ. Руководители Службы внешней разведки несут персональную ответственность перед Президентом РФ за достоверность, объективность разведывательной информации и своевременность ее предоставления.

Министерство обороны Российской Федерации (Минобороны России) — федеральный орган исполнительной власти, проводящий государственную политику и осуществляющий государственное управление в области обороны, а также координирующий деятельность федеральных министерств, иных федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ по вопросам обороны.

Министерство внутренних дел Российской Федерации (МВД России) — федеральный орган исполнительной власти, осуществляющий функции по реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, в сфере контроля за оборотом наркотических средств, психотропных веществ и их прекурсоров, а также в сфере миграции.

[1] Федеральный закон от 10 января 1996 г. № 5-ФЗ «О внешней разведке».

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных, а также функции по организации деятельности радиочастотной службы[1]. Роскомнадзор является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных.

Службу возглавляет руководитель, назначаемый на должность и освобождаемый от должности Правительством РФ по представлению Министра связи и массовых коммуникаций РФ.

В области технической защиты информации ключевыми органами являются ФСБ и ФСТЭК России.

Федеральная служба безопасности (ФСБ России) — единая централизованная система органов федеральной службы безопасности, осуществляющая решение в пределах своих полномочий задач по обеспечению безопасности Российской Федерации. Руководство деятельностью Службы осуществляется Президентом РФ.

Согласно Федеральному закону от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности» одним из направлений деятельности органов ФСБ России является обеспечение информационной безопасности, осуществляемое 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, сетей связи специального назначения и иных сетей связи, обеспечивающих передачу шифрованной информации, в Российской Федерации и ее учреждениях, находящихся за пределами Российской Федерации.

[1] Постановление Правительства РФ от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам[1]:

1) обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

2) противодействия иностранным техническим разведкам на территории РФ;

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

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

5) осуществления экспортного контроля.

ФСТЭК России возглавляет директор Службы, назначаемый на должность и освобождаемый от должности Президентом РФ по представлению Председателя Правительства РФ.

Контрольные вопросы и задания

1. Каковы основные задачи Комитета Государственной Думы Федерального РФ Федерации по безопасности и противодействию коррупции?
2. Каковы основные функции Комитета Государственной Думы Федерального Собрания РФ по безопасности и противодействию коррупции?
3. Каков состав, структура и общий порядок Комитета Государственной Думы Федерального Собрания РФ по безопасности и противодействию коррупции?
4. Какие вопросы находятся в ведении Комитета Государственной Думы Федерального Собрания РФ по безопасности и противодействию коррупции?
5. Каковы задачи Совета Безопасности РФ?
6. Каковы функции Совета Безопасности РФ?

[1] Указ Президента РФ от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

7. Каков состав Совета Безопасности РФ?

8. Кто информирует Президента РФ о состоянии национальной безопасности?

9. Каковы основные задачи аппарата Совета Безопасности РФ?

10. Каковы основные функции аппарата Совета Безопасности РФ?

11. Какие функции возложены на Межведомственную комиссию Совета Безопасности РФ по информационной безопасности?

12. Какие функции возложены на научный совет при Совете Безопасности РФ?

13. Каковы цели разведывательной деятельности в соответствии с Федеральным законом от 10 января 1996 г. № 5-ФЗ «О внешней разведке».

14. Определите методы и средства разведывательной деятельности, установленные Федеральным законом от 10 января 1996 г. № 5-ФЗ «О внешней разведке».

15. Какие полномочия осуществляет Роскомнадзор?

16. Какова процедура назначения руководителя Роскомнадзона? Его полномочия?

17. Каковы принципы деятельности ФСБ России?

18. Перечислите направления деятельности органов федеральной службы безопасности?

19. Какие вопросы в области государственной безопасности курирует ФСТЭК России?

20. При каких обстоятельствах ФСБ России осуществляет деятельность по обеспечению информационной безопасности в соответствии с Федеральным законом от 3 апреля 1995 г. № 40-ФЗ?

21. Определите основные задачи ФСТЭК России в соответствии с «Положением о федеральной службе по техническому и экспортному контролю» (утв. Указом Президента Российской Федерации от 16 августа 2004 г. № 1085)?

22. Федеральным органом какой ветви власти является ФСТЭК России?

23. Какие полномочия осуществляет ФСТЭК России?

24. На что имеет право ФСТЭК России в целях реализации своих полномочий?

25. Какова процедура назначения директора ФСТЭК России? Его полномочия?

Практическая работа 3.1. Полномочия органов государственной власти Российской Федерации в области защиты информации

Цель работы: изучить основные задачи, функции, состав и структуру государственных органов в области защиты информации.

Порядок выполнения работы

1. Изучить теоретический материал темы 3 «Государственные органы в области защиты информации» настоящего учебного пособия.
2. Выполнить задания практической части.
3. Представить оформленный отчет преподавателю. Отчет должен содержать номера пунктов работы, их наименование и (в правой колонке) результат выполнения каждого пункта.

Задания

1. Изучить основные задачи, функции, состав и структуру *Комитета Государственной Думы по безопасности и противодействию коррупции*.

1. Создайте файл отчета в MS Word по образцу, приведенному в приложении. Сохраните файл под именем «Ваша фамилия31» (например: Иванов31). Заполните его шапку.

2. Перейдите на сайт Комитета Государственной Думы по безопасности и противодействию коррупции, для чего:

— выйдите в Интернет на страницу http://komitet2-16.km.duma.gov.ru/ (рис. 3.1.1);

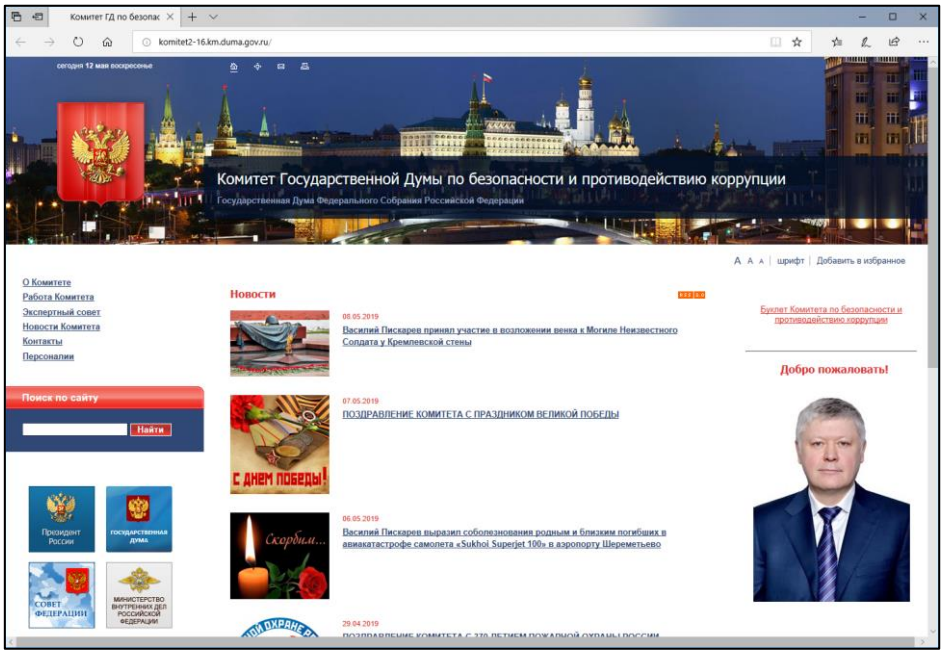


Рис. 3.1.1. **Сайт Комитета ГД по безопасности и противодействию коррупции http://komitet2-16.km.duma.gov.ru/**

Зафиксируйте копию данной страницы в своем отчете.

3. Перейдите по ссылке *О комитете* (рис. 3.1.1), занесите в отчет информацию о председателе комитета и его заместителях.

4. Ознакомьтесь с положением и вопросами ведения комитета (рис. 3.1.2). Внесите в отчет *Вопросы ведения Комитета*.

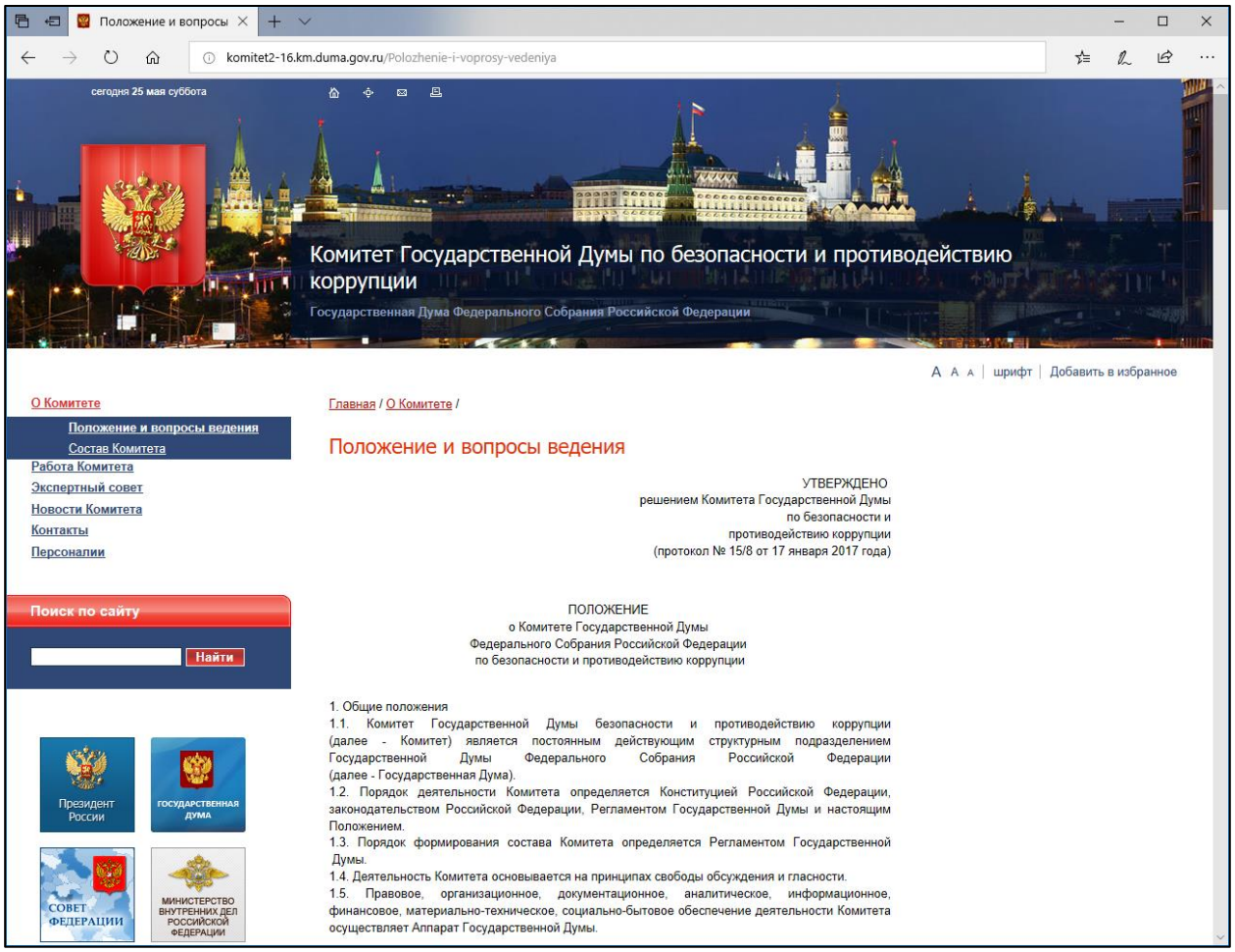


Рис. 3.1.2. **Сайт Комитета ГД по безопасности и противодействию коррупции/О Комитете http://komitet2-16.km.duma.gov.ru/Polozhenie-i-voprosy-vedeniya**

5. Перейдите по ссылке *Работа Комитета* (http://komitet2-16.km.duma.gov.ru/Zakonoproekty-nahodyashhiesya-na-rassmot). Занесите в отчет количество законопроектов, находящиеся на рассмотрении в Комитете.

6. Отобразите в отчете информацию о законопроекте (законе) № 2, находящемся на рассмотрении в Комитете:

– наименование законопроекта, закона;
– дата внесения;
– субъект права законодательной инициативы;
– форма законопроекта;
– ответственный комитет;
– отрасль законодательства;
– тематический блок законопроектов;

– профильный комитет.

7. Занесите в отчет количество законопроектов, подписанных Президентом РФ.

8. Отобразите в отчете информацию о законопроекте (законе) № 3, подписанном Президентом РФ:

– наименование законопроекта, закона;

– дата внесения;

– субъект права законодательной инициативы;

– форма законопроекта;

– комитеты-соисполнители;

– отрасль законодательства;

– тематический блок законопроектов;

– профильный комитет.

8. Занесите в отчет количество законопроектов, работа над которыми завершена.

9. Отобразите в отчете информацию о законопроекте (законе) № 1, работа над которыми завершена:

– наименование законопроекта, закона;

– дата внесения;

– субъект права законодательной инициативы;

– последнее событие;

– форма законопроекта.

2. Изучить основные задачи, функции, состав и структуру *Совета Безопасности Российской Федерации*.

1. Перейдите на сайт Совет Безопасности Российской Федерации, для чего:

— выйдите в Интернет на страницу http://www.scrf.gov.ru/ (рис. 3.1.3);

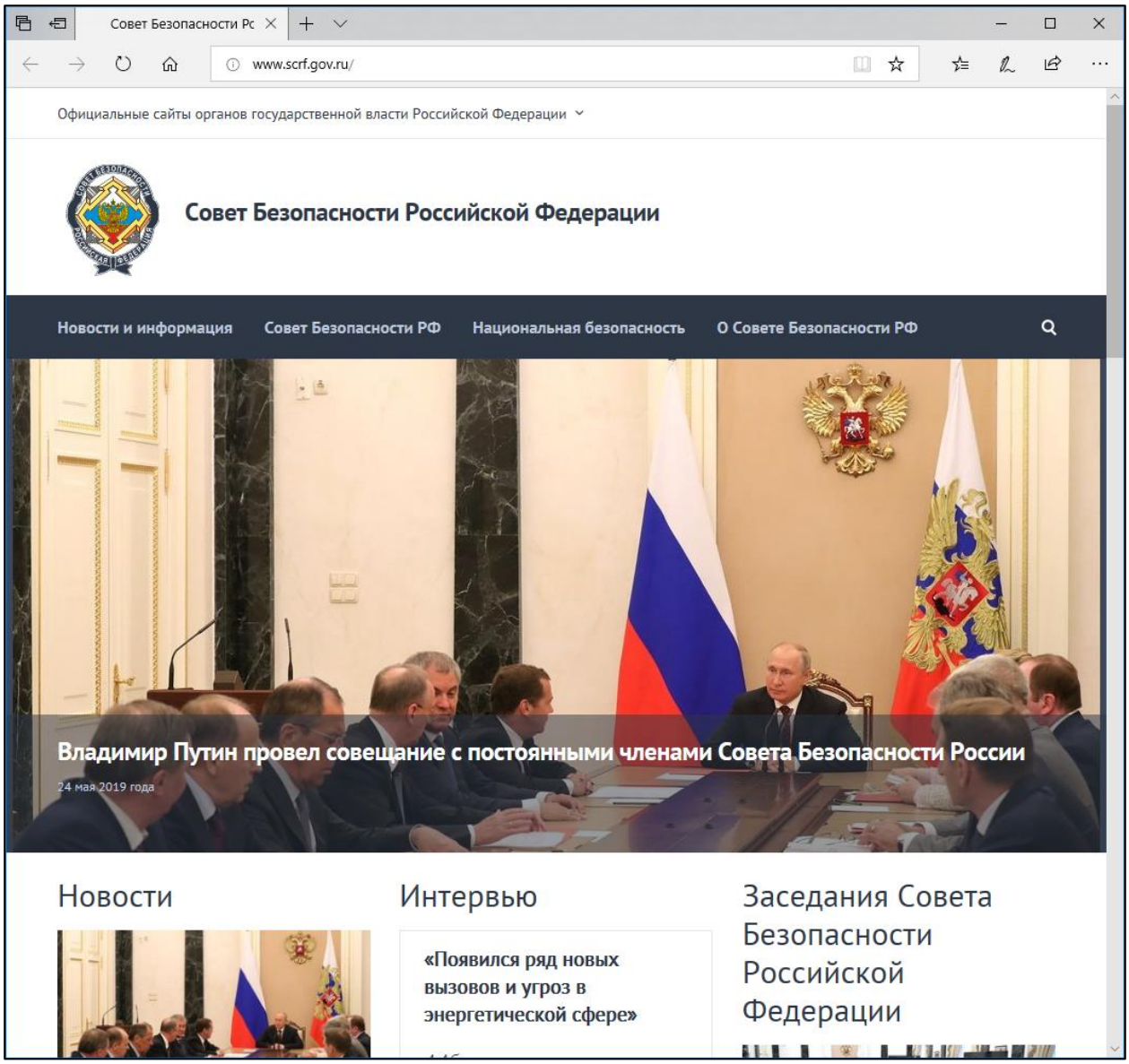


Рис. 3.1.3. **Сайт Совета Безопасности РФ http://www.scrf.gov.ru/**

Зафиксируйте копию данной страницы в своем отчете.

2. Перейдите по ссылке *Совет Безопасности РФ* (рис. 3.1.3), занесите в отчет информацию о председателе и постоянных членах Совета Безопасности Российской Федерации.

3. Перейдите по ссылке *О Совете Безопасности РФ* (рис. 3.1.3), ознакомьтесь с историей создания Совета Безопасности. Занесите в отчет основные направления деятельности Совета Безопасности Российской Федерации.

4. Перейдите по ссылке *Национальная безопасность* (рис. 3.1.3), затем по ссылке Информационная безопасность (3.1.4).

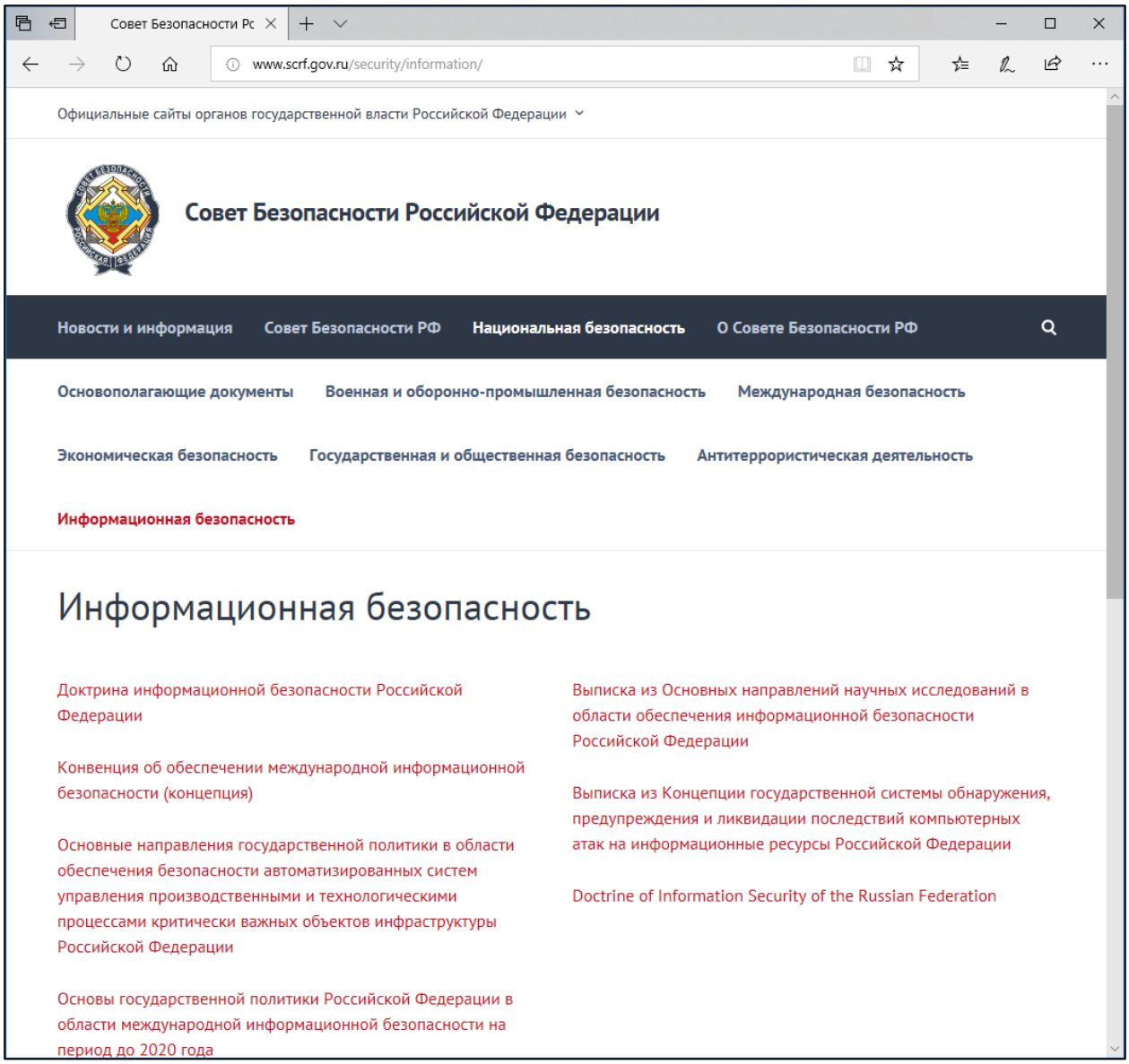


Рис. 3.1.4. **Сайт Совета Безопасности РФ / Национальная безопасность / Информационная безопасность http://www.scrf.gov.ru/security/information/**

5. Ознакомьтесь с основными направлениями государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов (КВО) инфраструктуры Российской Федерации (рис. 3.1.4). Внесите в отчет ответ на вопрос: *по каким направлениям должно осуществляться решение основных задач государственной политики в области обеспечения безопасности автоматизированных систем управления КВО?*

3. Изучить основные задачи, функции, состав и структуру *Службы внешней разведки Российской Федерации* (СВР России).

1. Перейдите на сайт Службы внешней разведки Российской Федерации, для чего:

— выйдите в Интернет на страницу http://svr.gov.ru/ (рис. 3.1.5);

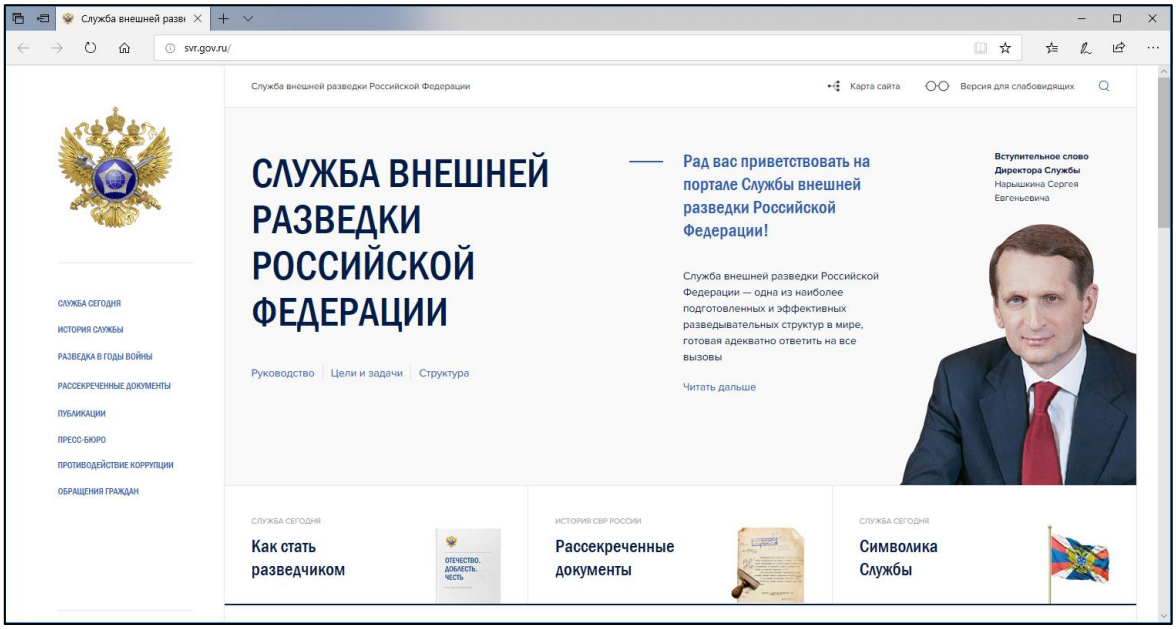


Рис. 3.1.5. **Сайт СВР России, http://svr.gov.ru/**

Зафиксируйте копию данной страницы в своем отчете.

2. Перейдите по ссылке *СЛУЖБА СЕГОДНЯ* (рис. 3.1.5), занесите в отчет информацию о Директоре Службы внешней разведки РФ.

3. Ознакомьтесь со структурой и руководством Службы внешней разведки РФ. Внесите в отчет *схему структуры СВР России*, перейдя по ссылке http://svr.gov.ru/svr_today/struktur.htm (рис. 3.1.6).

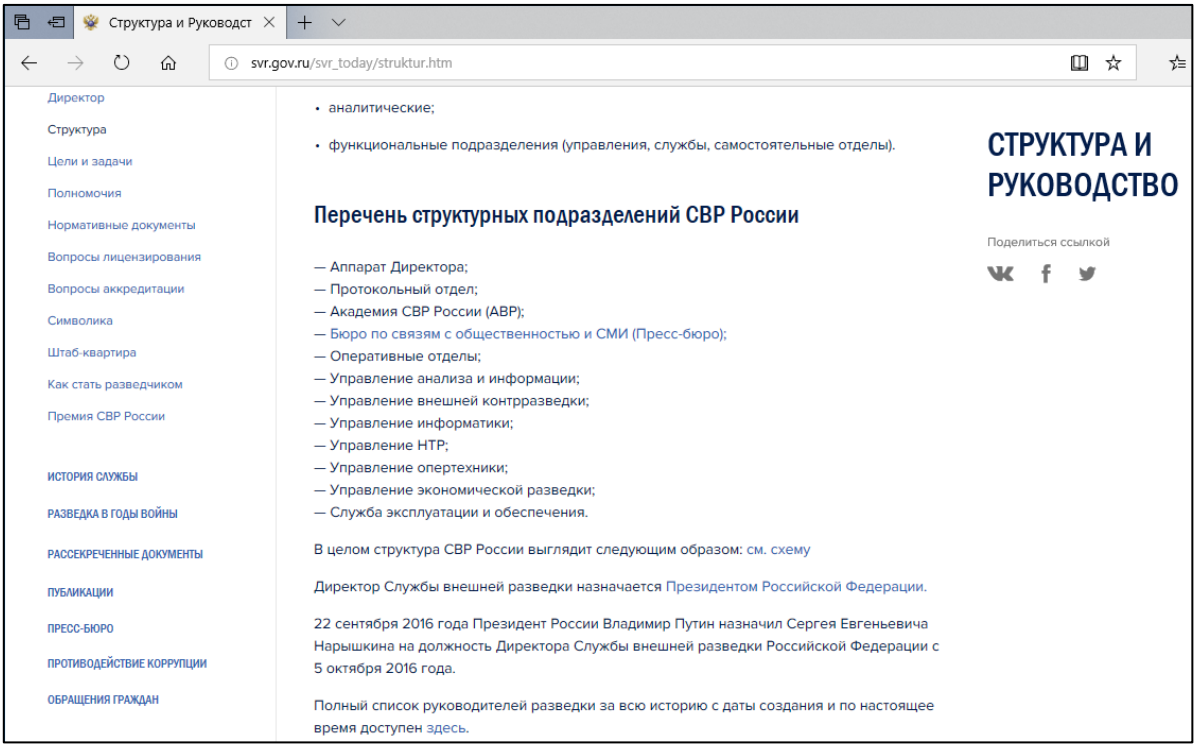


Рис. 3.1.6. **Сайт СВР России / Служба сегодня / Структура и Руководство http://svr.gov.ru/svr_today/struktur.htm**

4. Перейдите по ссылке *Цели и задачи* (рис. 3.1.6). Занесите в отчет цели разведывательной деятельности СВР России.

5. Перейдите по ссылке *Нормативные документы* (рис. 3.1.6). Ознакомьтесь с перечнем нормативных документов, регулирующих деятельность СВР России, которые могут быть опубликованы.

6. Откройте текст Закона РФ от 21.07.1993 № 5485-1 «О государственной тайне», перейдя по соответствующей ссылке (рис. 3.1.7).

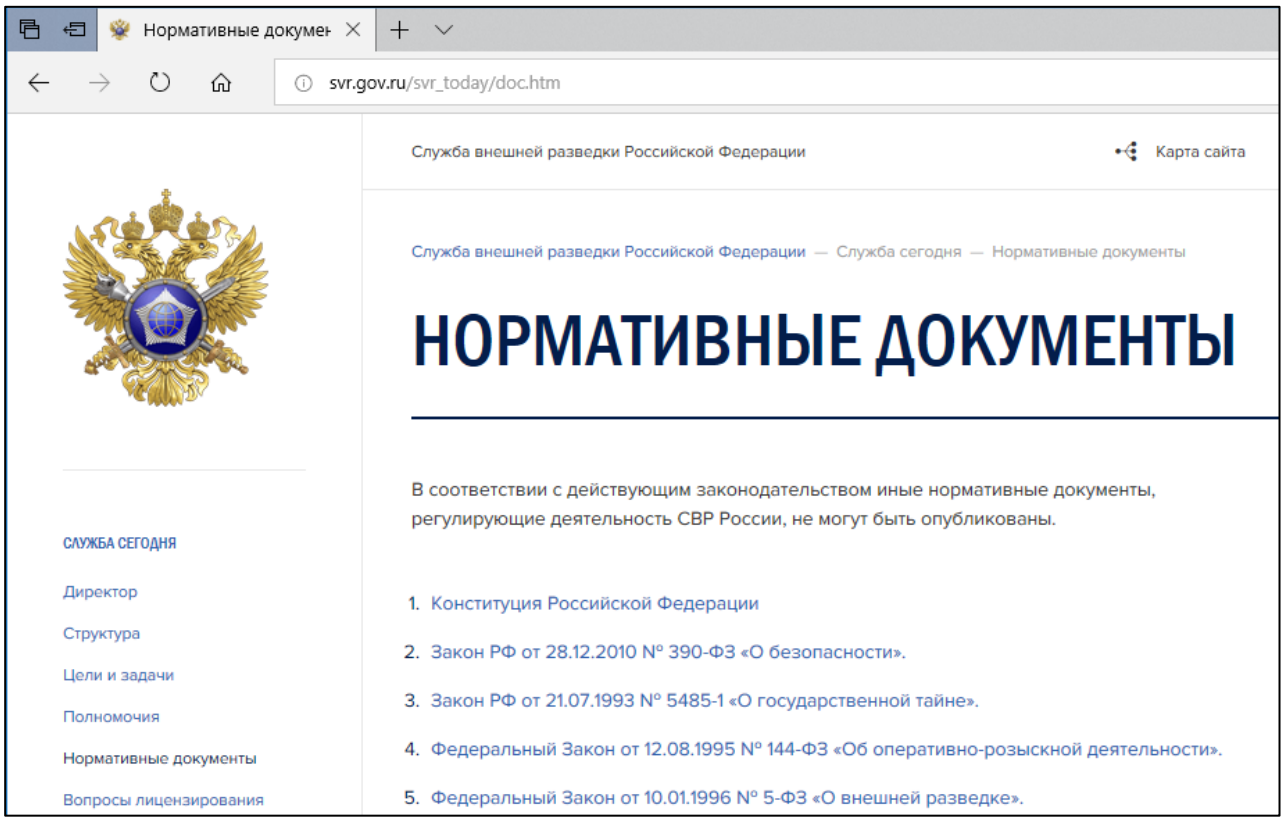


Рис. 3.1.6. **Сайт Службы внешней разведки Российской Федерации / Служба сегодня / Нормативные документы http://svr.gov.ru/svr_today/doc.htm**

7. Занесите в отчет определения следующих понятий, используемых в Законе РФ «О государственной тайне»:

– государственная тайна;

– система защиты государственной тайны;

– средства защиты информации.

4. Изучить основные задачи, функции, состав и структуру *Министерства обороны Российской Федерации* (Минобороны России).

1. Перейдите на сайт Министерства обороны Российской Федерации, для чего:

— выйдите в Интернет на страницу http://mil.ru/ (рис. 3.1.7);

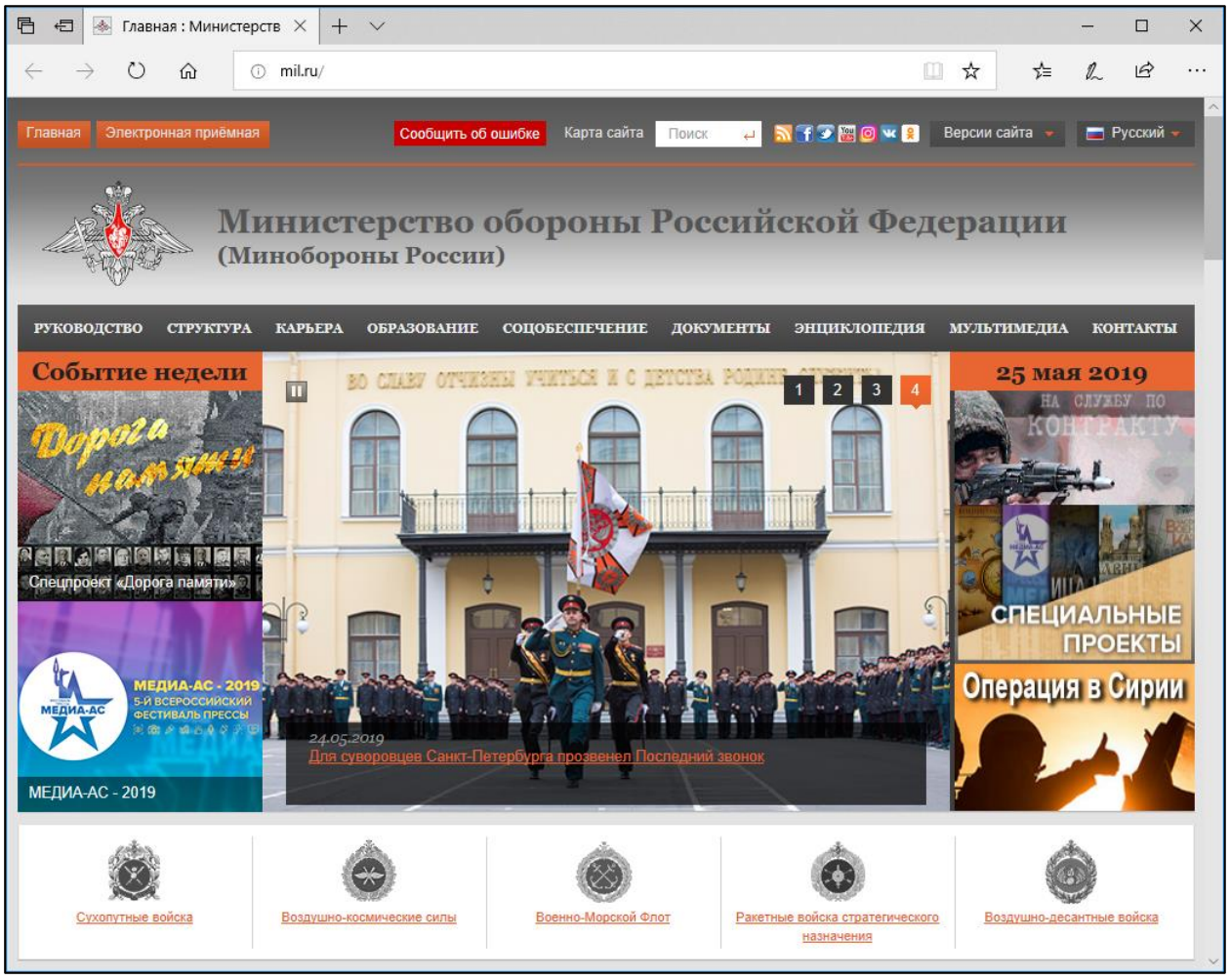


Рис. 3.1.7. **Сайт Министерства обороны Российской Федерации http://mil.ru/**

Зафиксируйте копию данной страницы в своем отчете.

3. Перейдите по ссылке *Руководство* (рис. 3.1.7), занесите в отчет информацию о заместителях Министра обороны РФ и их полномочиях.

4. Перейдите по ссылке *Документы* (рис. 3.1.7). Затем по ссылке *Международные договоры Российской Федерации, составляющие основу международного гуманитарного права* (рис. 3.1.8).

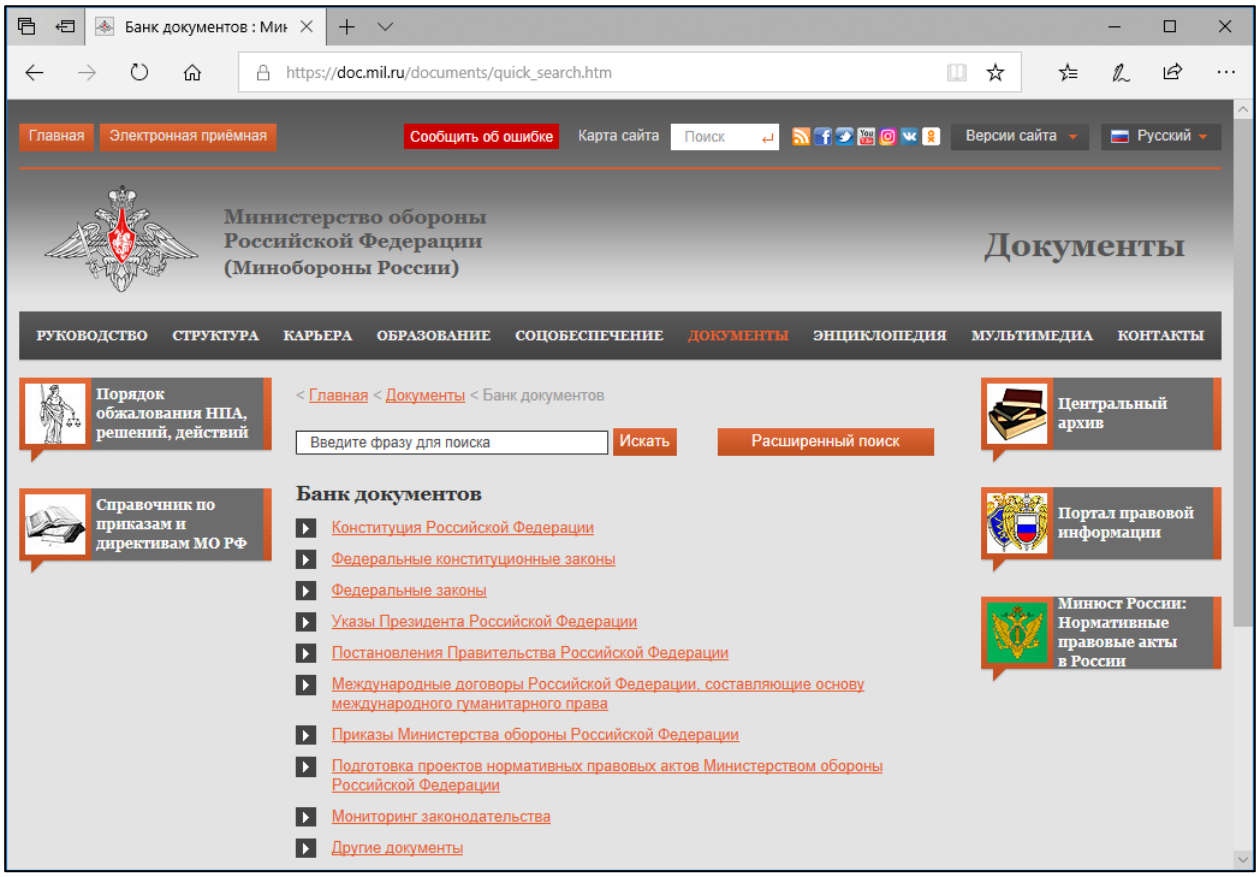


Рис. 3.1.8. **Сайт Министерства обороны Российской Федерации / Документы https://doc.mil.ru/documents/quick_search.htm**

5. Откройте *Устав Организации Объединенных Наций 1945 года*. Занесите в отчет цели Организация Объединенных Наций (ООН), а также перечень главных органов, которые учреждены ООН.

5. Изучить основные задачи, функции, состав и структуру *Министерства внутренних дел Российской Федерации* (МВД России).

1. Перейдите на сайт Министерства внутренних дел Российской Федерации, для чего:

— выйдите в Интернет на страницу https://мвд.рф/ (рис. 3.1.9).

Зафиксируйте копию данной страницы в своем отчете.

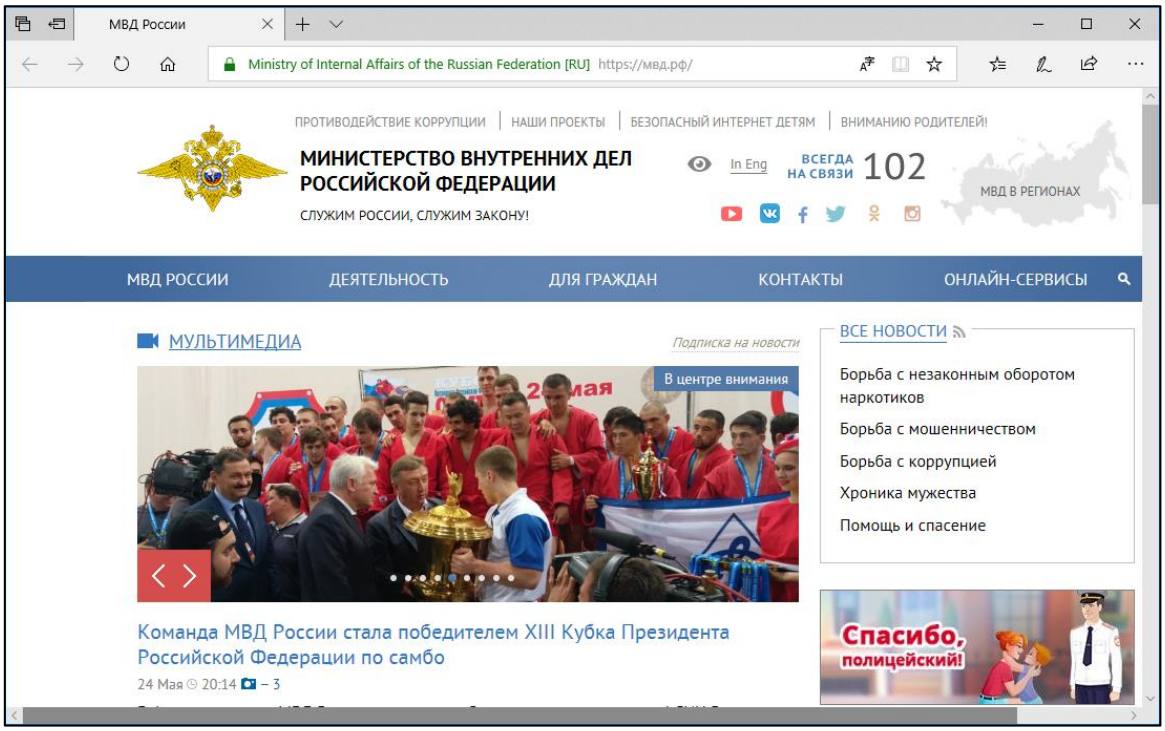


Рис. 3.1.9. **Сайт Министерства внутренних дел Российской Федерации, https://мвд.рф**

2. Перейдите по ссылке *МВД России / Структура Министерства* (рис. 3.1.10), занесите в отчет информацию о руководстве.

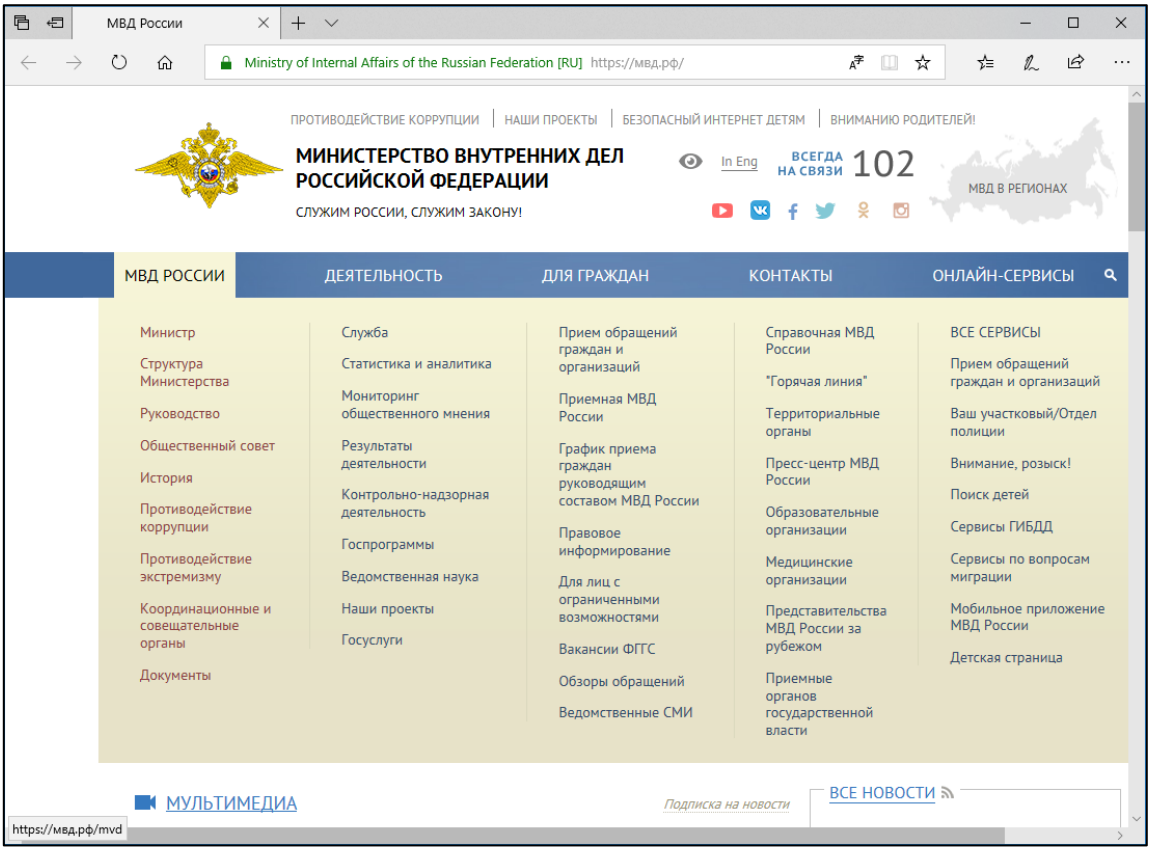


Рис. 3.1.10. **Сайт Министерства внутренних дел Российской Федерации / МВД России, https://мвд.рф**

3. Внесите в отчет *схему структуры МВД России*, перейдя по ссылке https://media.mvd.ru/files/embed/961570.

4. Перейдите по ссылке *Деятельность / Служба* (рис. 3.1.10). Затем перейдите по ссылке *Законодательная база* (рис. 3.1.11). *Зафиксируйте копию страницы с документами в своем отчете.*

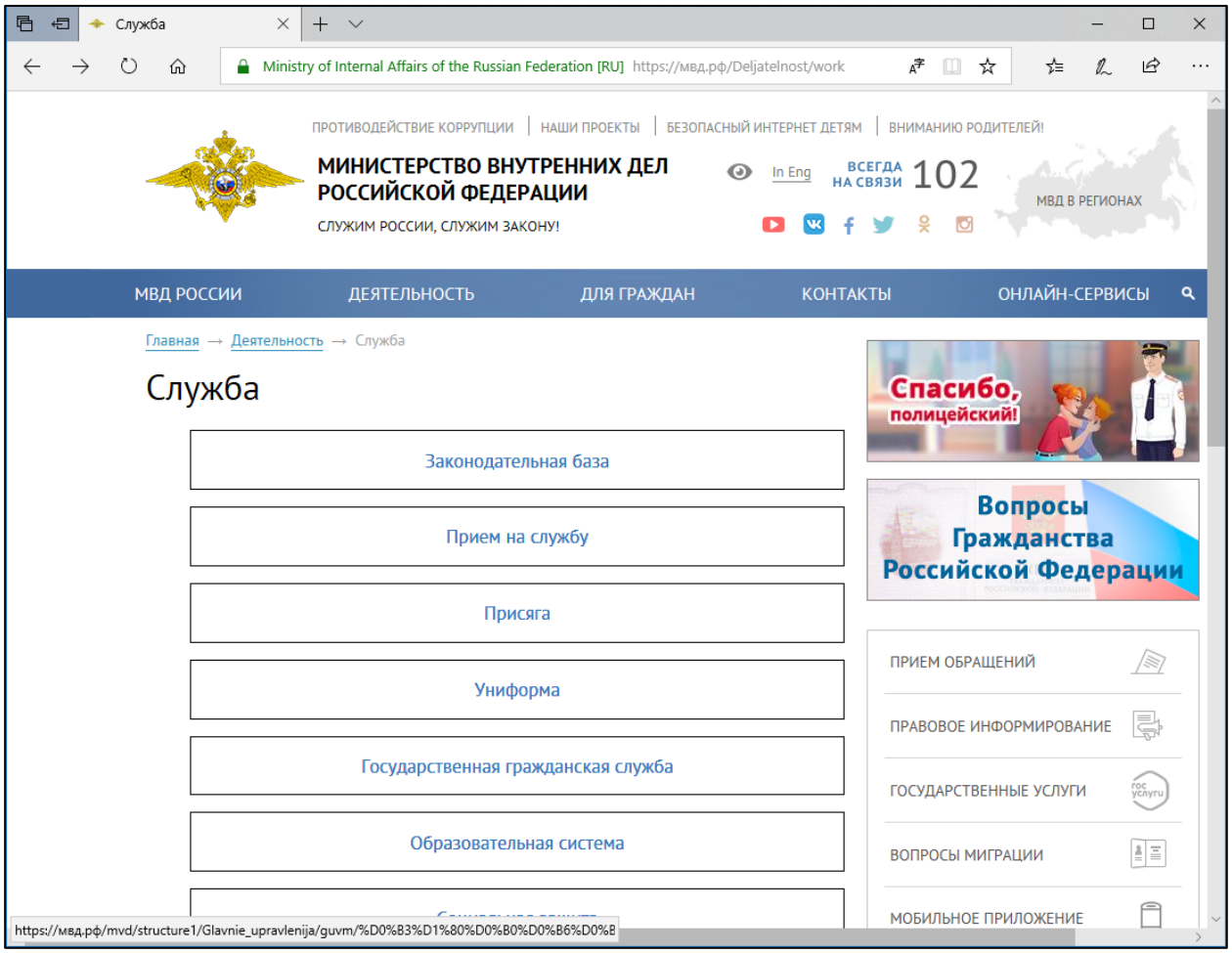


Рис. 3.1.11. **Сайт Министерства внутренних дел Российской Федерации / Детальность / Служба https://мвд.рф/Deljatelnost/work**

5. Откройте текст Федерального закона от 7 февраля 2011 года № 3-ФЗ «О полиции», перейдя по соответствующей ссылке.

6. Занесите в отчет содержание Ст. 1. Назначение полиции Федерального закона «О полиции».

7. Занесите в отчет содержание Ст. 2. Основные направления деятельности полиции Федерального закона «О полиции».

6. Изучить основные задачи, функции, состав и структуру *Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций* (Роскомнадзора).

1. Перейдите на сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, для чего:

— выйдите в Интернет на страницу https://rkn.gov.ru/ (рис. 3.1.12);

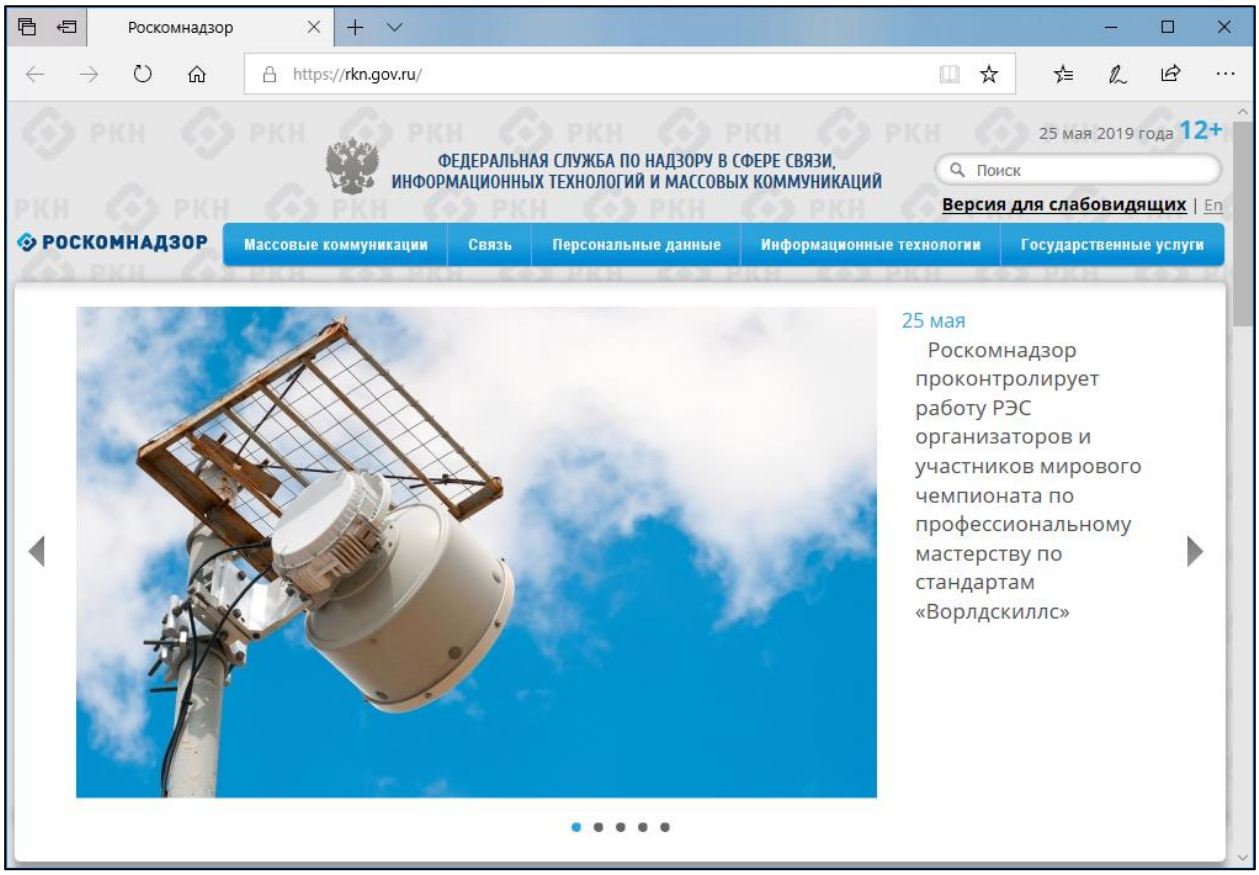


Рис. 3.1.12. **Сайт Роскомнадзора https://rkn.gov.ru/**

Зафиксируйте копию данной страницы в своем отчете.

2. Перейдите по ссылке *Массовые коммуникации* / *О Роскомнадзоре* (рис. 3.1.13). Затем откройте *Положение о Роскомнадзоре*, в отчет занесите ответ на вопрос: в каких сферах осуществляет государственный контроль и надзор Роскомнадзор?

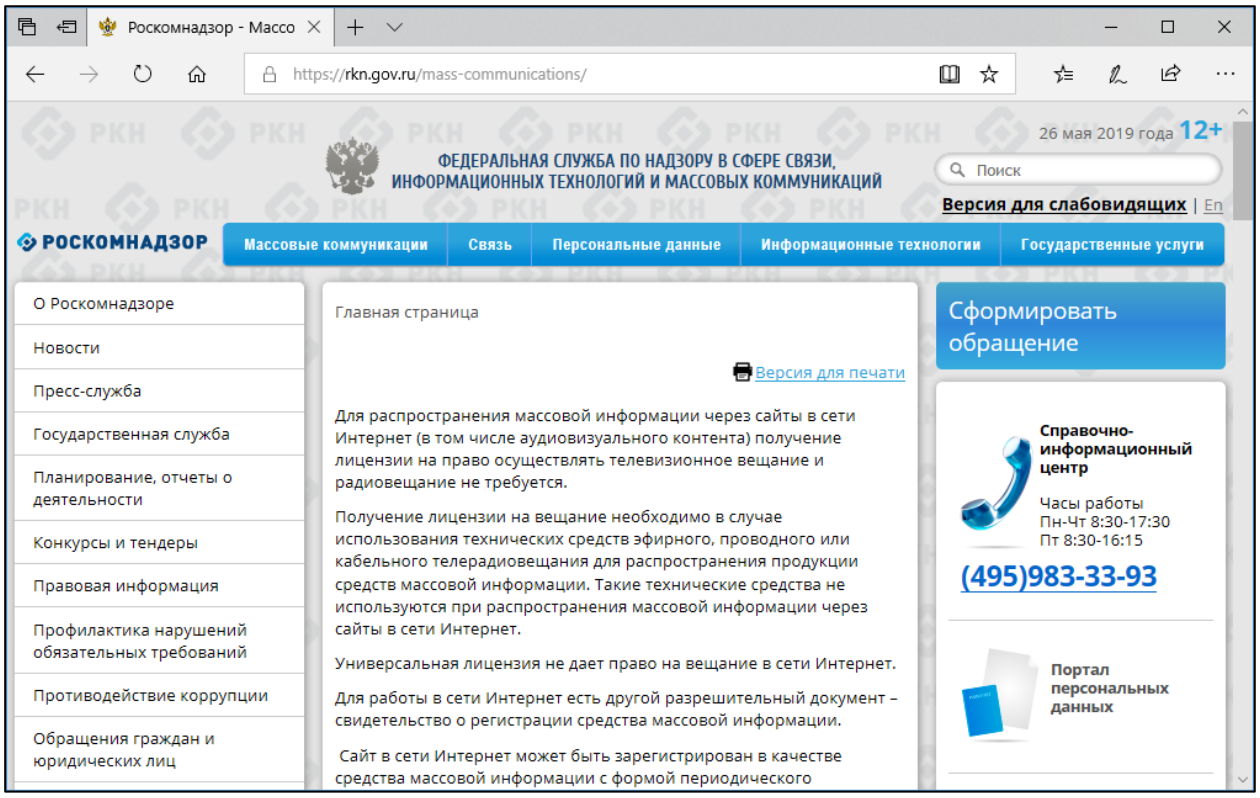


Рис. 3.1.13. **Сайт Роскомнадзора / Массовые коммуникации https://rkn.gov.ru/mass-communications/**

3. Перейдите по ссылке *Руководство* (рис. 3.1.14), занесите в отчет информацию о руководителе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций и его заместителях.

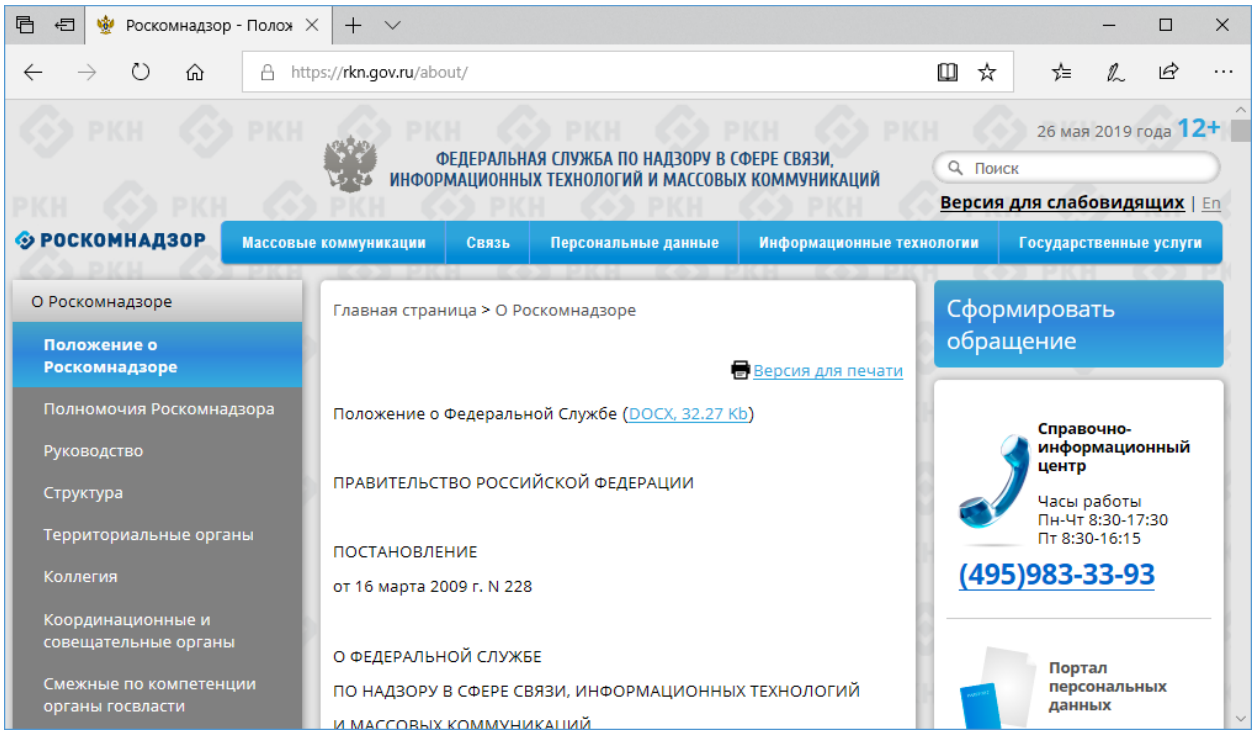


Рис. 3.1.14. **Сайт Роскомнадзора / О Роскомнадзоре https://rkn.gov.ru/about/**

4. Перейдите по ссылке *Структура* (рис. 3.1.14). Занесите в отчет структурную схему Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

5. Перейдите по ссылке *Информационные технологии* / *Контроль и надзор* (рис. 3.1.15), занесите в отчет информацию о контрольно-надзорных функциях осуществляемых Роскомнадзора в сфере информационных технологий.

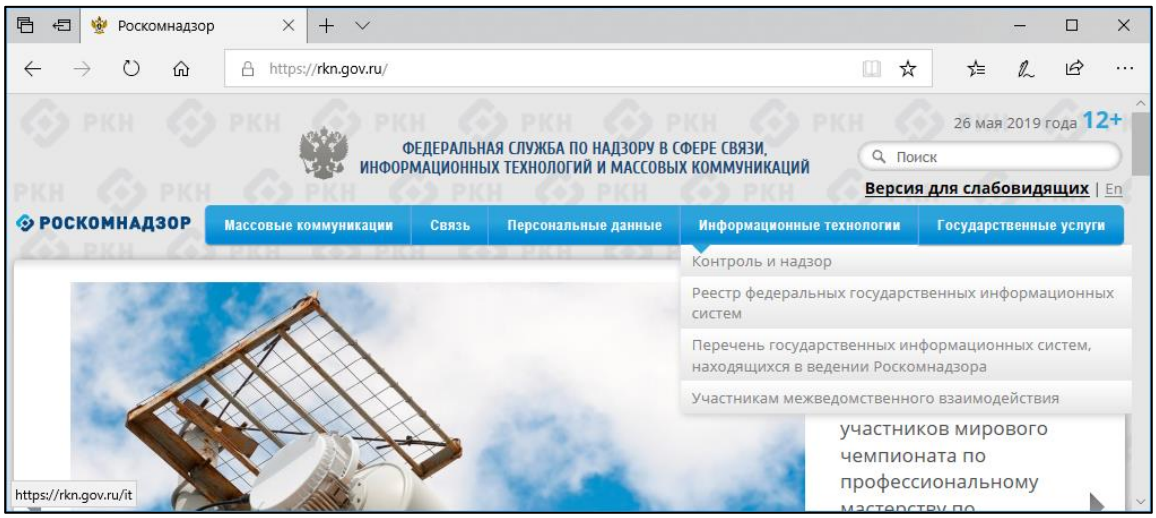


Рис. 3.1.15. **Сайт Роскомнадзора / Информационные технологии https://rkn.gov.ru/**

6. Перейдите по ссылке *Персональные данные* / *Реестр операторов персональных данных* (рис. 3.1.16).

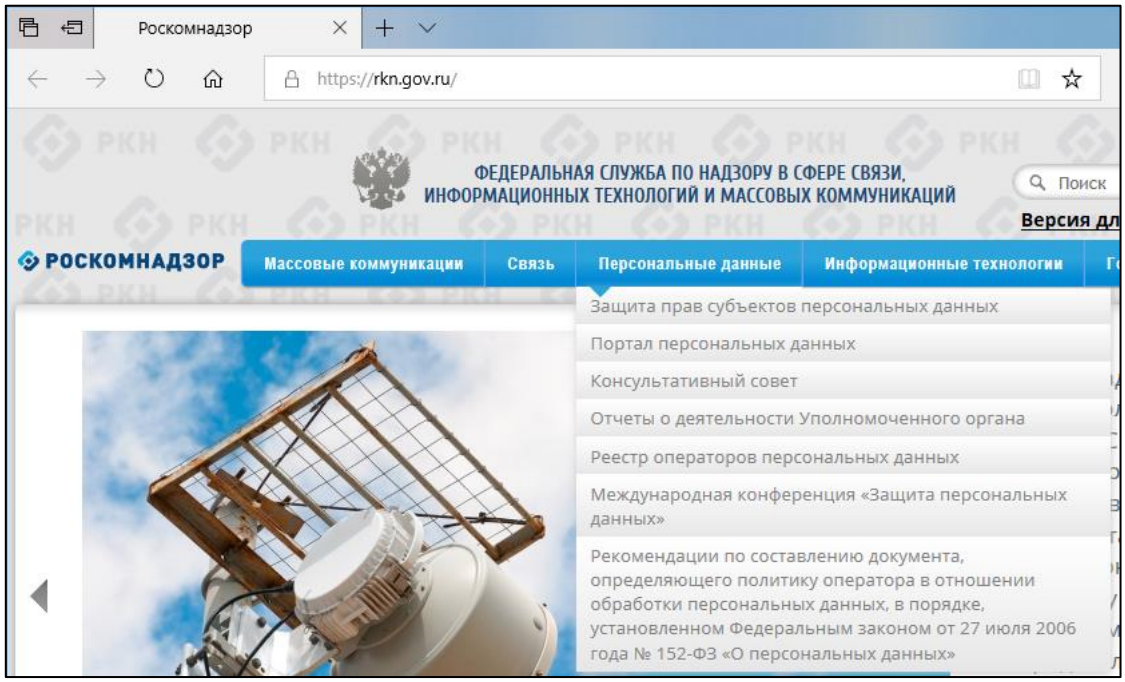


Рис. 3.1.16. **Сайт Роскомнадзора / Персональные данные https://rkn.gov.ru/**

Зафиксируйте копию открывшейся страницы в своем отчете.

7. Найдите в реестре операторов, осуществляющих обработку персональных данных, информацию о своей учебной организации. Для поиска информации о Российском университете транспорта достаточно в поле *Организация* ввести МИИТ.

8. Отобразите в отчете информацию о найденном операторе персональных данных:

– регистрационный номер;

– наименование оператора / ИНН;

– тип оператора;

– основание внесения оператора в реестр;

– дата регистрации уведомления;

– дата начала обработки персональных данных;

– адрес местонахождения;

– субъекты РФ, на территории которых происходит обработка персональных данных;

– цель обработки персональных данных;

– правовое основание обработки персональных данных;

– срок или условие прекращения обработки персональных данных;

– дата и основание внесения записи в реестр;

– категории персональных данных;

– категории субъектов, персональные данные которых обрабатываются;

– перечень действий с персональными данными;

– обработка персональных данных;

– трансграничная передача.

7. Изучить основные задачи, функции, состав и структуру *Федеральной службы безопасности* (ФСБ России).

1. Перейдите на сайт Федеральной службы безопасности, для чего:

— выйдите в Интернет на страницу http://www.fsb.ru/ (рис. 3.1.17);

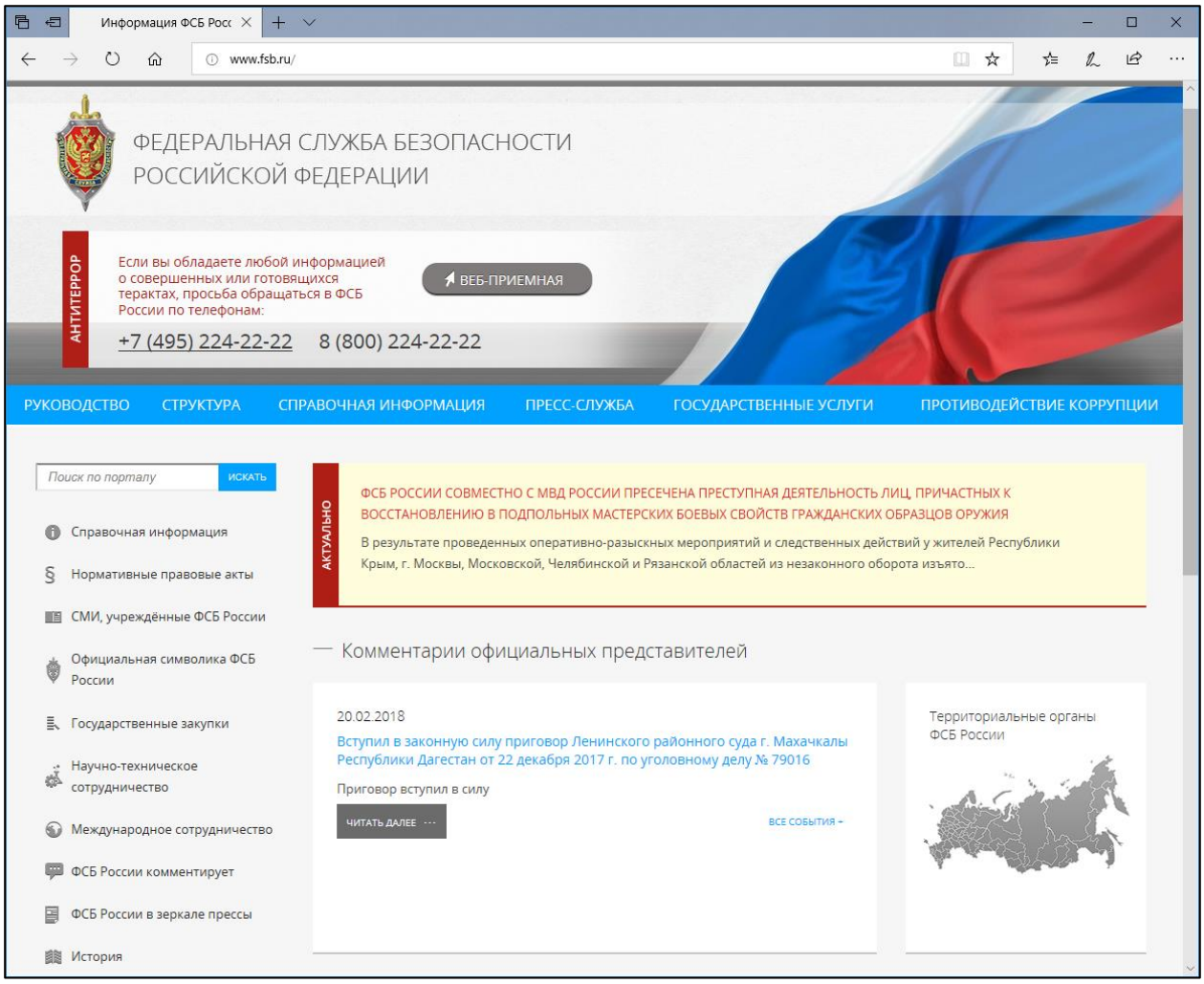


Рис. 3.1.17. **Сайт Федеральной службы безопасности http://www.fsb.ru/**

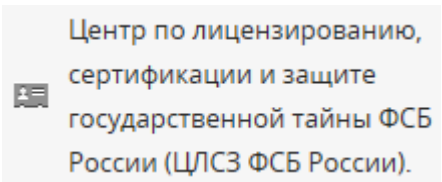
Зафиксируйте копию данной страницы в своем отчете.

2. Перейдите по ссылке *Руководство* (рис. 3.1.17), занесите в отчет информацию о директоре Федеральной службы безопасности Российской Федерации и его заместителях.

3. Перейдите по ссылке *История* (рис. 3.1.17), занесите в отчет информацию об истории создания ФСБ России.

4. Перейдите по ссылке *Структура* (рис. 3.1.17), занесите в отчет структурную схему органов федеральной службы безопасности.

5. Перейдите по ссылке *Справочная информация* (рис. 3.1.17), изучите информацию о способах связи с ФСБ России. Отобразите в своем отчете ответ на вопрос: какие обращения граждан рассматриваются следственным управлением ФСБ России?

6. Перейдите по ссылке 

. *Зафиксируйте копию открывшейся страницы в своем отчете*.

7. Перейдите по ссылке *Лицензирование* (рис. 3.1.18), отобразите в своем отчете ответ на вопрос: по каким видам деятельности юридических лиц и индивидуальных предпринимателей осуществляют лицензирование ЦЛСЗ ФСБ России и территориальные органы безопасности?

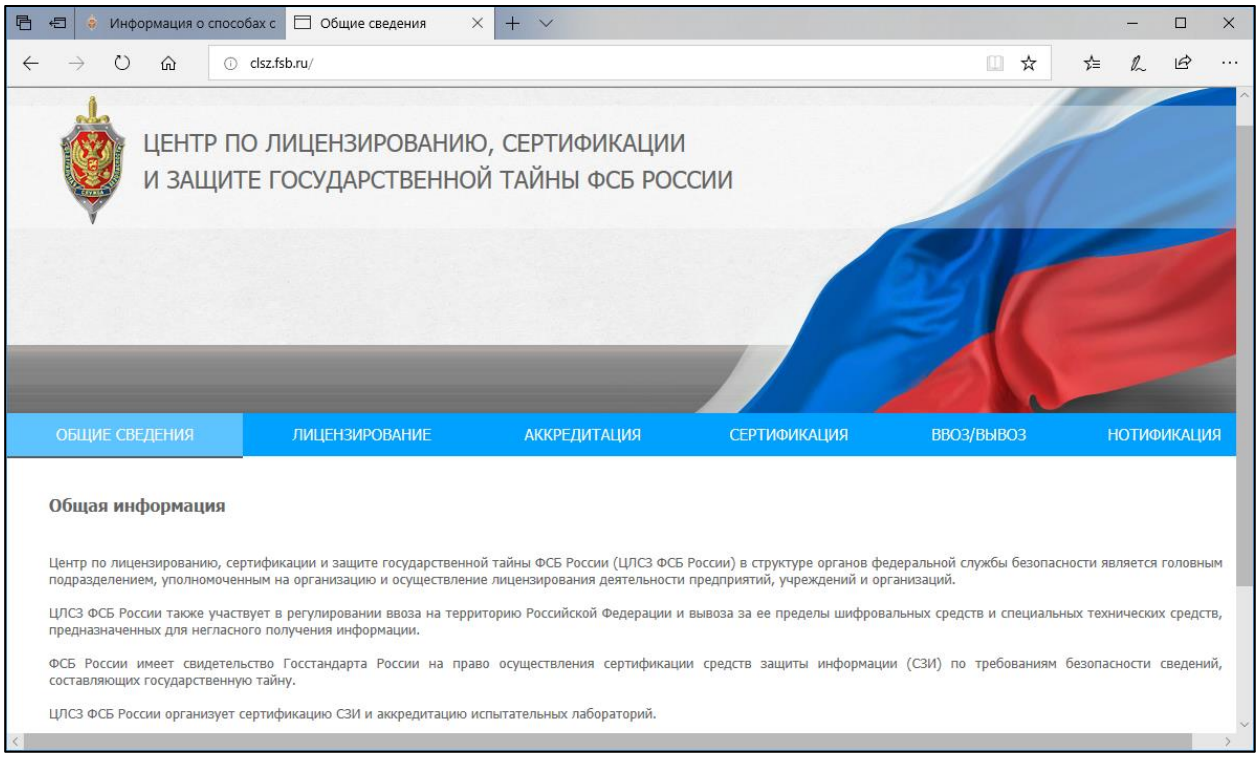


Рис. 3.1.18. **Сайт Центра по лицензированию, сертификации и защите государственной тайны ФСБ России (ЦЛСЗ ФСБ России) http://clsz.fsb.ru/**

8. Перейдите по ссылке *Аккредитация* (рис. 3.1.18), отобразите в своем отчете ответ на вопрос: в соответствии с какими нормативными документами осуществляется аккредитация?

9. Перейдите по ссылке *Сертификация* (рис. 3.1.18). Затем скачайте файл под именем «*Перечень средств защиты информации, сертифицированных ФСБ России*». Отобразите в своем отчете информацию о средстве СФ/СЗИ-0023:

– срок действия сертификата соответствия;
– условное наименование (индекс);
– выполняемая функция;
– изготовитель.

10. Перейдите по ссылке *Ввоз/ввоз* (рис. 3.1.18), изучите общую информацию по ввозу/вывозу. *Зафиксируйте копию экрана в своем отчете*.

11. Перейдите по ссылке *Нотификация* (рис. 3.1.18), изучите общую информацию по нотификации. *Зафиксируйте копию экрана в своем отчете*.

8. Изучить основные задачи, функции, состав и структуру *Федеральной службы по техническому и экспортному контролю* (ФСТЭК России).

1. Перейдите на сайт Федеральной службы по техническому и экспортному контролю, для чего:

— выйдите в Интернет на страницу https://fstec.ru/ (рис. 3.1.19);

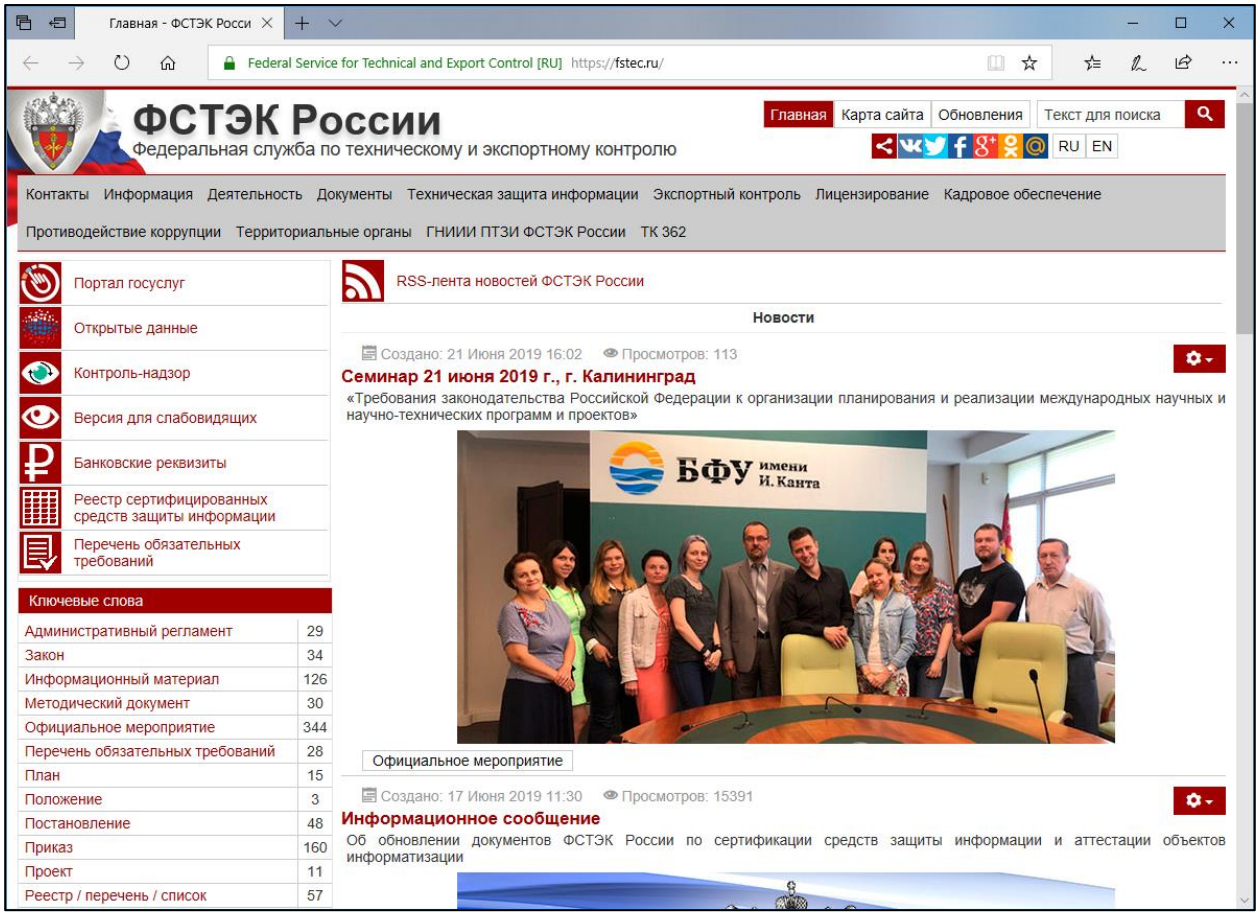


Рис. 3.1.19. **Сайт Федеральной службы по техническому и экспортному контролю https://fstec.ru/**

Зафиксируйте копию данной страницы в своем отчете.

2. Перейдите по ссылке *Информация* (рис. 3.1.19), затем по ссылке *Структура*. Занесите в отчет информацию о Структуре ФСТЭК России.

3. Отобразите в своем отчете ответы на вопросы:

– Кто осуществляет руководство деятельностью ФСТЭК России?

– Кому подведомственна ФСТЭК России?

– Какие органы государственной власти подведомственны ФСТЭК России?

– Имеются ли представительства ФСТЭК России за рубежом?

4. Занесите в отчет информацию о составе коллегии ФСТЭК России.

5. Перейдите по ссылке *Информация / Полномочия* (рис. 3.1.19), занесите в отчет перечень вопросов, по которым ФСТЭК России осуществляет реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности.

6. Перейдите по ссылке *Деятельность / Государственные функции и услуги* (рис. 3.1.19), занесите в отчет сведения о государственных функциях (услугах), исполняемых (предоставляемых) ФСТЭК России.

7. Перейдите по ссылке *Документы / Поиск по документам* (рис. 3.1.20), изучите представленный список административных регламентов, Законов, информационных и аналитических материалов и пр. *Зафиксируйте копию данной страницы в своем отчете*.

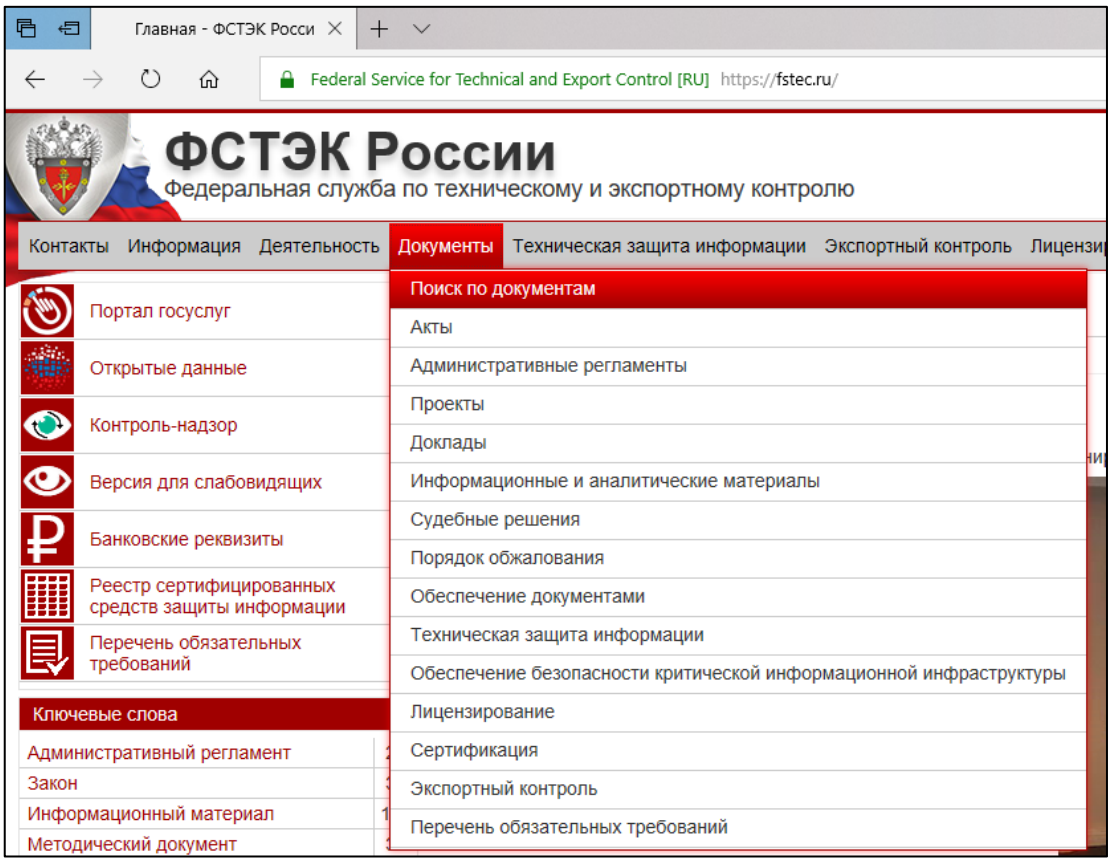
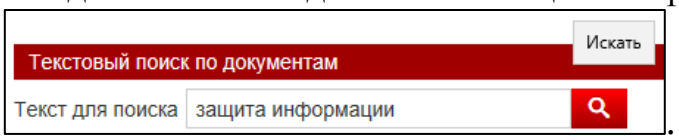


Рис. 3.1.20. **Сайт ФСТЭК России / Документы**

8. В поле для поиска введите текст: защита информации, затем нажмите искать 

. *Зафиксируйте копию открывшейся страницы в своем отчете*.

9. Перейдите по ссылке Федеральный закон от 18 июля 1999 г. N 183-ФЗ.

10. Изучите основные понятия и положения Федерального закона об экспортном контроле.

11. Ответьте на вопросы для изучения в файле отчета. Номера вопросов определяются по начальной букве фамилии студента (табл. 3.1.1).

Таблица 3.1.1

Варианты к работе 3.1

Начальная буква фамилии студента	Номера вопросов	Начальная буква фамилии студента	Номера вопросов
А, И, С, Щ	1, 9, 17, 25	Д, Н, Х	5, 13, 21, 29
Б, К, Т	2, 10, 18, 26	Е, О, Ц, Ю	6, 14, 22, 30
В, Л, У, Э	3, 11, 19, 27	Ж, П, Ч	7, 15, 23, 31
Г, М, Ф	4, 12, 20, 28	З, Р, Ш, Я	8, 16, 24, 32

12. Представьте оформленный отчет по выполненной работе преподавателю на проверку.

Вопросы для изучения

1. Какие принципы устанавливает Федеральный закон об экспортном контроле?
2. Составьте список изменяющих документов устанавливает Федеральный закон об экспортном контроле?
3. Дайте определение понятию «внешнеэкономическая деятельность».
4. Дайте определение понятию «экспортный контроль».
5. Дайте определение понятию «внутренняя программа экспортного контроля».
6. Дайте определение понятию «оружие массового поражения».
7. Дайте определение понятию «средства доставки».
8. Дайте определение понятию «продукция, являющаяся особо опасной в части подготовки и (или) совершения террористических актов».
9. Дайте определение понятию «контролируемые товары и технологии».
10. Дайте определение понятию «российские участники внешнеэкономической деятельности (российские лица)».
11. Дайте определение понятию «иностранные лица».
12. Дайте определение понятию «режим безлицензионного экспорта отдельных видов контролируемых товаров».
13. Какие отношения регулирует Федеральный закон об экспортном контроле?
14. Каковы основные цели экспортного контроля?
15. В соответствии с какими основными принципами формируется государственная политика в области экспортного контроля?
16. Каковы методы правового регулирования внешнеэкономической деятельности экспортного контроля в Российской Федерации?
17. Каковы полномочия президента Российской Федерации в области экспортного контроля?

18. Каковы полномочия правительства Российской Федерации в области экспортного контроля?

19. Каковы полномочия федеральных органов исполнительной власти, Государственной корпорации по атомной энергии «Росатом» и Государственной корпорации по космической деятельности «Роскосмос» в области экспортного контроля?

20. Какие органы в пределах своей компетенции оказывают содействие специально уполномоченному федеральному органу исполнительной власти в области экспортного контроля?

21. Каковы обязанности участников внешнеэкономической деятельности по предоставлению информации для целей экспортного контроля?

22. Каковы условия включения российских юридических лиц в реестр российских участников внешнеэкономической деятельности, которым разрешено осуществлять безлицензионный экспорт отдельных видов контролируемых товаров?

23. Какая деятельность запрещена российским лицам согласно ст. 20 Федерального закона от 18 июля 1999 г. N 183-ФЗ?

24. Каковы обязанности российских участников внешнеэкономической деятельности?

25. Каковы основания для отказа в выдаче лицензии или разрешения?

26. Кто может являться специалистом в области экспортного контроля?

27. В каких случаях может быть отозван квалификационный аттестат специалиста в области экспортного?

28. Каковы цели международного сотрудничества Российской Федерации в области экспортного контроля?

29. Посредством какой деятельности осуществляется международное сотрудничество Российской Федерации в области экспортного контроля?

30. Что является нарушением законодательства Российской Федерации в области экспортного контроля?

31. Какую ответственность несут должностные лица организаций и граждане, виновные в нарушении законодательства Российской Федерации в области экспортного контроля?

32. Какова ответственность организаций за нарушение законодательства Российской Федерации в области экспортного контроля?

Тема 4. Классификация факторов, воздействующих на безопасность защищаемой информации

Национальный стандарт Российской Федерации ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» устанавливает классификацию (табл. 4.1) и перечень факторов (рис. 4.1—4.3), воздействующих на безопасность защищаемой информации, в целях обоснования угроз безопасности информации[1] и требований по защите информации на объекте информатизации.

Стандарт ГОСТ Р 51275-2006 распространяется на объекты информатизации, создаваемые и эксплуатируемые в различных областях деятельности (обороны, экономики, науки и других областях).

Таблица 4.1

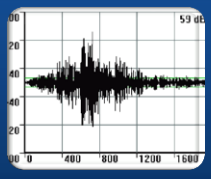
Классификация факторов, воздействующих на безопасность защищаемой информации в соответствии с ГОСТ Р 51275-2006

Объективные факторы		Субъективные факторы	
Внутренние (рис. 4.1)	Внешние	Внутренние (рис. 4.2)	Внешние (рис. 4.3)
— передача сигналов; — излучения сигналов; — электромагнитные излучения; — дефекты, сбои и отказы, аварии технических средств и пр.	— явления техногенного характера; — природные явления, стихийные бедствия.	— разглашение защищаемой информации лицами, имеющими к ней право доступа; — неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации; — недостатки организационного обеспечения защиты информации и пр.	— доступ к защищаемой информации с применением технических средств; — действия криминальных групп и отдельных преступных субъектов; — искажение, уничтожение или блокирование информации с применением технических средств и пр.

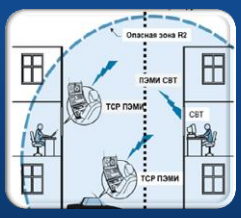
[1] *Угроза* (безопасности информации) — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [ГОСТ Р 50922-2006].

Под ***фактором, воздействующим на защищаемую информацию***, понимается явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

Передача сигналов:
- по проводным линиям связи;
- по оптико-волоконным линиям связи;
- в диапазоне радиоволн и в оптическом диапазоне длин волн.



Излучения сигналов, функционально присущие техническим средствам (ТС) объектов информатизации (ОИ):
- излучения акустических сигналов;
- электромагнитные излучения и поля.



Побочные электромагнитные излучения:
- элементов ТС обработки и передачи информации (ОПИ);
- на частотах работы высокочастотных генераторов устройств, входящих в состав ТС ОПИ;
- на частотах самовозбуждения усилителей, входящих в состав технических средств обработки и передачи информации.

Паразитное электромагнитное излучение:
-модуляция паразитного электромагнитного излучения информационными сигналами;
- модуляция паразитного электромагнитного излучения акустическими сигналами.

Наводка:
- в электрических цепях ТС, имеющих выход за пределы ОИ;
- в линиях связи;
- в цепях электропитания;
- в цепях заземления;
- в технических средствах, проводах, кабелях и иных токопроводящих коммуникациях и конструкциях, гальванически не связанных с ТС ОИ, вызванная побочными и (или) паразитными электромагнитными излучениями, несущими информацию.

Наличие акустоэлектрических преобразователей в элементах ТС ОИ.
Дефекты, сбои и отказы, аварии технических средств и систем объектов информатизации.
Дефекты, сбои и отказы программного обеспечения ОИ.

Рис. 4.1. **Перечень внутренних объективных факторов, воздействующих на безопасность защищаемой информации в соответствии с ГОСТ Р 51275-2006**

Разглашение защищаемой информации лицами, имеющими к ней право доступа, через:

- лиц, не имеющих права доступа к защищаемой информации;
- передачу информации по открытым линиям связи;
- обработку информации на незащищенных ТС обработки информации;
- опубликование информации в открытой печати и других средствах массовой информации;
- копирование информации на незарегистрированный носитель информации;
- передачу носителя информации лицам, не имеющим права доступа к ней;
- утрату носителя информации.

Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации, путем:

- несанкционированного изменения информации;
- несанкционированного копирования защищаемой информации.

Несанкционированный доступ к информации путем:

- подключения к техническим средствам и системам ОИ;
- использования закладочных средств [устройств];
- использования программного обеспечения технических средств ОИ;
- хищения носителя защищаемой информации;
- нарушения функционирования ТС обработки информации.

Недостатки организационного обеспечения защиты информации при:

- задании требований по защите информации (требования противоречивы, не обеспечивают эффективную защиту информации и т.д.);
- несоблюдении требований по защите информации;
- контроле эффективности защиты информации.

Ошибки обслуживающего персонала объекта информатизации при:

- эксплуатации ТС;
- эксплуатации программных средств;
- эксплуатации средств и систем защиты информации.

Рис. 4.2. **Перечень внутренних субъективных факторов, воздействующих на безопасность защищаемой информации в соответствии с ГОСТ Р 51275-2006**

Доступ к защищаемой информации с применением технических средств:

- разведки (радиоэлектронной, фотографической, визуально-оптической, акустической, технической компьютерной и др.);
- съема информации.

Несанкционированный доступ к защищаемой информации путем:

- подключения к техническим средствам и системам ОИ;
- использования закладочных средств [устройств];
- использования программного обеспечения технических средств ОИ через: маскировку под зарегистрированного пользователя; дефекты и уязвимости ПО; внесение программных закладок; применение вирусов или другого вредоносного программного кода;
- несанкционированного физического доступа к ОИ;
- хищения носителя информации.

Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку.

Действия криминальных групп и отдельных преступных субъектов:

- диверсия в отношении объектов информатизации;
- диверсия в отношении элементов объектов информатизации.

Искажение, уничтожение или блокирование информации с применением технических средств путем:

- преднамеренного силового электромагнитного воздействия;
- преднамеренного силового воздействия различной физической природы;
- использования программных или программно-аппаратных средств при осуществлении: компьютерной атаки, сетевой атаки;
- воздействия программными средствами в комплексе с преднамеренным силовым электромагнитным воздействием.

Рис. 4.3. **Перечень внешних субъективных факторов, воздействующих на безопасность защищаемой информации в соответствии с ГОСТ Р 51275-2006**

Выявление и учет факторов, воздействующих или могущих воздействовать на защищаемую информацию в конкретных условиях, составляют основу для планирования и проведения эффективных мероприятий, направленных на защиту информации на объекте информатизации.

Полнота и достоверность выявленных факторов, воздействующих или могущих воздействовать на защищаемую информацию, достигаются путем рассмотрения полного множества факторов, воздействующих на все элементы объекта информатизации и на всех этапах обработки информации.

Контрольные вопросы и задания

1. Какова область применения национального стандарта ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»?
2. Определите понятие «фактор, воздействующий на защищаемую информацию».
3. Дайте определение понятию «объект информатизации» в соответствии с ГОСТ Р 51275-2006.
4. Дайте определение понятию «система обработки информации» в соответствии с ГОСТ Р 51275-2006.
5. Дайте определения понятиям: «побочное электромагнитное излучение», «паразитное электромагнитное излучение», «наведенный в токопроводящих линейных элементах технических средств сигнал» в соответствии с ГОСТ Р 51275-2006.
6. Дайте определения понятиям «закладочное средство» и «программная закладка» в соответствии с ГОСТ Р 51275-2006.
7. Как может быть реализована программная закладка в соответствии с рекомендациями Р 50.1.053-2005 «Информационная технология. Основные термины и определения в области технической защиты информации»?
8. Какие действия составляют основу для планирования и проведения эффективных мероприятий, направленных на защиту информации на объекте информатизации?
9. Как достигается полнота и достоверность выявленных факторов, воздействующих или могущих воздействовать на защищаемую информацию?
10. С учетом каких требований должно осуществляться выявление факторов, воздействующих на защищаемую информацию?
11. На какие классы по отношению к природе возникновения подразделяются факторы, воздействующие или могущие воздействовать на безопасность защищаемой информации? Приведите примеры.
12. На какие классы по отношению к объектам информатизации подразделяются факторы, воздействующие на безопасность защищаемой информации? Приведите примеры.

Практическая работа 4.1. Основные положения национального стандарта Российской Федерации «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»

Цель работы: изучить классификацию и перечень факторов, воздействующих на безопасность защищаемой информации.

Порядок выполнения работы

1. Изучить теоретический материал темы 4 «Классификация факторов, воздействующих на безопасность защищаемой информации» настоящего учебного пособия.
2. Выполнить задания, фиксируя каждый пункт работы в отчете.
3. Представить оформленный отчет преподавателю. Отчет должен содержать номера пунктов работы, их наименование и (в правой колонке) результат выполнения каждого пункта.

Задания

1. Запуск электронного фонда правовой и нормативно-технической документации АО «Кодекс».

1. Создайте файл отчета в MS Word по образцу, приведенному в приложении. Сохраните файл под именем «Ваша фамилия41» (например: Иванов41). Заполните его шапку.
2. Откройте в электронной профессиональной справочной системе «Кодекс»/»Техэксперт» ГОСТ Р 51275-2006, для чего:

— выйдите в Интернет на страницу http://docs.cntd.ru/document/gost-r-51275-2006;

— откроется страница сайта, содержащая текст документа (рис. 4.1.1), ознакомитесь с ее содержимым;

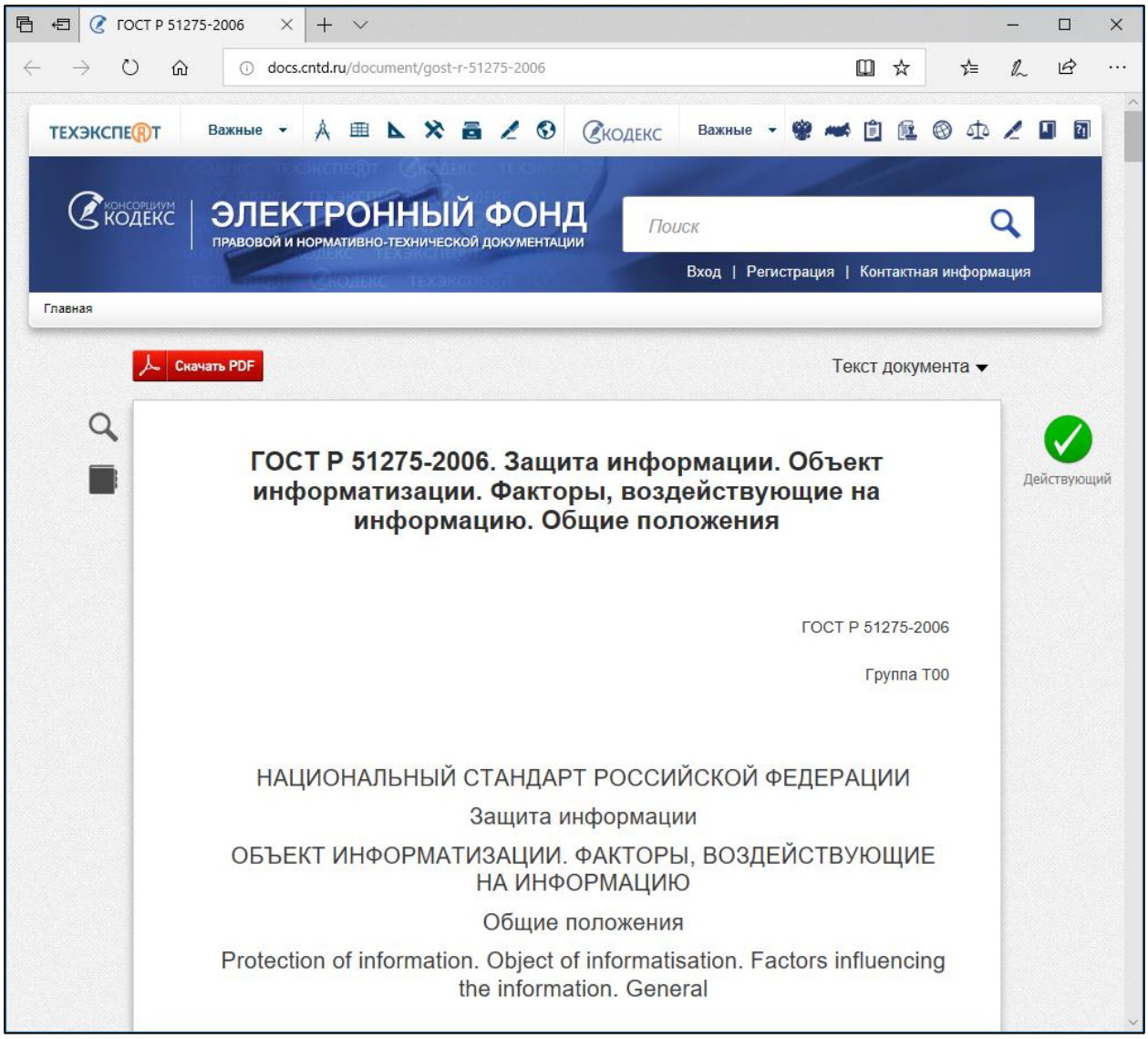


Рис. 4.1.1. **Текст документа ГОСТ Р 51275-2006 http://docs.cntd.ru/document/gost-r-51275-2006**

Зафиксируйте копию данной страницы в своем отчете.

2. Работа с текстом документа ГОСТ Р 51275-2006.

1. Откройте и *занесите в отчет копии* статус документа (рис 4.1.2).

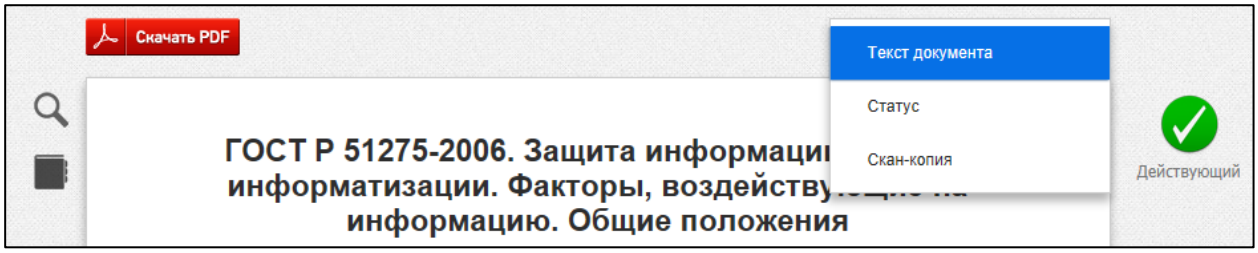


Рис. 4.1.2. **Разделы документа**

2. Вернитесь к тексту документа.

3. Откройте *Оглавление* документа с помощью кнопки  (рис 4.1.2), ознакомьтесь с ним и *скопируйте в отчет*.

4. С помощью *Оглавления* документа перейдите к Библиографии. *Копию экрана занесите в отчет*.

5. Изучите *Предисловие* стандарта. Внесите в отчет ответы на следующие вопросы:

– Кем разработан ГОСТ Р 51275-2006?
– Кем внесен ГОСТ Р 51275-2006?
– Когда утвержден и введен в действие?
– Взамен кого стандарта введен ГОСТ Р 51275-2006?

3. Изучить классификацию факторов и перечень факторов, воздействующих на безопасность защищаемой информации, установленных ГОСТ Р 51275-2006 в целях обоснования угроз безопасности информации и требований по защите информации на объекте информатизации.

1. С помощью *Оглавления* документа перейдите к разделу 5 Классификация факторов, воздействующих на безопасность защищаемой информации. *Копию экрана занесите в отчет*.

2. Внесите в отчет ответы на следующие вопросы:

– На какие классы по признаку отношения к природе подразделяют факторы, воздействующие или могущие воздействовать на безопасность защищаемой информации и подлежащие учету при организации защиты информации?
– Как подразделяют факторы, воздействующие на безопасность защищаемой информации, по отношению к объекту информатизации?
– Как подразделяют факторы, воздействующие на безопасность защищаемой информации, в соответствии с признаками классификации?

3. С помощью *Оглавления* документа перейдите к разделу 6 Перечень объективных и субъективных факторов, воздействующих на безопасность защищаемой информации. *Копию экрана занесите в отчет*.

4. Перенесите в отчет и заполните табл. 4.1.1.

Таблица 4.1.1

Перечень основных внутренних и внешних объективных факторов, воздействующих на безопасность защищаемой информации в соответствии с ГОСТ Р 51275-2006

№	Внутренние объективные факторы	Внешние объективные факторы
1.		
2.		
3.		
…		

5. Перенесите в отчет и заполните табл. 4.1.2.

Таблица 4.1.2

Перечень основных внутренних и внешних субъективных факторов, воздействующих на безопасность защищаемой информации в соответствии с ГОСТ Р 51275-2006

№	Внутренние субъективные факторы	Внешние субъективные факторы
1.		
2.		
3.		
…		

6. Ответьте на вопросы для изучения в файле отчета. Номера вопросов определяются по начальной букве фамилии студента (табл. 4.1.3).

Таблица 4.1.3

Варианты к работе 4.1

Начальная буква фамилии студента	Номера вопросов	Начальная буква фамилии студента	Номера вопросов
А, И, С, Щ	1, 9, 17	Д, Н, Х	5, 13, 21
Б, К, Т	2, 10, 18	Е, О, Ц, Ю	6, 14, 22
В, Л, У, Э	3, 11, 19	Ж, П, Ч	7, 15, 23
Г, М, Ф	4, 12, 20	З, Р, Ш, Я	8, 16, 24

7. Представьте оформленный отчет по выполненной работе преподавателю на проверку.

Вопросы для изучения

1. Как осуществляется передача сигналов, являющаяся внутренним объективным фактором, воздействующим на безопасность защищаемой информации?
2. Какие излучения сигналов функционально присущи техническим средствам [устройствам] объектов информатизации?
3. Какие побочные электромагнитные излучения являются внутренними объективными факторами, воздействующими на безопасность защищаемой информации?
4. Чем может быть вызвана наводка в линиях связи?
5. Чем может быть вызвана наводка в цепях электропитания?
6. Чем может быть вызвана наводка в цепях заземления?
7. Каковы явления техногенного характера, являющиеся внешними объективными факторами, воздействующими на безопасность защищаемой информации?

8. Каковы природные явления и стихийные бедствия, являющиеся внешними объективными факторами, воздействующими на безопасность защищаемой информации?

9. Аварии технических средств и систем объектов информатизации являются внешними или внутренними объективными факторами?

10. Дефекты, сбои и отказы программного обеспечения объектов информатизации являются внешними или внутренними объективными факторами, воздействующими на безопасность защищаемой информации?

11. Непреднамеренные электромагнитные облучения объектов информатизации являются внешними или внутренними объективными факторами, воздействующими на безопасность защищаемой информации?

12. Сбои, отказы и аварии систем обеспечения объектов информатизации являются внешними или внутренними объективными факторами, воздействующими на безопасность защищаемой информации?

13. Пожары, наводнения и землетрясения являются внешними или внутренними объективными факторами?

14. Микробы и грызуны являются внешними или внутренними объективными факторами, воздействующими на безопасность защищаемой информации?

15. Химические агрессивные среды являются внешними или внутренними объективными факторами, воздействующими на безопасность защищаемой информации?

16. Разглашение защищаемой информации лицами, имеющими к ней право доступа, является внутренним или внешним субъективным фактором?

17. Как может быть осуществлено разглашение защищаемой информации лицами, имеющими к ней право доступа?

18. Какие неправомерные действия могут быть осуществлены лицами, имеющими право доступа к защищаемой информации?

19. Как может быть получен несанкционированный доступ к информации?

20. При каких условиях недостатки организационного обеспечения защиты информации являются внутренними субъективными факторами, воздействующими на безопасность защищаемой информации?

21. Когда ошибки обслуживающего персонала объекта информатизации являются внутренними субъективными факторами, воздействующими на безопасность защищаемой информации?

22. С помощью каких видов разведок с применением технических средств может быть получен доступ к защищаемой информации с применением технических средств?

23. Как применение вирусов или другого вредоносного программного кода может нанести ущерб защищаемой информации?

24. Могут ли действия криминальных групп и отдельных преступных субъектов являться факторами, воздействующими на безопасность защищаемой информации?

Тема 5. Техническая защита информации

Рекомендации по стандартизации Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения» устанавливают термины и определения понятий в области технической защиты информации в различных сферах деятельности.

Согласно с ГОСТ Р 50922-2006 ***объект защиты информации*** — информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации (рис. 5.1).

Рис. 5.1. **Схема взаимосвязи терминов (Р 50.1.053-2005)**

Схема взаимосвязи общих понятий представлена на рис. 5.2, где

информационная безопасность объекта информатизации — состояние защищенности объекта информатизации, при котором обеспечивается безопасность информации и автоматизированных средств ее обработки;

показатель защищенности информации — количественная или качественная характеристика безопасности информации, определяющая уровень требований, предъявляемых к конфиденциальности, целостности и доступности этой информации и реализуемых при ее обработке.

Рис. 5.2. **Схема взаимосвязи общих понятий (Р 50.1.056-2005)**

Схема основных терминов в области технической защиты информации приведена на рис. 5.3.

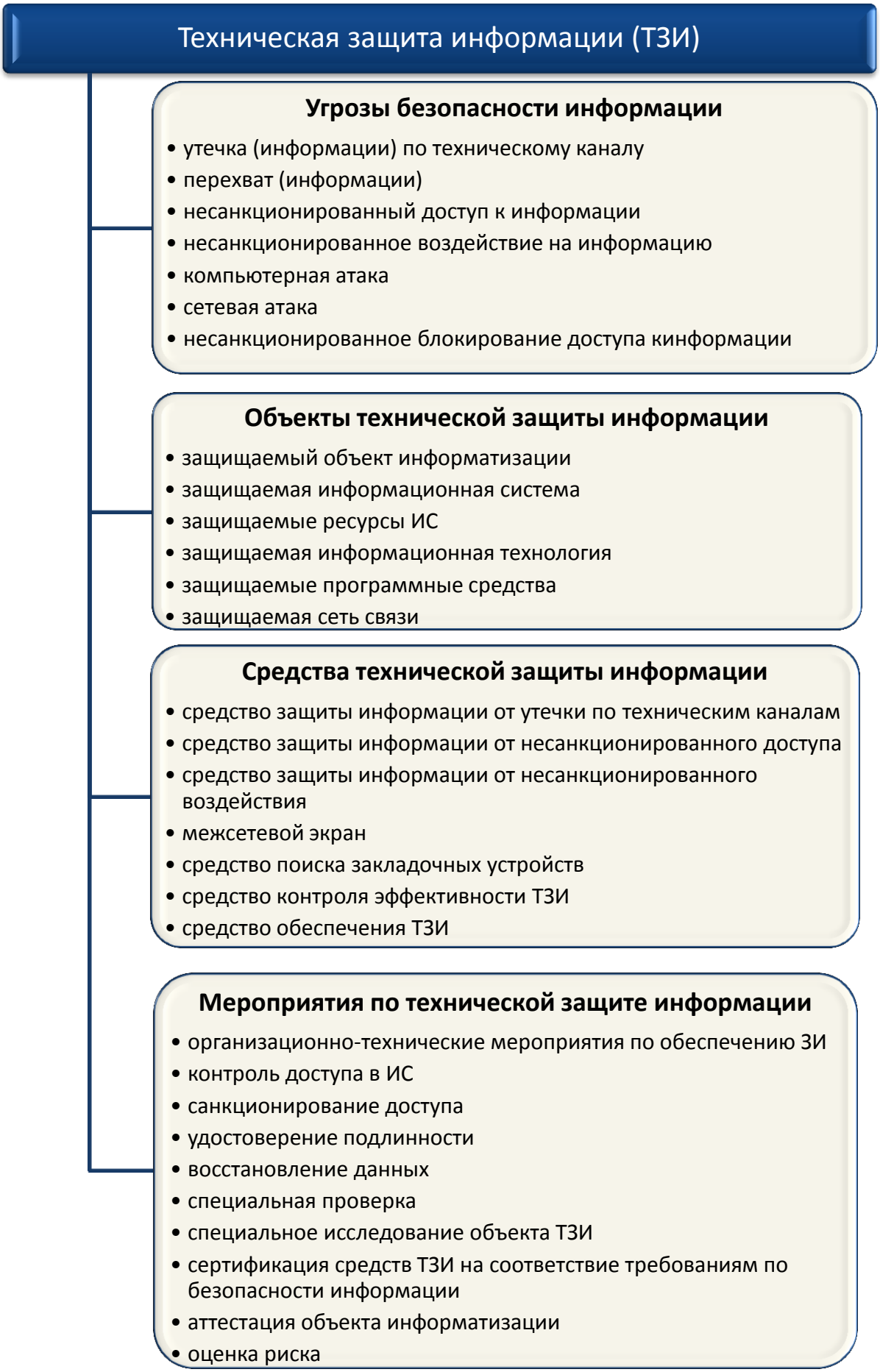


Рис. 5.3. **Схема основных терминов в области ТЗИ (Р 50.1.056-2005)**

5.1. Угрозы безопасности информации

Рекомендации по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» устанавливают термины и определения понятий в области технической защиты информации при применении информационных технологий.

Схема взаимосвязи стандартизованных терминов угроз безопасности информации приведена на рис. 5.4.

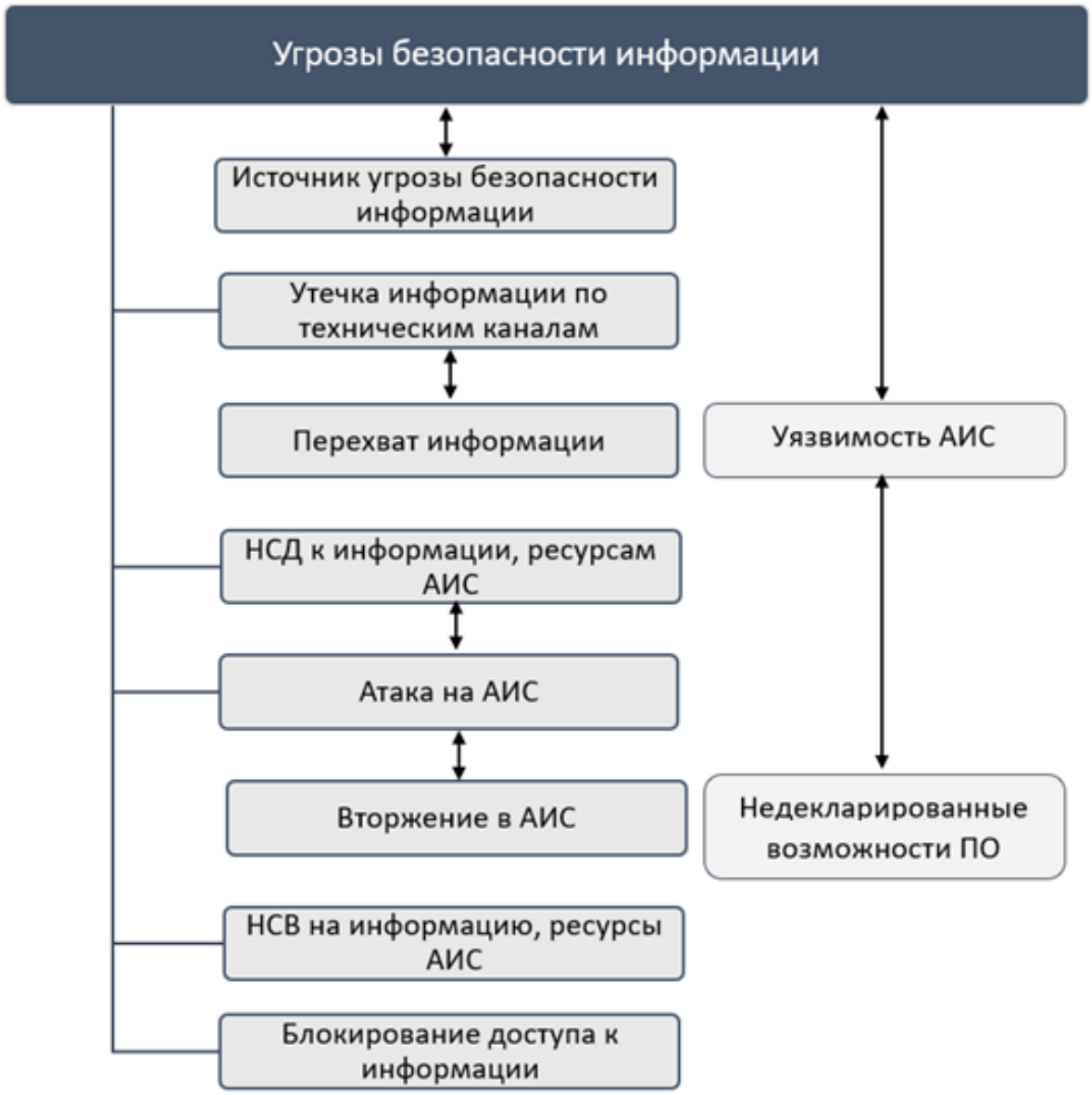


Рис. 5.4. **Схема стандартизированных терминов (Р 50.1.053-2005)**

Источник угрозы безопасности информации — субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации (рис. 5.5, 5.7).

Рис. 5.5. **Классификация потенциальных источников угроз по природе их возникновения**

В 2017 г. наблюдался резкий рост числа инцидентов, сопряженных с мошенничеством, совершенных в России (рис. 5.6).

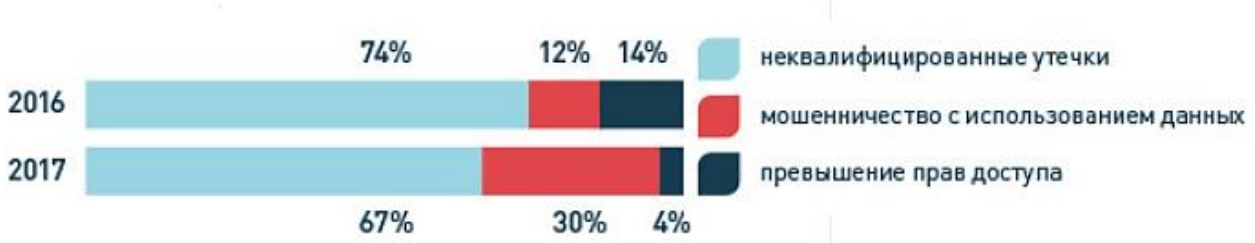


Рис. 5.6. **Распределение утечек данных по инцидентам в России**

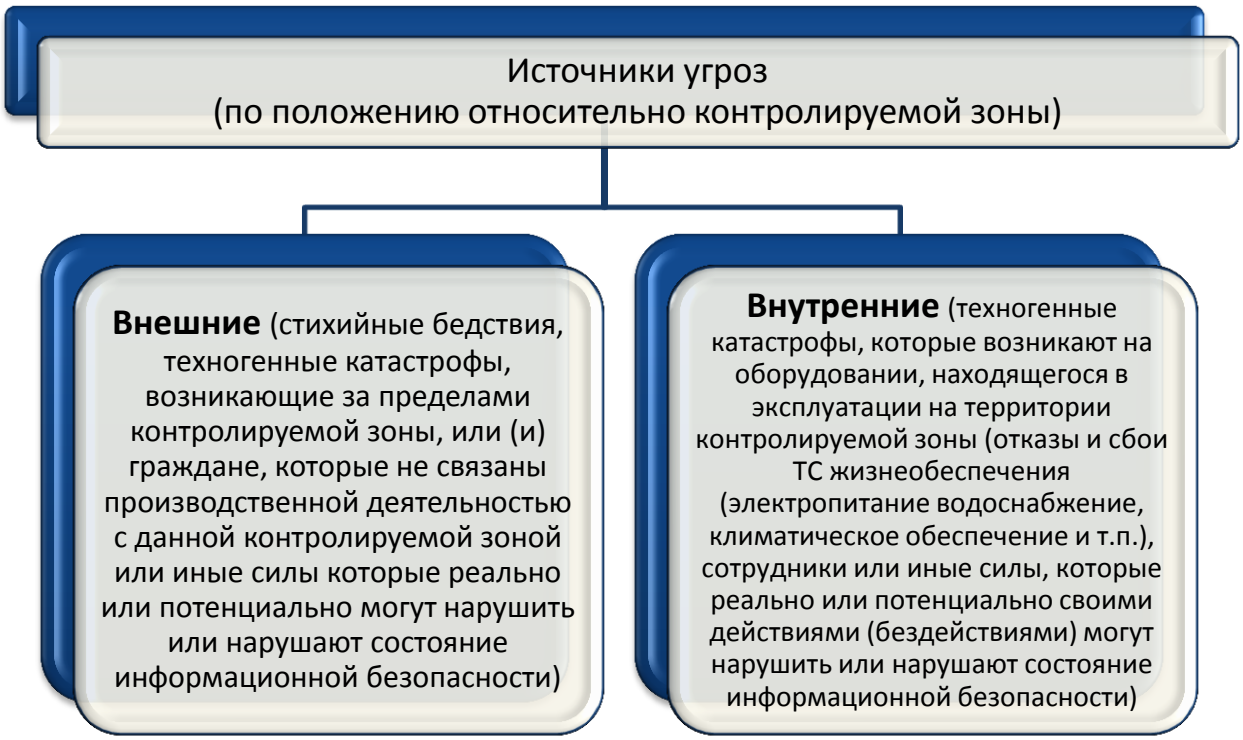


Рис. 5.7. **Классификация потенциальных источников угроз по положению относительно контролируемой зоны**

На рис. 5.8 представлено распределение утечек информации по типам инцидентов в 2018 г. не только в России, но и в мире. Для России характерна высокая доля так называемых «квалифицированных утечек», т.е. инцидентов, в результате которых информация была не только скомпрометирована, в том числе в результате нелегитимного доступа, но и осознанно использована в личных целях (рис. 5.6, 5.8).

Рис. 5.8. **Распределение утечек информации по типам инцидентов, мир – Россия, 2018 г.** (данные компании InfoWatch)

Под *утечкой* информации аналитический центр InfoWatch понимает намеренные или случайные действия (как внешних злоумышленников, так и внутренних нарушителей), в результате которых нарушена конфиденциальность данных.

Число зарегистрированных утечек данных из организаций в 2018 г. выросло более чем на 5% по сравнению с 2017 г. Более половины всех случаев

зафиксированы в высокотехнологичных компаниях, госсекторе и медицинских организациях.

В 2018 г. зарегистрировано 270 случая утечки конфиденциальной информации из организаций, работающих в России. В результате скомпрометировано 5,8 млн записей, относящихся к персональным и финансовым данным, а также к другим типам конфиденциальной информации. Львиная доля утечек происходит по вине внутренних нарушителей (рис. 5.9).

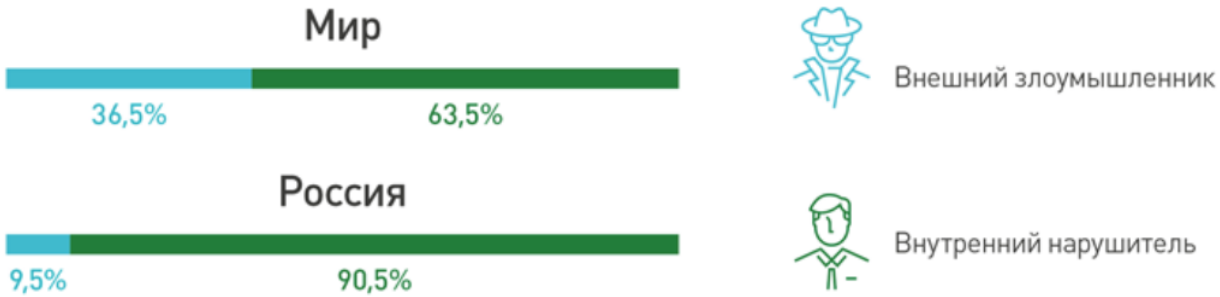


Рис. 5.9. **Распределение утечек информации по вектору воздействия, мир – Россия, 2018 г.**

По способу реализации угрозы безопасности информации подразделяют следующим образом:

1) *утечка (информации) по техническому каналу*, *leakage*: неконтролируемое распространение информации от носителя защищаемой информации[1] через физическую среду до технического средства, осуществляющего перехват информации[2].

2) *несанкционированный доступ* (к информации), НСД, *unauthorized access*: доступ к информации[3], осуществляемый с нарушением установленных прав и (или) правил доступа к информации (рис. 5.8);

3) *несанкционированное воздействие* (на информацию), НСВ: изменение информации, осуществляемое с нарушением установленных прав и (или) правил (рис. 5.10).

[1] *Носитель защищаемой информации* — физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин [ГОСТ Р 50922-2006].

[2] Перехват (информации), interception — неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

[3] *Доступ к информации* — возможность получения информации и ее использования [Федеральный закон от 27.07.2006 № 149-ФЗ].

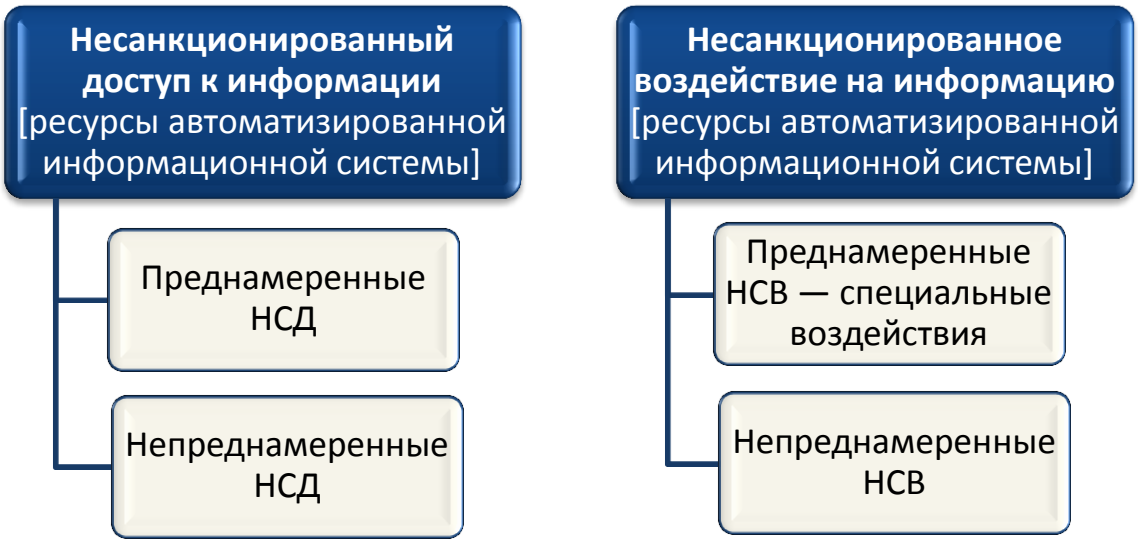


Рис. 5.10. **Виды НСД и НСВ**

5.2. Уязвимости информационных систем

Стандарт ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» устанавливает классификацию уязвимостей информационных систем (ИС), направлен на совершенствование методического обеспечения определения и описания угроз безопасности информации при проведении работ по защите информации в ИС.

Настоящий стандарт не распространяется на уязвимости информационных систем, связанные с утечкой информации по техническим каналам, в том числе уязвимости электронных компонентов технических (аппаратных и аппаратно-программных) средств информационных систем.

Стандарт ГОСТ Р 56546-2015 определяет ***уязвимость*** как недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации.

Одной из важных характеристик уязвимостей информационных систем можно выделить ***степень опасности уязвимости***, то есть меру, характеризующую подверженность информационной системы уязвимости и ее влияние на нарушение свойств безопасности информации (конфиденциальность, целостность, доступность).

Определение термина «информационная система» в данном стандарте соответствует Федеральному закону «Об информации, информационных технологиях и о защите информации», а именно *информационная система* — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий[1] и технических средств.

[1] *Информационная технология* — процесс, метод поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов.

В основе классификации уязвимостей информационных систем используются следующие классификационные признаки[1]:

– область происхождения уязвимости (рис. 5.10);
– типы недостатков информационных систем (рис. 5.11);
– место возникновения (проявления) уязвимости ИС (рис. 5.12).

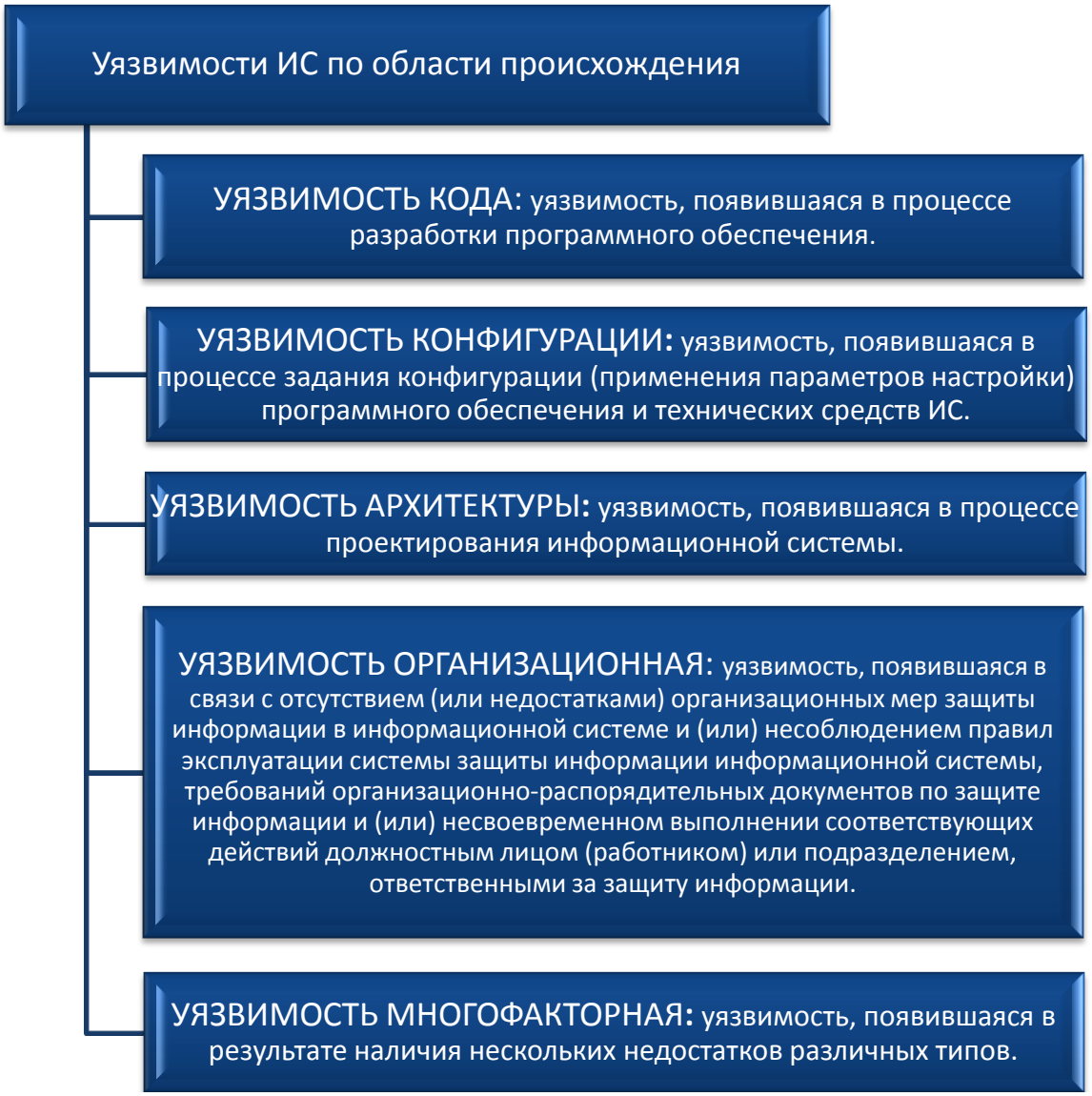


Рис. 5.10. **Классификация уязвимостей ИС по области происхождения**

Примечание: в целях выявления и оценки уязвимостей информационных систем могут выделяться подклассы уязвимостей.

[1] *Признак классификации уязвимостей* — свойство или характеристика уязвимостей, по которым производится классификация.

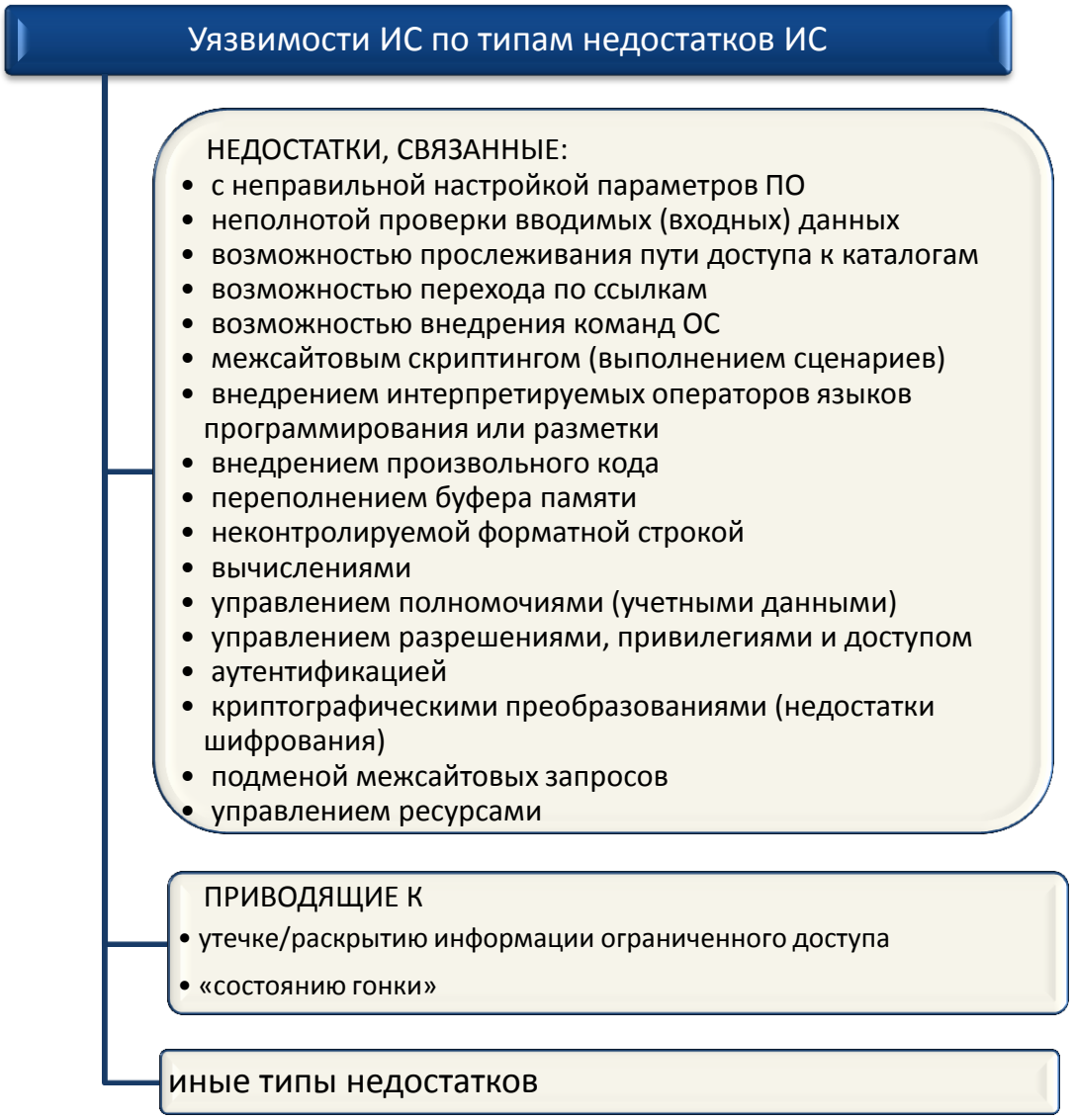


Рис. 5.11. **Классификация уязвимостей ИС по типам недостатков ИС**

Примечание: по результатам выявления уязвимостей информационных систем перечень типов недостатков может дополняться.

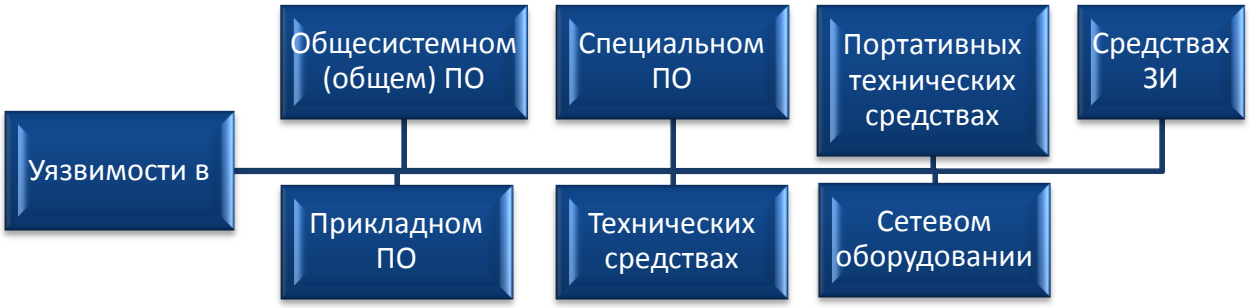


Рис. 5.12. **Классификация уязвимостей ИС по месту возникновения (проявления)**

В качестве *уязвимых компонентов информационной системы* рассматриваются:

– общесистемное (общее) программное обеспечение;
– прикладное программное обеспечение;
– специальное программное обеспечение;
– технические средства;
– сетевое (коммуникационное, телекоммуникационное) оборудование;
– средства защиты информации.

Помимо классификационных признаков уязвимостей ИС используются поисковые признаки (*основные* и *дополнительные*). Поисковые признаки предназначены для организации расширенного поиска в базах данных уязвимостей.

К *основным поисковым признакам уязвимостей информационных систем* относятся следующие:

– наименование операционной системы и тип аппаратной платформы;
– наименование программного обеспечения и его версия;
– степень опасности уязвимости.

К *дополнительным поисковым признакам уязвимостей информационных систем* относятся следующие:

– язык программирования;
– служба (порт), которая (который) используется для функционирования программного обеспечения.

Государственный научно-исследовательский испытательный институт проблем технической защиты информации (ФАУ «ГНИИИ ПТЗИ ФСТЭК России») создал и ведет *Банк данных угроз безопасности информации* (рис. 5.13), целью которого является повышение информированности заинтересованных лиц о существующих угрозах безопасности информации в информационных (автоматизированных) системах.

Банк данных угроз безопасности информации предназначен для заказчиков, операторов, разработчиков информационных (автоматизированных) систем и их систем защиты, разработчиков и производителей средств защиты информации, испытательных лабораторий и органов по сертификации средств защиты информации, а также иных заинтересованных организаций и лиц.

Банк данных угроз безопасности информации содержит сведения об основных угрозах безопасности информации и уязвимостях, в первую очередь, характерных для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов.

Сведения об угрозах безопасности информации и уязвимостях программного обеспечения, содержащиеся в Банке данных угроз безопасности информации, не являются исчерпывающими и могут быть дополнены по результатам анализа угроз безопасности информации и уязвимостей в конкретной информационной (автоматизированной) системе с учетом особенностей ее эксплуатации.

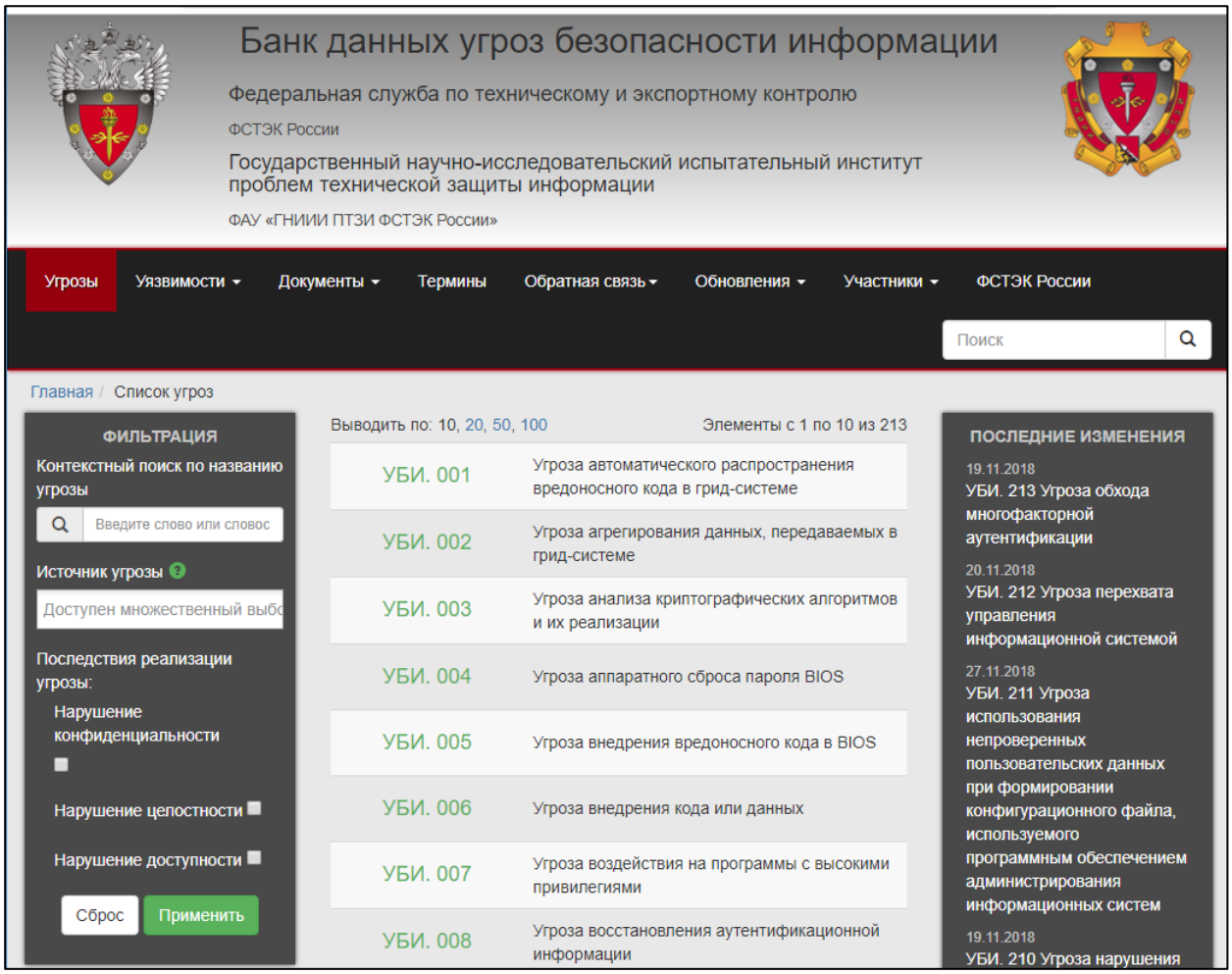


Рис. 5.13. **Банк данных угроз безопасности информации**

Включение неизвестных ранее уязвимостей в Банк данных угроз безопасности информации осуществляется в соответствии с утвержденным Регламентом включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России.

5.3. Техника защиты информации

Стандарт ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества» распространяется на основные средства защиты информации и средства контроля эффективности защиты информации, входящие в состав техники защиты информации.

Настоящий стандарт устанавливает номенклатуру основных показателей качества средств защиты информации: от утечки по техническим каналам, от несанкционированного доступа, а также средств контроля эффективности защиты информации, которые должны быть включены в тактико-технические задания на научно-исследовательские и опытно-конструкторские работы по определению и реализации перспектив развития этой группы продукции и в национальные стандарты.

Основные средства, входящие в состав техники защиты информации, представлены на рис. 5.14:

средство защиты информации от утечки по техническим каналам — техническое средство, вещество или материал, предназначенные и (или) используемые для защиты информации от утечки по техническим каналам;

средство защиты информации от несанкционированного доступа — техническое, программное или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа к информации или ресурсам информационной системы;

средство защиты информации от несанкционированного воздействия — техническое, программное или программно-техническое средство, предназначенное для предотвращения несанкционированного воздействия на информацию или ресурсы информационной системы;

межсетевой экран — локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство(комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и (или) выходящей из автоматизированной системы;

средство поиска закладочных устройств — техническое средство, предназначенное для поиска закладочных устройств, установленных на объекте информатизации;

средство контроля эффективности технической защиты информации — средство измерений, программное средство, вещество и (или) материал, предназначенные и (или) используемые для контроля эффективности технической защиты информации;

средство обеспечения технической защиты информации — техническое, программное, программно-техническое средство, используемое и (или) создаваемое для обеспечения технической защиты информации на всех стадиях жизненного цикла защищаемого объекта.

Для классификации техники защиты информации используют следующие признаки:

– функциональное назначение защиты информации (контроль эффективности защиты информации);

– вид предотвращаемых угроз (НСД, НСВ, утечка информации по техническим каналам);

– по решаемым задачам;

– функциональная сложность (средство, комплекс, система);

– метод защиты (*пассивные*, *активные*);

– место установки (наземные, воздушные, морские и космические);

– сфера применения (*специального назначения*, *общего применения*);

– конструктивное исполнение (встроенные в объект защиты, выполненные в виде отдельного образца изделия);

– вид исполнения (*технические*, *программные*, *программно-технические* средства).

Рис. 5.14. **Основные средства, входящие в состав техники ЗИ**

5.4. Мероприятия по технической защите информации

Организационно-технические мероприятия по обеспечению защиты информации, *en Technical safeguards* — совокупность действий, направленных на применение организационных мер и программно-технических способов защиты информации на объекте информатизации (рис. 5.15).

Организационно-технические мероприятия по обеспечению защиты информации должны осуществляться на всех этапах жизненного цикла объ-

екта информатизации. Организационные меры предусматривают установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации.

Рис. 5.15. **Схема взаимосвязи терминов (Р 50.1.053-2005)**

Политика безопасности (информации в организации), *organizational security policy* — одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Профиль защиты, *protection profile* — совокупность типовых требований по обеспечению безопасности информации, которые должны быть реализованы в защищаемой автоматизированной информационной системе.

Правила разграничения доступа (в автоматизированной информационной системе) — правила, регламентирующие условия доступа субъектов доступа к объектам доступа в автоматизированной информационной системе.

Аутентификация (субъекта доступа), *authentication* — действия по проверке подлинности субъекта доступа[1] в автоматизированной информационной системе.

[1] *Субъект доступа* (в АИС), *subject* — лицо или единица ресурса автоматизированной информационной системы, действия которой по доступу к ресурсам автоматизированной информационной системы регламентируются правилами разграничения доступа [Р 50.1.053-2005].

Идентификация, identification — действия по присвоению субъектам и объектам доступа[1] идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Мониторинг безопасности информации (при применении информационных технологий), *IT security monitoring* — процедуры регулярного наблюдения за процессом обеспечения безопасности информации при применении информационных технологий.

Аудит безопасности автоматизированной информационной системы, *computer-system audit* — проверка реализованных в автоматизированной информационной системе процедур обеспечения безопасности с целью оценки их эффективности и корректности, а также разработки предложений по их совершенствованию.

Сертификация средств технической защиты информации на соответствие требованиям по безопасности информации — деятельность органа по сертификации по подтверждению соответствия средств технической защиты информации требованиям технических регламентов, положениям стандартов или условиям договоров.

Аттестация объекта информатизации — деятельность по установлению соответствия комплекса организационно-технических мероприятий по защите объекта информатизации требованиям по безопасности информации.

Аттестация производится в порядке, установленном Положением по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Государственной технической комиссии при Президенте РФ 25 ноября 1994 г.). Под *аттестацией объектов информатизации* понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России (в настоящее время ФСТЭК России).

Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленным в «Аттестате соответствия».

Обязательной аттестации подлежат объекты информатизации, предназначенные:

- для обработки информации, составляющей государственную тайну;
- управления экологически опасными объектами;
- ведения секретных переговоров.

В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации.

[1] *Объект доступа* (в АИС), *object* — единица ресурса автоматизированной информационной системы, доступ к которой регламентируется правилами разграничения доступа.

Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

«Аттестат соответствия» выдается владельцу аттестованного объекта информатизации органом по аттестации на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более чем на три года.

Оценка риска[1]; анализ риска, *en Risk assessment, risk analysis* — выявление угроз безопасности информации, уязвимостей информационной системы[2], оценка вероятностей реализации угроз с использованием уязвимостей и оценка последствий реализации угроз для информации и информационной системы, используемой для обработки этой информации.

При определении угроз на конкретном объекте защиты важно понимать, что нельзя учесть абсолютно все угрозы, а тем более защититься от них.

Не может быть абсолютной безопасности — некоторый риск (*остаточный*) будет оставаться.

Остаточный риск — риск, остающийся после предпринятых защитных мер.

При идентификации угрозы необходимо установить все возможные источники этой угрозы, так как зачастую угроза возникает вследствие наличия определенной уязвимости и может быть устранена с помощью механизма защиты (например, механизм аутентификации).

К идентификации угроз можно подходить двумя путями:

— *по уязвимостям*, повлекшим за собой появление угрозы;

— *по источникам угроз*.

Опасность[3] угрозы определяется риском в случае ее успешной реализации. Допустимость риска означает, что ущерб[4] в случае реализации угрозы не приведет к серьезным негативным последствиям для владельца информации.

Ущерб подразделяется на:

---

[1] *Риск* — сочетание вероятности нанесения ущерба и тяжести этого ущерба [ГОСТ Р 51898-2002].

[2] *Уязвимость* (информационной системы), брешь, *vulnerability* — свойство информационной системы, предоставляющее возможность реализации угроз безопасности обрабатываемой в ней информации [ГОСТ Р 50922-2006].

[3] *Опасность* — потенциальный источник возникновения ущерба [ГОСТ Р 51898-2002].

[4] *Ущерб* — нанесение физического повреждения или другого вреда здоровью людей, или вреда имуществу или окружающей среде [ГОСТ Р 51898-2002].

– *опосредованный* (косвенный) — связан с причинением вреда государству или обществу, но не владельцу информации;

– *непосредственный* — связан с причинением материального, морального, финансового, физического вреда владельцу информации.

Безопасность достигают путем снижения уровня риска до допустимого.

Допустимый риск — риск, который в данной ситуации считают приемлемым при существующих общественных ценностях.

Допустимый риск представляет собой оптимальный баланс между безопасностью и требованиями, которым должны удовлетворять продукция, процесс или услуга, а также такими факторами, как выгодность для пользователя, эффективность затрат и др. Допустимый риск достигают с помощью итеративного процесса оценки риска и уменьшения риска (рис. 5.16).

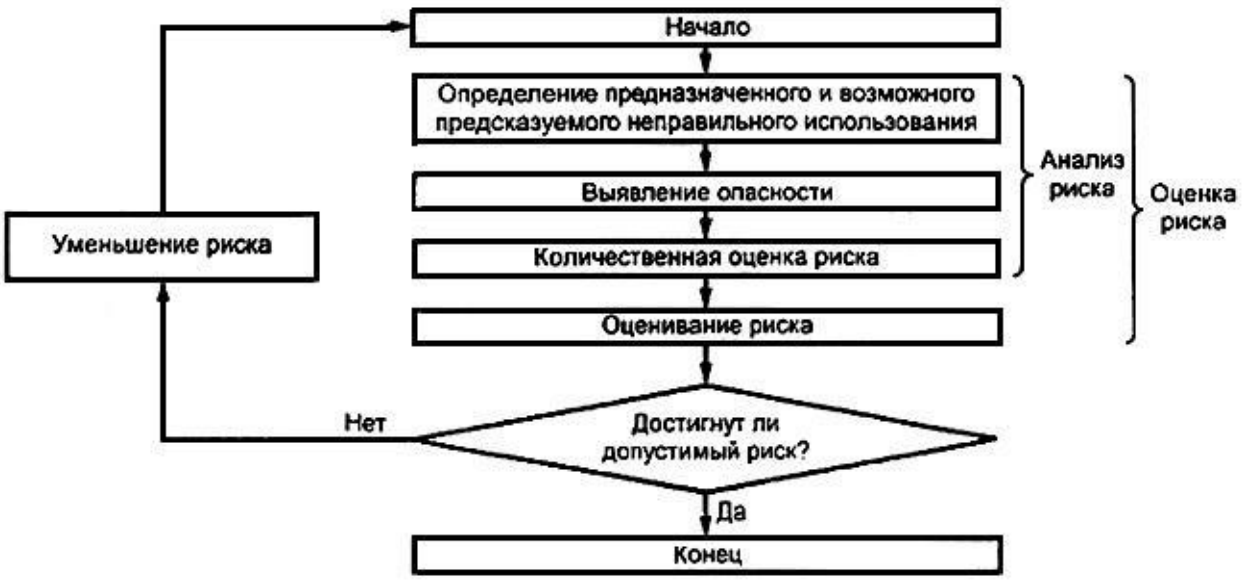


Рис. 5.16. **Итеративный процесс оценки риска и уменьшения риска (в соответствии с ГОСТ Р 51898-2002)**

Для оценки рисков целесообразно привлекать экспертов — специалистов в области информационной безопасности, которые должны обладать:

– знаниями законодательства РФ, международных и национальных стандартов в области обеспечения информационной безопасности;

– знаниями нормативных актов и предписаний регулирующих и надзорных органов в области обеспечения информационной безопасности;

– знаниями внутренних документов организаций, регламентирующих деятельность в области обеспечения информационной безопасности;

– знаниями о современных средствах вычислительной и телекоммуникационной техники, операционных системах, системах управления базами данных, а также о конкретных способах обеспечения информационной безопасности в них;

– знаниями о возможных источниках угроз информационной безопасности, способах реализации угроз информационной безопасности, частоте реализации угроз информационной безопасности в прошлом;

– пониманием различных подходов к обеспечению информационной безопасности, знания защитных мер, свойственных им ограничений.

Существуют различные *методы оценки риска*, образующие два взаимодополняющих друг друга вида:

❖ *количественный метод оценки риска*. Целью количественной оценки риска является получение числовых значений потенциального ущерба для каждой конкретной угрозы и для совокупности угроз на защищаемом объекте, а также выгоды от применения средств защиты. Основным недостатком данного подхода является невозможность получения конкретных значений в некоторых случаях. Например, если в результате реализации угрозы наносится ущерб имиджу организации, непонятно, как количественно оценить подобный ущерб;

❖ *качественный метод оценки риска*. Качественная оценка рисков оперирует не численными значениями, а качественными характеристиками угроз. Как правило, анализ рисков выполняется путем заполнения опросных листов и проведения совместных обсуждений с участием представителей различных групп организации, таких как эксперты по информационной безопасности, менеджеры и сотрудники ИТ-подразделений, владельцы и пользователи бизнес-активов.

Пользователь участвует в процедуре уменьшения риска путем выполнения предписаний, представленных разработчиком/поставщиком (рис. 5.17). Меры, предпринимаемые в процедуре разработки проекта, расположены на рис. 5.17 в порядке приоритета. Меры, предпринимаемые пользователем, расположены не в порядке приоритета, так как этот порядок зависит от их применимости в конкретных условиях.

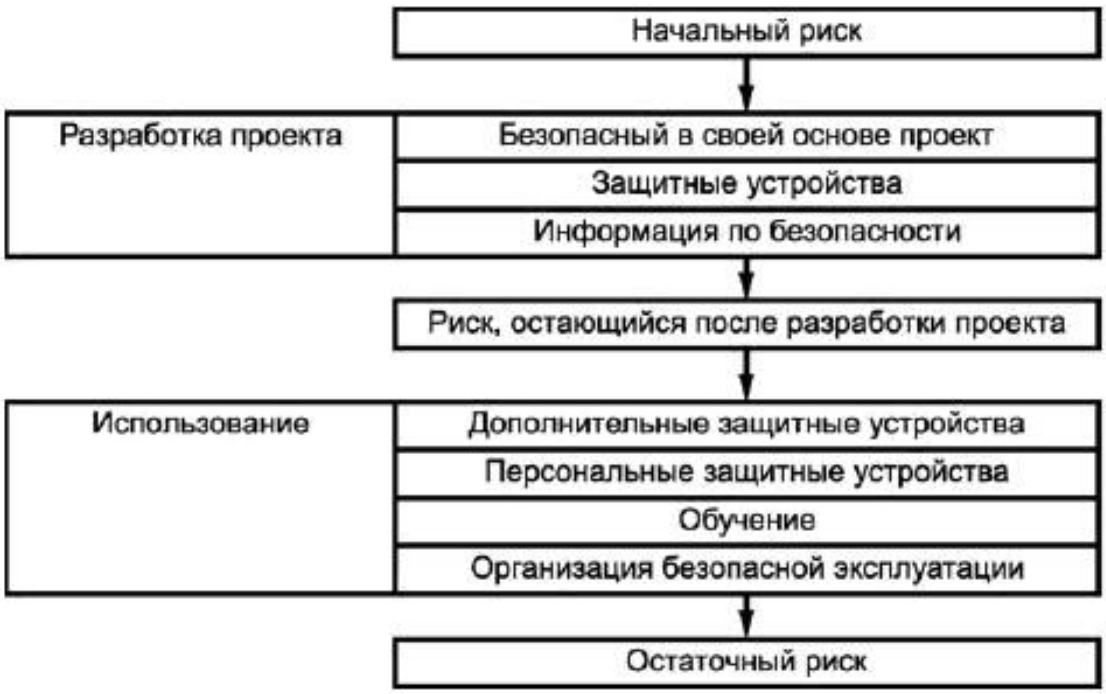


Рис. 5.17. **Уменьшение риска (в соответствии с ГОСТ Р 51898-2002)**

Способы уменьшения риска (в порядке приоритетов):

- разработка безопасного в своей основе проекта;
- защитные устройства и персональное защитное оборудование;
- информация по установке и применению;
- обучение.

Контрольные вопросы и задания

1. Какова область применения рекомендаций по стандартизации Р 50.1.056-2005?
2. Определите понятие «техническая защита информации» в соответствии с Р 50.1.056-2005.
3. Определите понятие «угроза (безопасности информации)» в соответствии с Р 50.1.056-2005.
4. Определите понятие «уязвимость (информационной системы)» в соответствии с Р 50.1.056-2005.
5. Определите основные угрозы безопасности информации в соответствии с Р 50.1.056-2005.
6. Определите объекты технической защиты информации в соответствии с Р 50.1.056-2005.
7. Определите основные средства технической защиты информации в соответствии с Р 50.1.056-2005.
8. Определите основные мероприятия по технической защите информации в соответствии с Р 50.1.056-2005
9. Дайте определение понятию «организационно-технические мероприятия по обеспечению защиты информации».
10. Дайте определения понятиям: «политика безопасности информации в организации», «аудиторская проверка информационной безопасности в организации», «мониторинг безопасности информации» и «оценка риска».
11. Какова область применения рекомендаций по стандартизации Р 50.1.053-2005?
12. Определите объекты технической защиты информации в соответствии с Р 50.1.053-2005.
13. Определите основные угрозы безопасности информации в соответствии с Р 50.1.053-2005.
14. Какова область применения стандарта ГОСТ Р 56546-2015?
15. На какие классы подразделяются уязвимости информационной системы по области происхождения?
16. На какие классы подразделяются уязвимости информационной системы по типам недостатков информационных систем?
17. На какие классы подразделяются уязвимости информационной системы по месту возникновения (проявления)?
18. Какова область применения стандарта ГОСТ Р 52447-2005?

19. Какие признаки используют для классификации техники защиты информации?

20. Перечислите основные средства, входящие в состав техники защиты информации в соответствии с ГОСТ Р 52447-2005.

21. Что устанавливает Положение по аттестации объектов информатизации по требованиям безопасности информации?

22. Что понимается под аттестацией объектов информатизации?

23. Какие объекты информатизации подлежат обязательной аттестации?

24. На что дает право наличие на объекте информатизации действующего «Аттестата соответствия»?

25. Дайте определения понятиям: «риск», «ущерб» и «допустимый риск» в соответствии с ГОСТ Р 51898-2002.

26. Как достигается безопасность информации в соответствии с ГОСТ Р 51898-2002?

27. Как достигается допустимый риск в соответствии с ГОСТ Р 51898-2002?

28. Опишите процесс уменьшения риска в соответствии с ГОСТ Р 51898-2002.

Практическая работа 5.1. Угрозы безопасности информации. Классификации источников угроз

Цель работы: изучить термины, относящиеся к угрозам безопасности информации, стандартизованные в рекомендациях Р 50.1.053-2005. Ознакомиться с классификациями источников угроз.

Порядок выполнения работы

1. Изучить теоретический материал п. 5.1. «Угрозы безопасности информации» настоящего учебного пособия.
2. Выполнить задания практической части.
3. Представить оформленный отчет преподавателю.

Задания

1. Создайте файл отчета в MS Word. Сохраните файл под именем «Ваша фамилия51» (например: Иванов51).

2. Откройте в электронной профессиональной справочной системе «Кодекс»/»Техэксперт» рекомендации по стандартизации Р 50.1.053-2005, для чего:

— выйдите в Интернет на страницу http://docs.cntd.ru/document/1200039555;

— откроется страница сайта, содержащая текст документа (рис. 5.1.1), ознакомитесь с ее содержимым.

3. Изучите *Предисловие* документа. Внесите в отчет ответы на следующие вопросы:

– Кем разработаны Р 50.1.053-2005?

– Кем внесены Р 50.1.053-2005?

– Когда утверждены и введены в действие Р 50.1.053-2005?

– Если Р 50.1.053-2005 введены не впервые, то укажите взамен каких рекомендаций?

4. Отразите в отчете область применения рекомендации по стандартизации Р 50.1.053-2005.

5. Внесите в отчет ответы на следующие вопросы:

– Совместно с каким государственным стандартом Российской Федерации должны применяться рекомендации Р 50.1.053-2005?

– Какие нормативные ссылки использованы в рекомендациях Р 50.1.053-2005?

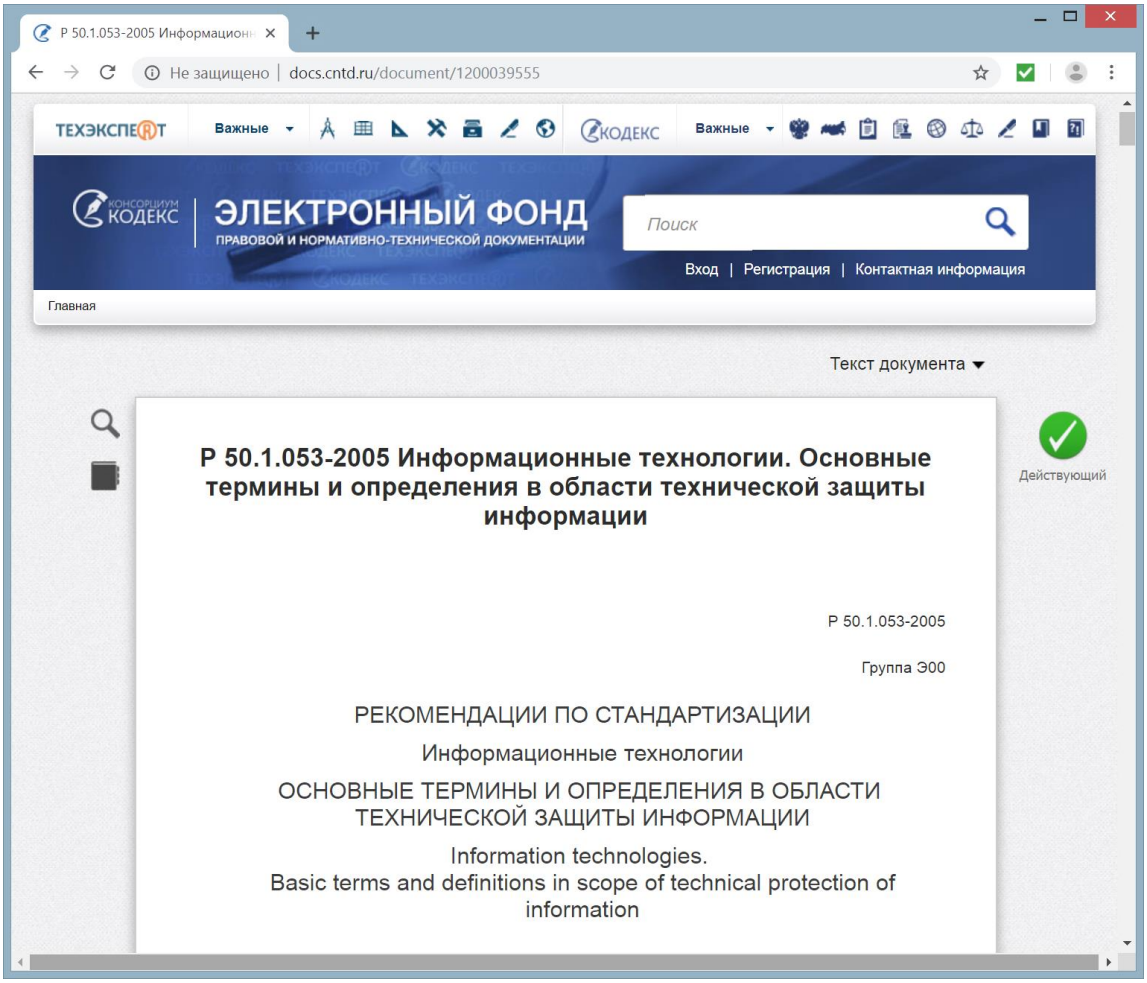


Рис. 5.1.1. **Текст документа Р 50.1.053-2005, http://docs.cntd.ru/document/1200039555**

6. Перенесите в отчет и заполните табл. 5.1.1.

Таблица 5.1.1

Термины, относящиеся к угрозам безопасности информации

№	Термин	Русский перевод термина	Определение
1.	Threat		
2.	Vulnerability		
3.	Leakage		
4.	Interception		
5.	Informative signal		
6.	Access		
7.	Subject		
8.	Object		
9.	Unauthorized access		
10.	Attack		
11.	Intrusion		
12.	Computer virus		
13.	Malicious logic		

7. Откройте *Список угроз*, который создал и ведет Государственный научно-исследовательский испытательный институт проблем технической защиты информации (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»), перейдя по ссылке https://bdu.fstec.ru/threat (рис. 5.1.2).

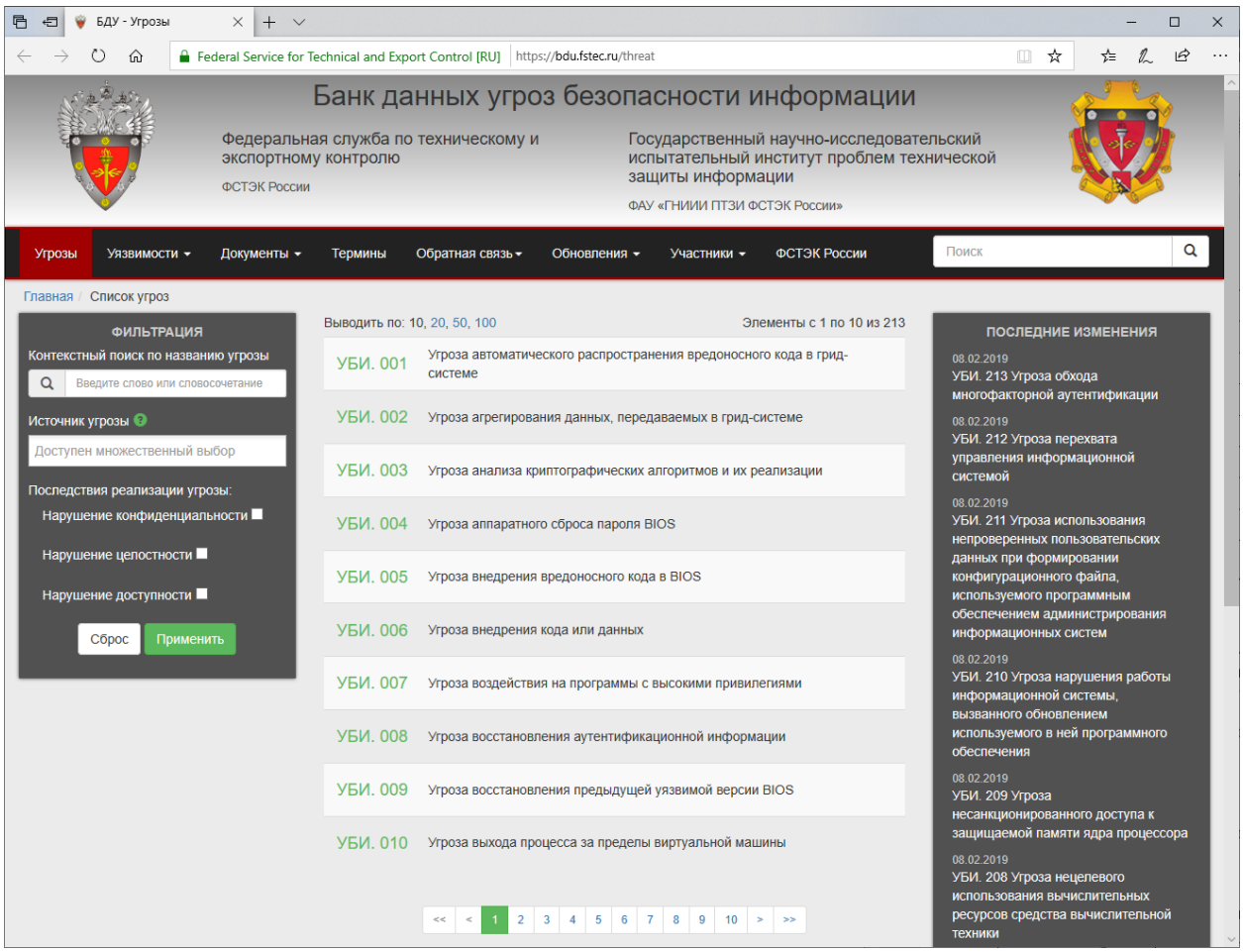


Рис. 5.1.2. **Банк данных угроз безопасности информации / Список угроз, https://bdu.fstec.ru/threat**

8. Введите в поле «Контекстный поиск по названию угрозы» (рис. 5.1.2) следующий текст: Угроза распространения.

9. Перейдите по ссылке номера угрозы, например, **УБИ. 172** и добавьте в отчет описание, источники, объект воздействия и последствия реализации каждой угрозы из представленного списка.

10. Зафиксируйте в отчете описание трех угроз, которые были добавлены в банк последними (рис. 5.1.2).

11. Найдите определение термина «Угроза», для этого перейдите по ссылке *Термины* (рис. 5.1.2). Для ускорения поиска выберите букву «У». Внесите в отчет определение на русском и английском языках, а также источник, в котором введен данный термин.

12. Внесите в отчет определение термина «Угроза безопасности информации».

13. Ответьте на вопросы для изучения в файле отчета. Номера вопросов определяются по начальной букве фамилии студента (табл. 5.1.2).

Таблица 5.1.2

Варианты к работе 5.1

Начальная буква фамилии студента	Номера вопросов	Начальная буква фамилии студента	Номера вопросов
А, И, С, Щ	1, 9, 17, 25	Д, Н, Х	5, 13, 21, 29
Б, К, Т	2, 10, 18, 26	Е, О, Ц, Ю	6, 14, 22, 30
В, Л, У, Э	3, 11, 19, 27	Ж, П, Ч	7, 15, 23, 31
Г, М, Ф	4, 12, 20, 28	З, Р, Ш, Я	8, 16, 24, 32

14. Представьте оформленный отчет по выполненной работе преподавателю на проверку.

Вопросы для изучения

1. Что такое защищаемая автоматизированная информационная система?
2. Что такое защищаемые информационные ресурсы?
3. Что такое защищаемая информационная технология?
4. Что такое безопасность информации [данных]?
5. Что такое безопасность информации (при применении информационных технологий)?
6. Что такое безопасность автоматизированной информационной системы?
7. Что называют источником угрозы безопасности информации?
8. Каковы источники угроз по природе их возникновения?
9. Что называют искусственными источниками угроз?
10. Как возникают непреднамеренные источники угроз?
11. Как возникают преднамеренные источники угроз?
12. Что называют естественными источниками угроз?
13. Каковы источники угроз по положению относительно контролируемой зоны?
14. Каковы источники внешних угроз?
15. Каковы источники внутренних?
16. К каким источникам угроз можно отнести действия людей, совершаемые ими с целью получения выгоды от доступа к защищаемой информации?
17. К каким источникам угроз относят стихийные природные явления, независящие от человека?
18. К каким источникам угроз относят техногенные катастрофы, возникающие на оборудовании, находящемся на территории контролируемой зоны?
19. Кого или что относят к субъектам доступа (в автоматизированной информационной системе)?

20. Как может быть осуществлен несанкционированный доступ к информации (данным)?

21. Для чего устанавливаются права и правила доступа к информации и ресурсам информационной системы?

22. Как определен термин «несанкционированное воздействие» в Р 50.1.053-2005?

23. Как может быть осуществлено несанкционированное воздействие на к информации (ресурсы автоматизированной информационной системы)?

24. Как может быть осуществлено изменение информации [ресурсов автоматизированной информационной системы] с нарушением установленных прав и (или) правил?

25. Как определен термин «блокирование доступа (к информации)» в Р 50.1.053-2005?

26. Когда может быть осуществлено создание условий, препятствующих доступу к информации?

27. Как определен термин «закладочное устройство» в Р 50.1.053-2005?

28. Что может быть выбрано в качестве мест установки закладочных устройств на охраняемой территории?

29. Как определен термин «программное воздействие» в Р 50.1.053-2005?

30. Как определен термин «вредоносная программа» в Р 50.1.053-2005?

31. Как определен термин «недекларированные возможности» в Р 50.1.053-2005?

32. Как может быть реализована программная закладка?

Практическая работа 5.2. Уязвимости информационных систем. Классификация уязвимостей информационных систем

Цель работы: изучить термины и классификацию уязвимостей информационных систем, установленных в стандарте Р 56546-2015.

Порядок выполнения работы

1. Изучить теоретический материал п. 5.2. «Уязвимости информационных систем» настоящего учебного пособия.

2. Выполнить задания практической части.

3. Представить оформленный отчет преподавателю.

Задания

1. Создайте файл отчета в MS Word. Сохраните файл под именем «Ваша фамилия52» (например: Иванов52).

2. Откройте в электронной профессиональной справочной системе «Кодекс»/»Техэксперт» национальный стандарт Российской Федерации ГОСТ Р 56546-2015, для чего:

— выйдите в Интернет на страницу http://docs.cntd.ru/document/1200123702 ;

— откроется страница сайта, содержащая текст документа (рис. 5.2.1), ознакомитесь с ее содержимым.

3. Изучите *Предисловие* документа. Внесите в отчет ответы на следующие вопросы:

– Кем разработан ГОСТ Р 56546-2015?

– Кем внесен ГОСТ Р 56546-2015?

– Когда утвержден и введен в действие ГОСТ Р 56546-2015?

– Если ГОСТ Р 56546-2015 введен не впервые, то укажите взамен какого?

4. Отразите в отчете область применения стандарта ГОСТ Р 56546-2015.

5. Внесите в отчет ответы на следующие вопросы:

– В комплекс каких стандартов входит ГОСТ Р 56546-2015?

– На какую деятельность распространяется стандарт ГОСТ Р 56546-2015?

– Какие нормативные ссылки использованы в стандарте ГОСТ Р 56546-2015?

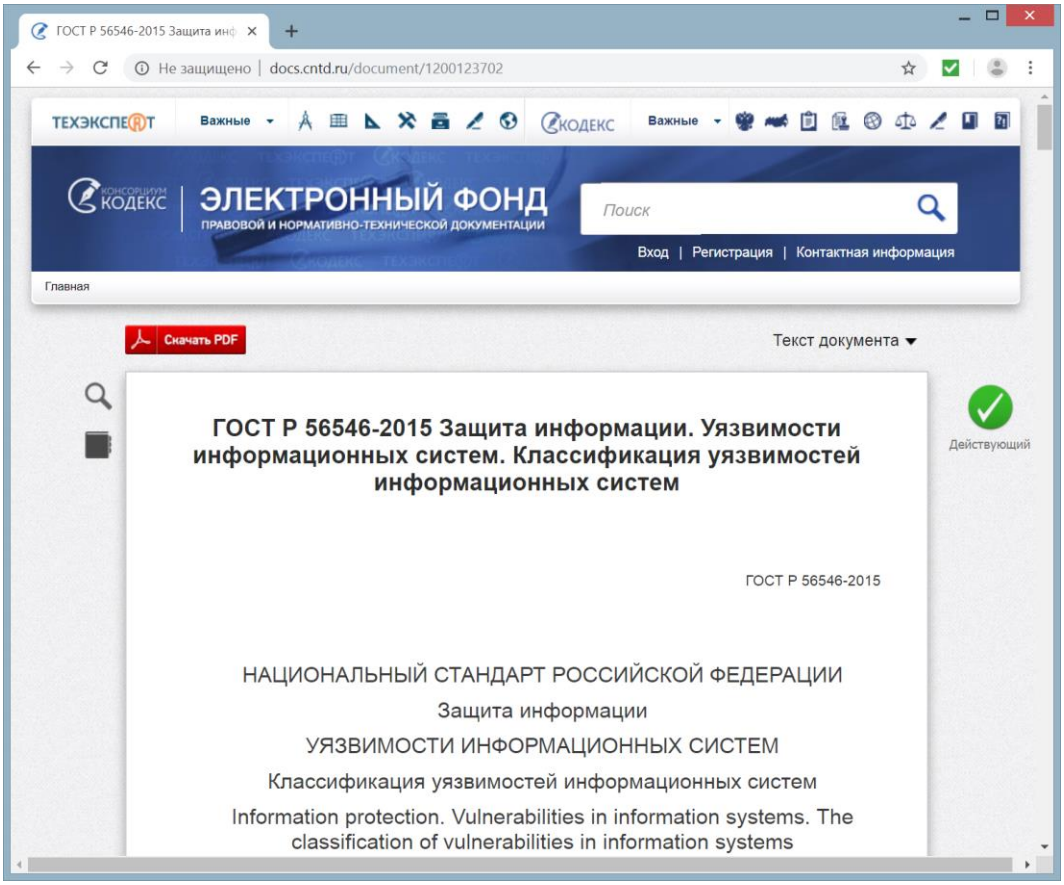


Рис. 5.2.1. **Текст документа ГОСТ Р 56546-2015 http://docs.cntd.ru/document/1200123702**

6. Перенесите в отчет и заполните табл. 5.2.1.

Таблица 5.2.1

Классы уязвимостей информационных систем по области происхождения

№	Термин	Определение
1.	Уязвимость кода	
2.	Уязвимость конфигурации	
3.	Уязвимость архитектуры	
4.	Организационная уязвимость	
5.	Многофакторная уязвимость	

7. Перенесите в отчет и заполните табл. 5.2.2.

Таблица 5.2.2

Классификация уязвимости ИС по типам недостатков ИС

№	Класс уязвимости ИС	Описание уязвимости ИС
1.		
2.		
3.		
…		

8. Перенесите в отчет и заполните табл. 5.2.3.

Таблица 5.2.3

Классификация уязвимости ИС по месту возникновения (проявления)

№	Класс уязвимости ИС	Описание уязвимости ИС
1.		
2.		
3.		
…		

9. Откройте *Список уязвимостей*, который создал и ведет Государственный научно-исследовательский испытательный институт проблем технической защиты информации (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»), перейдя по ссылке https://bdu.fstec.ru/vul (рис. 5.2.2).

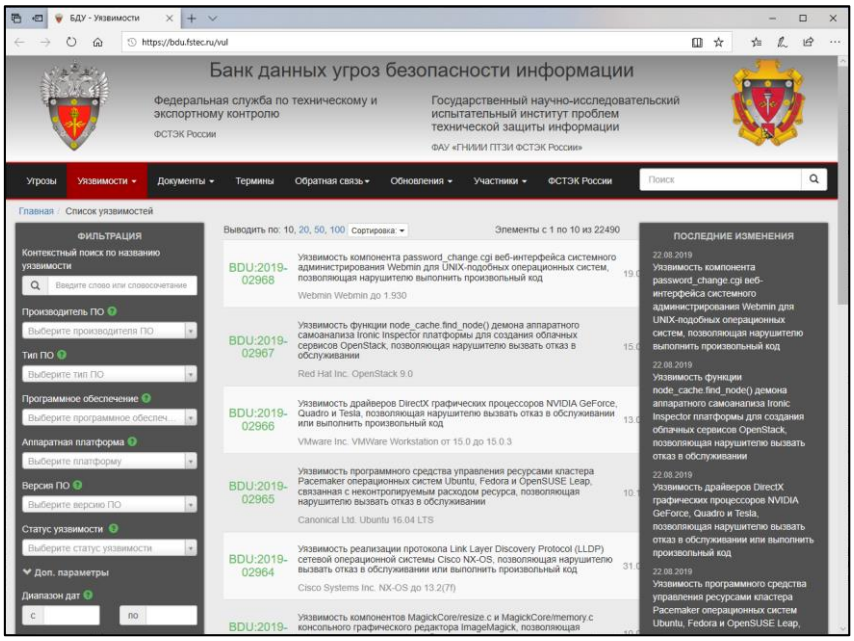


Рис. 5.2.2. **Банк данных угроз безопасности информации / Список уязвимостей, https://bdu.fstec.ru/vul**

10. Введите в поле «Контекстный поиск по названию уязвимости» (рис. 5.2.2) следующий текст: Уязвимость почтового сервера.

11. Откройте описание первой в списке уязвимости, перейдите по ссылке ее номера, например, BDU:2016-00107. Перенесите в отчет и заполните табл. 5.2.4.

Таблица 5.2.4

Описание уязвимости №_____

	Содержание	Комментарий
Описание уязвимости		
Вендор		Компания (организация) - производитель (разработчик) ПО, в котором обнаружена уязвимость
Наименование программного обеспечения		Наименование ПО, в котором обнаружена уязвимость
Версия программного обеспечения (ПО)		Версия ПО, в которой обнаружена уязвимость, или ПО, подверженное уязвимости

Тип программного обеспечения		Тип ПО, в котором обнаружена уязвимость
Операционные системы и аппаратные платформы		Операционная система, под управлением которой функционирует ПО с обнаруженной уязвимостью
Тип ошибки		
Класс уязвимости		Класс уязвимости, обнаруженной в ПО
Дата выявления		
Уровень опасности уязвимости		
Возможные меры по устранению уязвимости		

12. Зафиксируйте в отчете описание трех уязвимостей, которые были добавлены в банк последними (рис. 5.2.2).

13. Найдите определение термина «Уязвимость», для этого перейдите по ссылке *Термины* (рис. 5.2.2). Для ускорения поиска выберите букву «У». Внесите в отчет все найденные определения на русском и английском языках, а также источники, в которых введен данный термин.

14. Внесите в отчет определение термина «Уязвимость программного обеспечения».

15. Ответьте на вопросы для изучения в файле отчета. Номера вопросов определяются по начальной букве фамилии студента (табл. 5.2.4).

Таблица 5.2.4

Варианты к работе 5.2

Начальная буква фамилии студента	Номера вопросов	Начальная буква фамилии студента	Номера вопросов
А, И, С, Щ	1, 9, 17, 25	Д, Н, Х	5, 13, 21, 29
Б, К, Т	2, 10, 18, 26	Е, О, Ц, Ю	6, 14, 22, 30
В, Л, У, Э	3, 11, 19, 27	Ж, П, Ч	7, 15, 23, 31
Г, М, Ф	4, 12, 20, 28	З, Р, Ш, Я	8, 16, 24, 32

16. Представьте оформленный отчет по выполненной работе преподавателю на проверку.

Вопросы для изучения

1. Что такое информационная система?
2. Что такое информационная система?
3. Что такое признак классификации уязвимостей?
4. Что такое язык программирования?
5. Что такое степень опасности уязвимости?
6. Какие классификационные признаки лежат в основе классификации уязвимостей информационных систем?
7. Какие поисковые признаки предназначены для организации расширенного поиска в базах данных уязвимостей?
8. Какие признаки уязвимостей информационных систем относятся к основным поисковым признакам?
9. Какие признаки относятся к дополнительным поисковым признакам уязвимостей ИС?
10. На какие классы подразделяются уязвимости информационных систем по области происхождения?
11. В каких целях могут выделяться подклассы уязвимостей?
12. В чем заключается неправильная настройка параметров программного обеспечения?
13. В чем заключается недостаточность проверки вводимых (входных) данных?
14. В чем заключается прослеживание пути доступа к каталогам?
15. В чем заключается внедрение команд операционной системы?
16. Где обычно распространен межсайтовый скриптинг?
17. Когда возникает переполнение буфера?
18. Что относят к недостаткам, связанным с вычислениями?
19. Когда могут возникать недостатки, приводящие к утечке/раскрытию информации ограниченного доступа?
20. Что относят к недостаткам, связанным с управлением полномочиями (учетными данными)?
21. Что относят к недостаткам, связанным с управлением разрешениями, привилегиями и доступом?
22. Что относят к недостаткам, связанным с аутентификацией?
23. Что относят к недостаткам, связанным с криптографическими преобразованиями?
24. В чем заключается подмена межсайтового запроса?
25. Что такое «состоянию гонки»?
26. Что относят к недостаткам управления ресурсами?
27. Что относят к уязвимостям в общесистемном (общем) программном обеспечении?
28. Что относят к уязвимостям в прикладном программном обеспечении?
29. Что относят к уязвимостям в специальном программном обеспечении?

30. Что относят к уязвимостям в технических средствах?

31. Что относят к уязвимостям в сетевом (коммуникационном, телекоммуникационном) оборудовании?

32. Что относят к уязвимостям в средствах защиты информации?

Тема 6. Лицензирование в области технической защиты информации

Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» регулирует отношения, возникающие между федеральными органами исполнительной власти, органами исполнительной власти субъектов РФ, юридическими лицами и индивидуальными предпринимателями в связи с осуществлением лицензирования отдельных видов деятельности. Для целей настоящего Закона используются следующие основные понятия:

лицензирование — деятельность лицензирующих органов по предоставлению, переоформлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, осуществлению лицензионного контроля, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса, а также по предоставлению в установленном порядке информации по вопросам лицензирования;

лицензия — специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается документом, выданным лицензирующим органом на бумажном носителе или в форме электронного документа, подписанного электронной подписью, в случае, если в заявлении о предоставлении лицензии указывалось на необходимость выдачи такого документа в форме электронного документа;

лицензируемый вид деятельности — вид деятельности, на осуществление которого на территории РФ и на иных территориях, над которыми Российская Федерация осуществляет юрисдикцию в соответствии с законодательством РФ и нормами международного права, требуется получение лицензии в соответствии с настоящим Законом, в соответствии с федеральными

законами, указанными в ч. 3 ст. 1 Закона и регулирующими отношения в соответствующих сферах деятельности;

лицензирующие органы — уполномоченные федеральные органы исполнительной власти и (или) их территориальные органы, а в случае передачи осуществления полномочий Российской Федерации в области лицензирования органам государственной власти субъектов РФ органы исполнительной власти субъектов РФ, осуществляющие лицензирование;

соискатель лицензии — юридическое лицо или индивидуальный предприниматель, обратившиеся в лицензирующий орган с заявлением о предоставлении лицензии;

лицензиат — юридическое лицо или индивидуальный предприниматель, имеющие лицензию;

лицензионные требования — совокупность требований, которые установлены положениями о лицензировании конкретных видов деятельности, основаны на соответствующих требованиях законодательства РФ и направлены на обеспечение достижения целей лицензирования;

место осуществления отдельного вида деятельности, подлежащего лицензированию, — объект (помещение, здание, сооружение, иной объект), который предназначен для осуществления лицензируемого вида деятельности и (или) используется при его осуществлении, соответствует лицензионным требованиям, принадлежит соискателю лицензии или лицензиату на праве собственности либо ином законном основании, имеет почтовый адрес или другие позволяющие идентифицировать объект данные. Место осуществления лицензируемого вида деятельности может совпадать с местом нахождения соискателя лицензии или лицензиата.

В соответствии со ст.12 Федерального закона «О лицензировании отдельных видов деятельности» лицензированию подлежат 57 видов деятельности, в том числе:

– разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

– разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;

– деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если

указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

– разработка и производство средств защиты конфиденциальной информации;

– деятельность по технической защите конфиденциальной информации.

Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации (утверждено постановлением Правительства РФ от 3 марта 2012 г. № 171) определяет порядок лицензирования деятельности по разработке и производству средств защиты конфиденциальной информации (не содержащей сведения, составляющие государственную тайну, но защищаемой в соответствии с законодательством РФ), осуществляемой юридическими лицами и индивидуальными предпринимателями (рис. 6.1).

Разработка и производство средств защиты конфиденциальной информации, в том числе

- технических средств защиты информации;
- защищенных технических средств обработки информации;
- технических средств контроля эффективности мер защиты информации;
- программных (программно-технических) средств защиты информации;
- защищенных программных (программно-технических) средств обработки информации;
- программных (программно-технических) средств контроля защищенности информации.

Рис. 6.1. **Виды работ и услуг, подлежащие лицензированию**

Лицензирование деятельности по разработке и производству средств защиты конфиденциальной информации осуществляет ФСТЭК России, а в части разработки и производства средств защиты конфиденциальной информации, устанавливаемых на объектах Администрации Президента РФ, Совета Безопасности РФ, Федерального Собрания РФ, Правительства РФ, Конституционного Суда РФ и Верховного Суда РФ, — ФСБ России.

Положение о лицензировании деятельности по технической защите конфиденциальной информации (утверждено постановление Правительства РФ от 3 февраля 2012 г. № 79) определяет порядок лицензирования деятельности по технической защите конфиденциальной информации (не содержащей сведения, составляющие государственную тайну, но защищаемой в соответствии с законодательством РФ), осуществляемой юридическими лицами и индивидуальными предпринимателями.

Под *технической защитой конфиденциальной информации* понимается выполнение работ и (или) оказание услуг по ее защите от несанкционированного доступа, от утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней (рис. 6.2).

Лицензирование деятельности по технической защите конфиденциальной информации осуществляет ФСТЭК России.

Рис. 6.2. **Лицензируемые виды деятельности по технической защите конфиденциальной информации**

Контрольные вопросы и задания

1. Какие отношения регулирует Федеральный закон «О лицензировании отдельных видов деятельности»?
2. Когда не применяются положения Федерального закона «О лицензировании отдельных видов деятельности»?
3. Каковы цели и задачи лицензирования отдельных видов деятельности определены в Федеральном законе «О лицензировании отдельных видов деятельности»?
4. Какое положение определяет порядок лицензирования деятельности по разработке и производству средств защиты конфиденциальной информации?
5. Какие службы осуществляют лицензирование деятельности по разработке и производству средств защиты конфиденциальной информации?
6. Какие виды работ и услуг подлежат лицензированию при осуществлении деятельности по разработке и производству средств защиты конфиденциальной информации?
7. Какое положение определяет порядок лицензирования деятельности по технической защите конфиденциальной информации?
8. Что понимается под технической защитой конфиденциальной информации?
9. Какая служба осуществляет лицензирование деятельности по технической защите конфиденциальной информации?
10. Какие виды деятельности по технической защите конфиденциальной информации подлежат лицензированию?

Практическая работа 6.1. Основные положения и нормы Федерального закона «О лицензировании отдельных видов деятельности»

Цель работы: изучить основные положения Федерального закона 4 мая 2011 г. № 99-ФЗ, принципы правового регулирования отношений, возникающих в связи с осуществлением лицензирования отдельных видов деятельности.

Порядок выполнения работы

1. Изучить теоретический материал темы 6 «Лицензирование в области технической защиты информации» настоящего учебного пособия.
2. Выполнить задания, фиксируя каждый пункт работы в отчете.
3. Представить оформленный отчет преподавателю. Отчет должен содержать номера пунктов работы, их наименование и (в правой колонке) результат выполнения каждого пункта.

Задания

1. Запуск on-line версии КонсультантПлюс.

10. Создайте файл отчета в MS Word по образцу, приведенному в приложении. Сохраните файл под именем «Ваша фамилия61» (например: Иванов61). Заполните его шапку.

11. Запустите интернет-версию КонсультантПлюс, для чего:

— выйдите в Интернет на страницу http://www.consultant.ru/online (рис. 6.1.1);

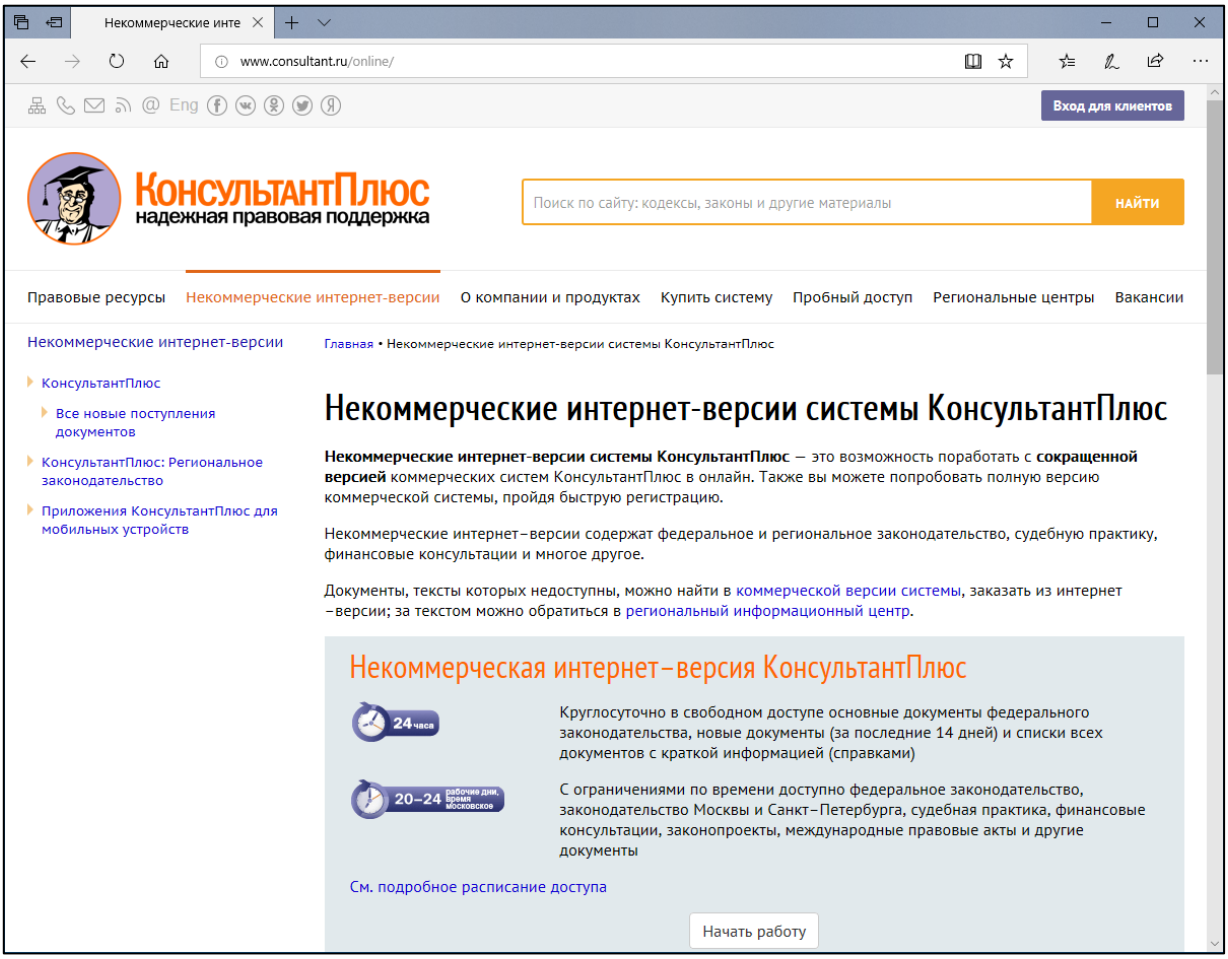


Рис. 6.1.1. **Интернет-страница КонсультантПлюс**

— перейдите на некоммерческую интернет-версию КонсультантПлюс по ссылке «Начать работу». Откроется первая страница системы (рис 6.1.2), ознакомитесь с ее содержимым;

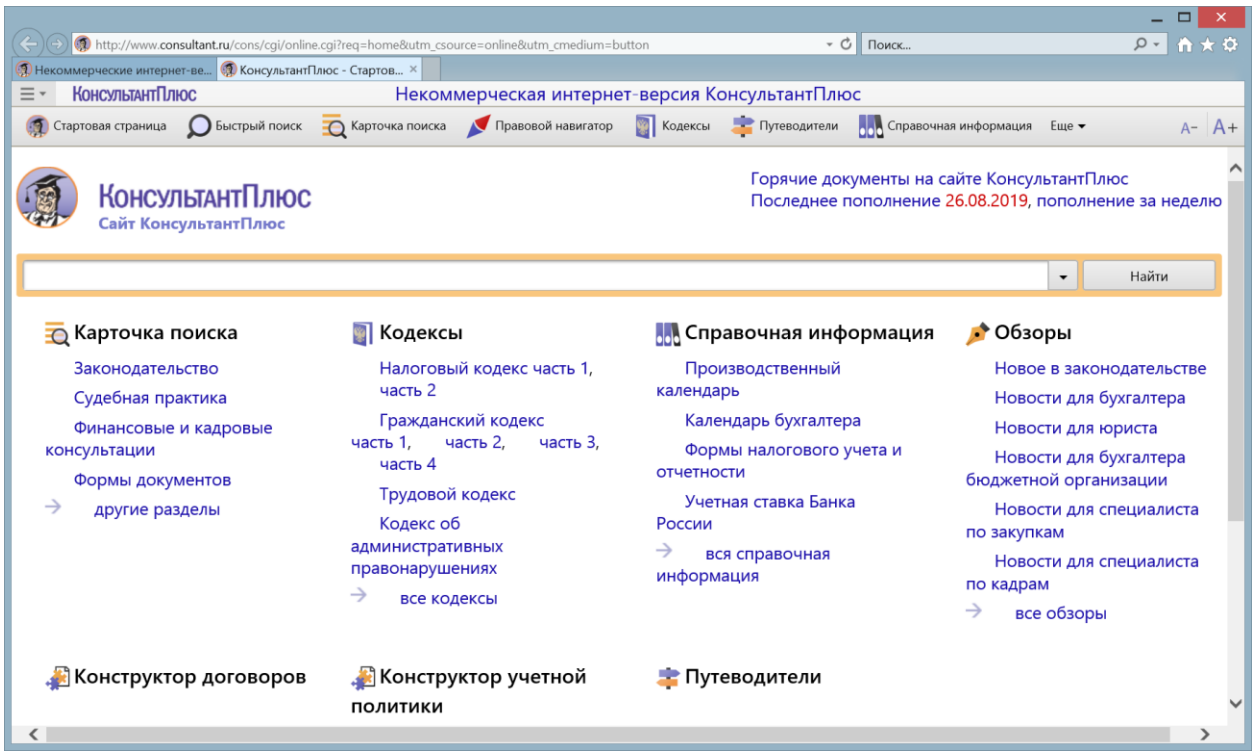


Рис. 6.1.2. **Некоммерческая интернет-версия КонсультантПлюс**

Зафиксируйте копию данной страницы в своем отчете.

12. Ознакомьтесь с расписанием доступа к некоммерческой версии КонсультантПлюс и *копию страницы с расписанием занесите в отчет*.

2. Работа с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

1. В строке быстрого поиска введите следующий текст: № 99-ФЗ и нажмите кнопку Найти.

КонсультантПлюс сформирует перечень документов, наиболее соответствующих запросу. Каждый документ сопровождается символом (означает, что текст документа находится в свободном доступе) или (означает, что текст документа в некоммерческой интернет-версии КонсультантПлюс в данный момент недоступен.).

Сохраните копию экрана со списком в отчете.

2. Откройте искомый Федеральный закон. Скорее всего он будет первым по списку. *Копию экрана занесите в отчет.*

3. Откройте и *занесите в отчет копии* следующих разделов, связанных с выбранным документом (рис 6.1.3):

— Дополнительная информация к документу;
— Обзор изменений документа;
— Сравнить с предыдущей редакцией.

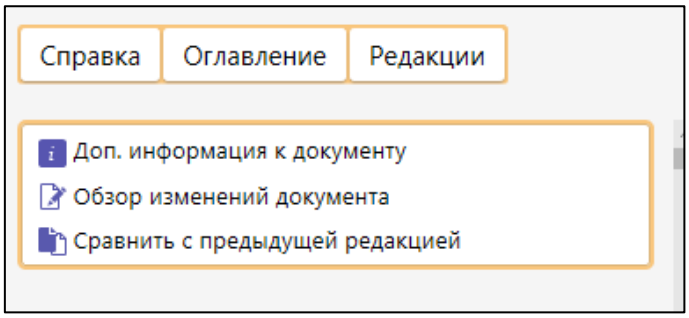


Рис. 6.1.3. **Разделы документа в КонсультантПлюс**

13. Используя кнопку *Редакции* (рис 6.1.3), определите действующую редакцию и редакции, еще не вступившие в силу. *Список редакций занесите в отчет*.

14. Откройте, ознакомьтесь и *скопируйте в отчет* для Федерального закона «О лицензировании отдельных видов деятельности» (рис 6.1.3):

— Справку;

— Оглавление.

15. Раскройте статью документа «Сфера применения настоящего Федерального закона» и *копию экрана занесите в отчет*.

16. Изучите отношения, связанные с осуществлением лицензирования, к которым не применяются положения настоящего Федерального закона. *Перенесите список данных отношений в отчет*.

17. Откройте Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне», для этого перейдите по ссылке деятельности (рис. 6.1.4).

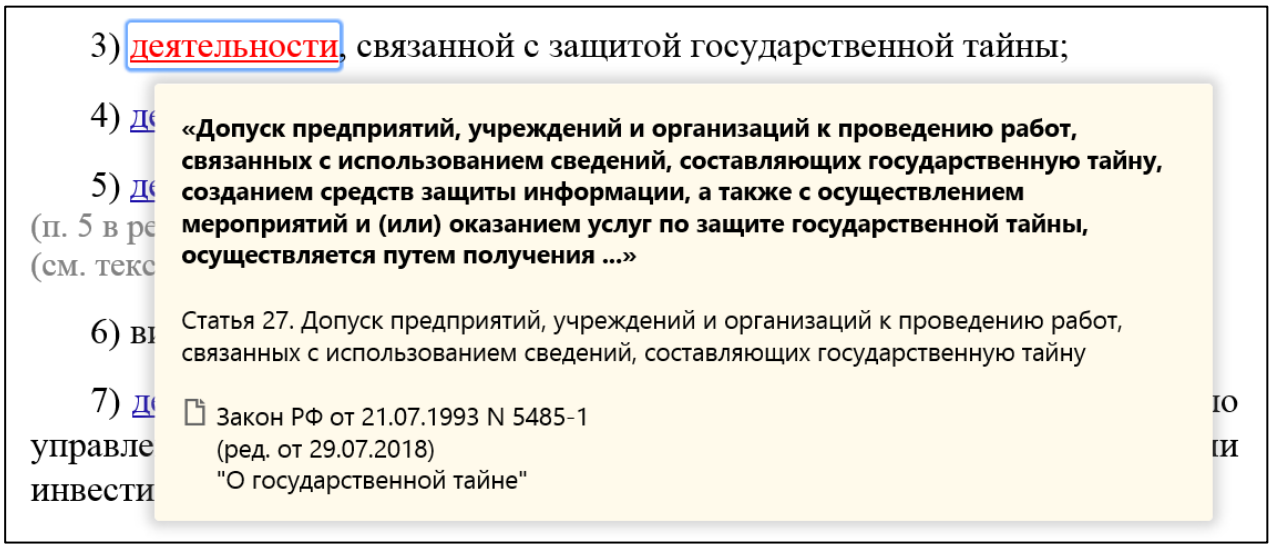


Рис. 6.1.4. **Статья 1. Сфера применения настоящего Федерального закона, пункт 2**

18. Найдите в тексте Закона РФ от 21.07.1993 № 5485-1 ответы на следующие вопросы и отобразите их в своем отчете:

– Как осуществляется допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а так-

же с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны?

– При каких условиях предприятию, учреждению и организации выдается лицензия на проведение работ с использованием сведений, составляющих государственную тайну?

3. Изучить основные понятия и положения Закона.

1. Вернитесь к тексту Федерального закона «О лицензировании отдельных видов деятельности».

2. Ответьте на вопросы для изучения в файле отчета. Номера вопросов определяются по начальной букве фамилии студента (табл. 6.1).

Таблица 6.1.1

Варианты к работе 6.1

Начальная буква фамилии студента	Номера вопросов	Начальная буква фамилии студента	Номера вопросов
А, И, С, Щ	1, 9, 17, 25	Д, Н, Х	5, 13, 21, 29
Б, К, Т	2, 10, 18, 26	Е, О, Ц, Ю	6, 14, 22, 30
В, Л, У, Э	3, 11, 19, 27	Ж, П, Ч	7, 15, 23, 31
Г, М, Ф	4, 12, 20, 28	З, Р, Ш, Я	8, 16, 24, 32

3. Представьте оформленный отчет по выполненной работе преподавателю на проверку.

Вопросы для изучения

1. Каковы цели лицензирования отдельных видов деятельности?
2. Каковы задачи лицензирования отдельных видов деятельности?
3. Как определено понятие «лицензирование» в Федеральном законе «О лицензировании отдельных видов деятельности»?
4. Как определено понятие «лицензия»?
5. Как определено понятие «лицензируемый вид деятельности»?
6. Как определено понятие «лицензирующие органы»?
7. Как определено понятие «соискатель лицензии»?
8. Как определено понятие «лицензиат»?
9. Как определено понятие «лицензионные требования»?
10. Какие основные принципы осуществления лицензирования определены в Федеральном законе «О лицензировании отдельных видов деятельности»?
11. Какие виды деятельности относятся к полномочиям Правительства РФ в области лицензирования?
12. Какие виды деятельности относятся к полномочиям лицензирующих органов?

13. Кому могут быть передано осуществление полномочий Российской Федерации в области лицензирования отдельных видов деятельности?

14. Каковы права должностных лиц лицензирующих органов при осуществлении лицензирования?

15. Каковы обязанности должностных лиц лицензирующих органов при осуществлении лицензирования?

16. В каких нормативных актах устанавливаются лицензионные требования?

17. Какие требования включают в себя лицензионные требования?

18. Какие требования могут быть включены в перечень лицензионных требований с учетом особенностей осуществления лицензируемого вида деятельности?

19. Какие требования не могут быть отнесены к лицензионным требованиям?

20. Каковы права юридических лиц или индивидуальных предпринимателей, получивших лицензию на вид деятельности?

21. Каков срок действия лицензии?

22. Подлежит ли лицензированию деятельность по разработке и производству средств защиты конфиденциальной информации?

23. Подлежит ли лицензированию деятельность по технической защите конфиденциальной информации?

24. Как оформляется решение о предоставлении лицензии или об отказе в ее предоставлении?

25. В течении какого срока после дня подписания и регистрации лицензии лицензирующим органом она вручается лицензиату или направляется ему заказным почтовым отправлением с уведомлением о вручении?

26. Каковы основания для отказа в предоставлении лицензии?

27. Какие документы лицензионный орган включает в лицензионное дело соискателя лицензии и/или лицензиата?

28. В течении какого срока со дня получения заявления о предоставлении дубликата лицензии лицензирующий орган оформляет дубликат лицензии?

29. Какие сведения являются предметом документарной проверки соискателя лицензии или лицензиата?

30. Что является предметом внеплановой выездной проверки соискателя лицензии или лицензиата?

31. Как часто могут проводится плановые проверки лицензиатов?

32. По каким основаниям проводятся внеплановые выездные проверки лицензиата?

Тема 7. Сертификация средств защиты информации

Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» определяет основные понятия в области сертификации:

сертификация — форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;

сертификат соответствия — документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;

система сертификации — совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом.

Положение о сертификации средств защиты информации (утверждено постановление Правительства РФ от 26 июня 1995 г. № 608) устанавливает порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом.

Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются *средствами защиты информации*.

Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных ФСБ России.

В соответствии с Положением о системе сертификации средств защиты информации (утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55) сертификации в системе сертификации ФСТЭК России подлежат:

– средства противодействия иностранным техническим разведкам, а также средства контроля эффективности противодействия иностранным техническим разведкам;

– средства технической защиты информации, включая средства, в которых они реализованы, а также средства контроля эффективности технической защиты информации;

– средства обеспечения безопасности информационных технологий, включая защищенные средства обработки информации.

Участниками системы сертификации ФСТЭК России являются:

– федеральный орган по сертификации (ФСТЭК России организует проведение сертификации средств защиты информации, разрабатывает и устанавливает в пределах своей компетенции требования по безопасности информации к средствам защиты информации, а также выполняет функции федерального органа по сертификации);

– организации, аккредитованные ФСТЭК России в качестве органа по сертификации (осуществляют сертификацию средств защиты информации, оформляют сертификаты соответствия средств защиты информации требованиям по безопасности информации);

– организации, аккредитованные ФСТЭК России в качестве испытательной лаборатории (проводят сертификационные испытания средств защиты информации и по их результатам оформляют технические заключения и протоколы. Испытательные лаборатории должны обеспечивать полноту сертификационных испытаний средств защиты информации и достоверность их результатов);

– изготовители средств защиты информации (разрабатывают и (или) производят средства защиты информации в соответствии с требованиями по безопасности информации. Изготовители средств защиты информации, составляющей государственную тайну, должны иметь лицензию ФСТЭК России на проведение работ, связанных с созданием средств защиты информации, составляющей государственную тайну. Изготовители средств защиты информации ограниченного доступа, не составляющей государственную тайну, должны иметь лицензию ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации).

Срок действия сертификата соответствия не может превышать пять лет. Сертификат соответствия (рис. 7.1) выдается на срок, указанный в заявке на сертификацию. По окончании срока действия сертификата соответствия заявитель вправе подать заявку на продление срока действия сертификата соответствия. Средство защиты информации может применяться по окончании срока действия сертификата соответствия при условии соблюдения требований по безопасности информации и осуществления заявителем его технической поддержки.

Сертификация средств защиты информации включает *процедуры*:

– подача заявки на сертификацию;

– принятие решения о проведении сертификации средства защиты информации;

– сертификационные испытания средства ЗИ;

– оформление экспертного заключения по результатам сертификации средства защиты информации и проекта сертификата соответствия;

– выдача (отказ в выдаче) сертификата соответствия;

– предоставление дубликата сертификата соответствия;

– маркирование средств защиты информации;

– внесение изменений в сертифицированное средство защиты информации;

– переоформление сертификата соответствия;

– продление срока действия сертификата соответствия;

– приостановление действия сертификата соответствия;

– прекращение действия сертификата соответствия.

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3840

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
25 декабря 2017 г.

Выдан: 25 декабря 2017 г. Переоформлен: 26 сентября 2018 г.
Действителен до: 25 декабря 2020 г.

Настоящий сертификат удостоверяет, что **программное изделие «Kaspersky Security 10.1 для Windows Server»,** разработанное и производимое АО «Лаборатория Касперского» в соответствии с техническими условиями ТУ 643.46856491.00084-03, является средством антивирусной защиты, соответствует требованиям по безопасности информации, установленным в задании по безопасности 643.46856491.00084-03 99 01, и документах «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012) и «Профиль защиты средств антивирусной защиты типа Б второго класса защиты. ИТ.САВ3.Б2.ПЗ» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре 643.46856491.00084-03 30 01.

Сертификат выдан на основании технического заключения от 15.11.2017, оформленного по результатам сертификационных испытаний испытательной лабораторией ЗАО ГИЦ ПС ВТ (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.Б005), экспертного заключения от 17.11.2017, оформленного органом по сертификации АО «БИТК» (аттестат аккредитации от 23.05.2016 № СЗИ RU.0001.01БИ00.А003), и технического заключения от 12.09.2018, оформленного по результатам инспекционного контроля испытательной лабораторией АО «СИНКЛИТ» аттестат аккредитации от 11.12.2017 № СЗИ RU.0001.01БИ00.Б025).

Заявитель: АО «Лаборатория Касперского» (ИНН 7713140469)
Адрес: 125212, г. Москва, Ленинградское шоссе, д. 39А, стр. 2
Телефон: (495) 797-8700

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Рис. 7.1. **Пример сертификата ФСТЭК России**

Действие сертификата соответствия *приостанавливается* в случаях:

– изменения требований по безопасности информации;

– установления факта несоответствия сертифицированного средства защиты информации требованиям по безопасности информации на основании поступившей в ФСТЭК России информации, в том числе о наличии в сертифицированном средстве защиты информации уязвимостей или недекларированных возможностей;

– прекращения технической поддержки сертифицированного средства защиты информации, отсутствие которой может привести к несоответствию средства защиты информации требованиям по безопасности информации, а также к невыполнению требований о защите информации при применении средства защиты информации;

– обращения заявителя о приостановлении действия сертификата соответствия.

Действие сертификата соответствия может быть *приостановлено* на срок не более 90 календарных дней. В случае приостановления действия сертификата соответствия заявитель должен прекратить производство и реализацию сертифицированного средства защиты информации.

Действие сертификата соответствия *возобновляется* в случае:

– устранения несоответствия средства защиты информации требованиям по безопасности информации и представления в ФСТЭК России материалов, подтверждающих устранение несоответствия;

– возобновления технической поддержки средства защиты информации;

– обращения заявителя о возобновлении действия сертификата соответствия в случае, если решение о приостановлении действия сертификата соответствия было принято по обращению заявителя.

Действие сертификата соответствия *прекращается* в случае:

– непредставления заявителем в установленный срок материалов, подтверждающих устранение несоответствия средства защиты информации требованиям по безопасности информации;

– невозобновления заявителем в установленный срок технической поддержки средства защиты информации;

– обращения заявителя о прекращении действия сертификата соответствия.

В случае прекращения действия сертификата соответствия заявитель должен прекратить производство и реализацию сертифицированного средства защиты информации, если такие мероприятия не были проведены в связи с приостановлением действия сертификата соответствия.

ФСТЭК России вносит сведения о приостановлении, возобновлении и прекращении действия сертификата соответствия в государственный реестр сертифицированных средств защиты информации (рис. 7.2).

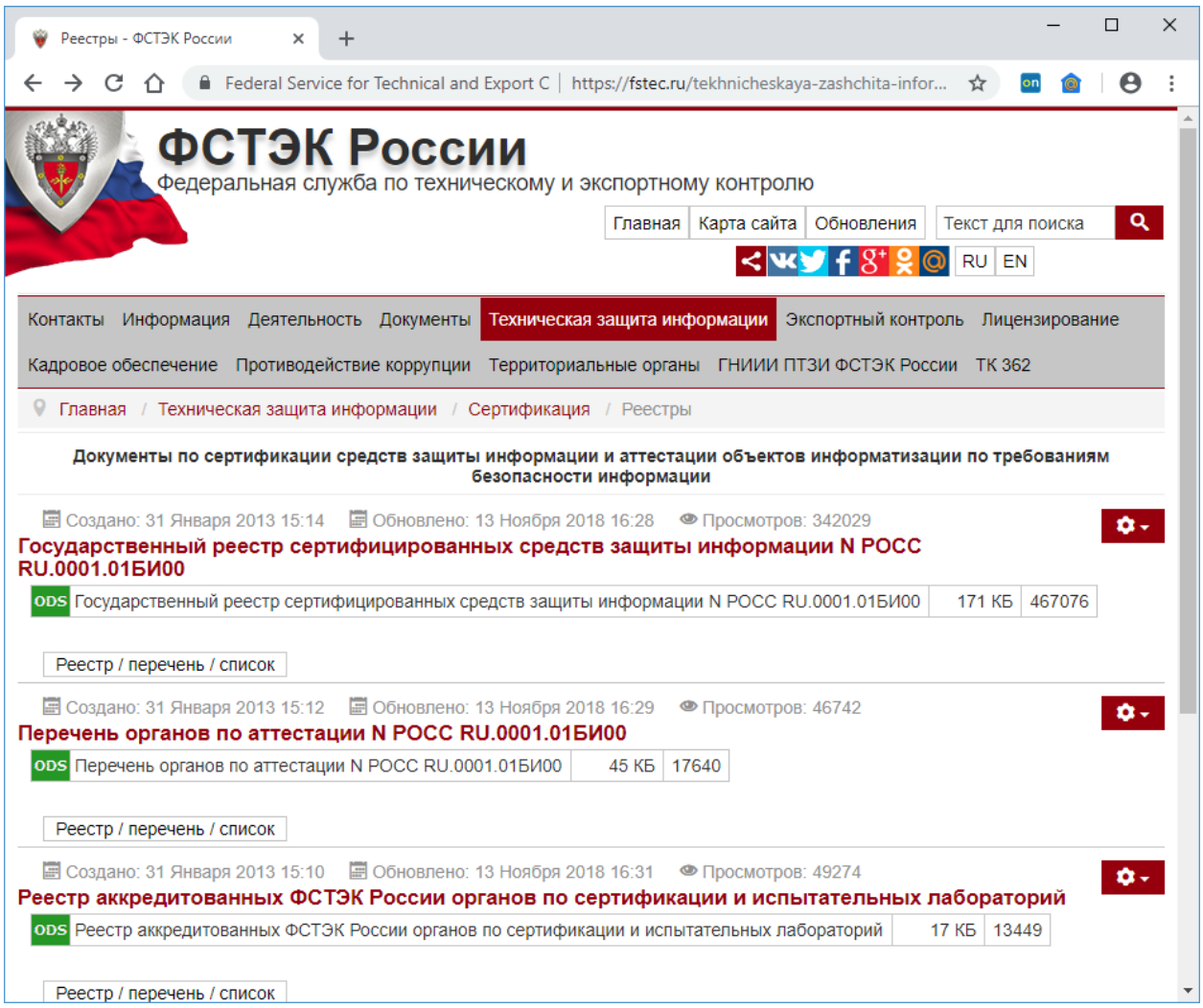


Рис. 7.2. **Официальный сайт ФСТЭК России**

Контрольные вопросы и задания

1. Какие отношения регулирует Федеральный закон «О техническом регулировании»?
2. Дайте определение понятию «риск» в соответствии с Федеральным законом «О техническом регулировании».
3. Дайте определение понятию «сертификация» в соответствии с Федеральным законом «О техническом регулировании».
4. Дайте определение понятию «сертификат соответствия» в соответствии с Федеральным законом «О техническом регулировании».
5. Дайте определение понятию «система сертификации» в соответствии с Федеральным законом «О техническом регулировании».
6. В соответствии с какими принципами осуществляется техническое регулирование?
7. Какое положение устанавливает порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом?
8. Что представляет собой система сертификации средств защиты информации?

9. Кем создаются системы сертифицирования средств защиты информации?

10. Кто является участниками сертификации средств защиты информации?

11. Что определяет Положение о системе сертификации средств защиты информации (утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55)?

12. Какие средства подлежат сертификации в системе сертификации ФСТЭК России?

13. Кто является участниками системы сертификации ФСТЭК России?

14. По какой схеме осуществляется сертификация средств защиты информации?

15. На сколько лет выдается сертификат соответствия на средства защиты информации?

16. Какие процедуры включает сертификация средства защиты информации?

Практическая работа 7.1. Основные положения и нормы документов по сертификации средств защиты информации

Цель работы: изучить основные положения документов по сертификации средств защиты информации, представленных на сайте Федеральной службы по техническому и экспортному контролю.

Порядок выполнения работы

1. Изучить теоретический материал темы 7 «Сертификация средств защиты информации» настоящего учебного пособия.
2. Выполнить задания, фиксируя каждый пункт работы в отчете.
3. Представить оформленный отчет преподавателю. Отчет должен содержать номера пунктов работы, их наименование и (в правой колонке) результат выполнения каждого пункта.

Задания

1. Создайте файл отчета в MS Word по образцу, приведенному в приложении. Сохраните файл под именем «Ваша фамилия71» (например: Иванов71). Заполните его шапку.
2. Перейдите на сайт Федеральной службы по техническому и экспортному контролю, для чего:

— выйдите в Интернет на страницу https://fstec.ru/ (рис. 7.1.1);

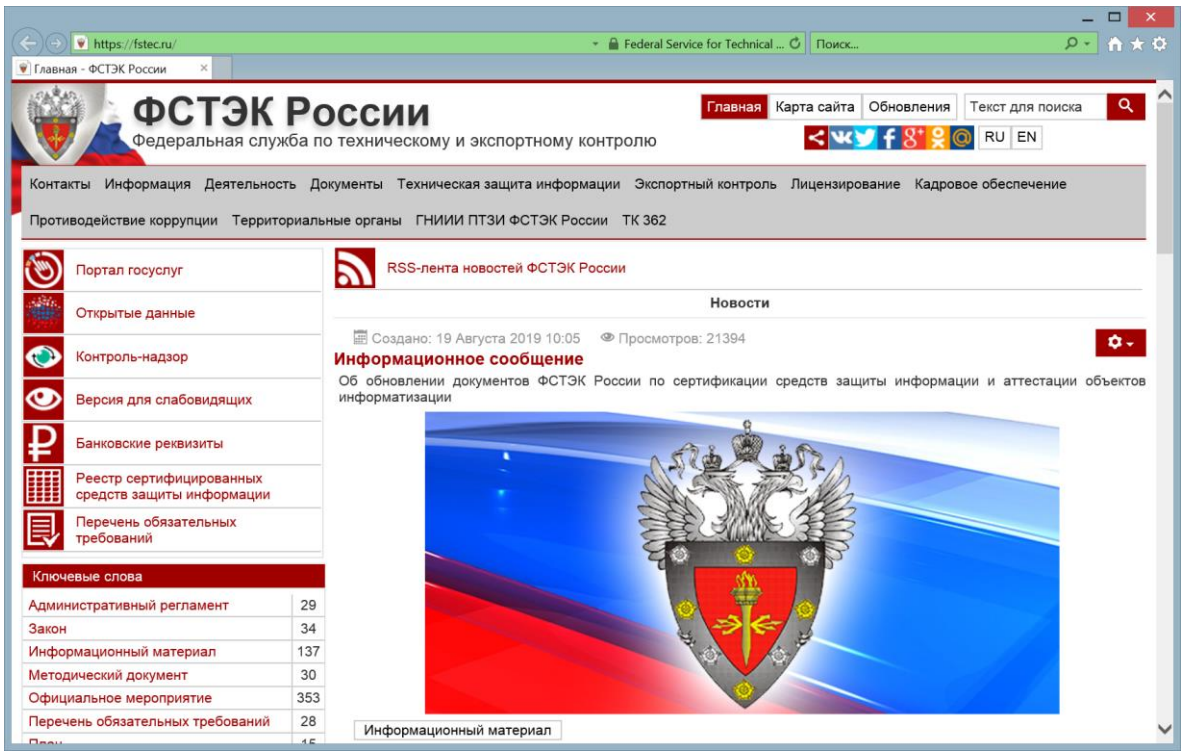


Рис. 7.1.1. **Сайт Федеральной службы по техническому и экспортному контролю, https://fstec.ru/**

3. Перейдите по ссылке *Документы / Сертификация* (рис. 7.1.2).

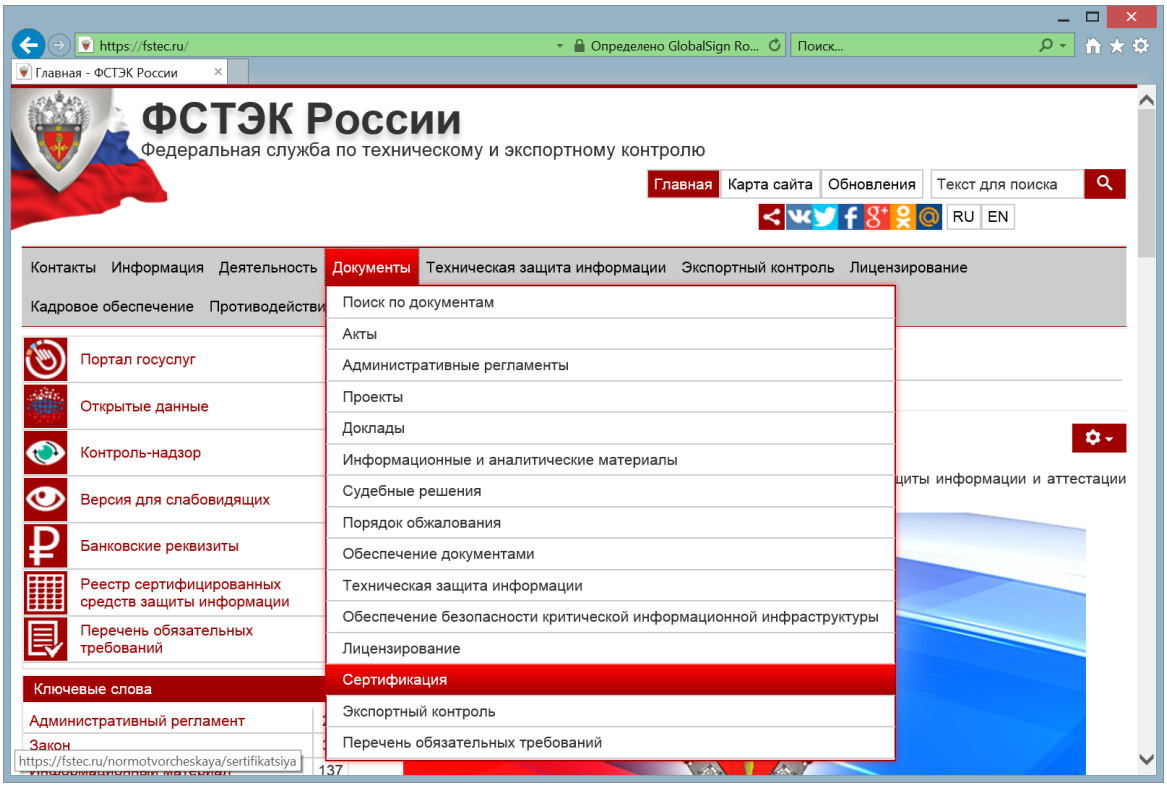


Рис. 7.1.2. **Сайт ФСТЭК России / Документы**

4. Изучите представленный список документов по сертификации средств защиты информации (рис. 7.1.3). Открывая каждую категорию, со-

держащую информационные материалы, *зафиксируйте копии страниц в своем отчете*.

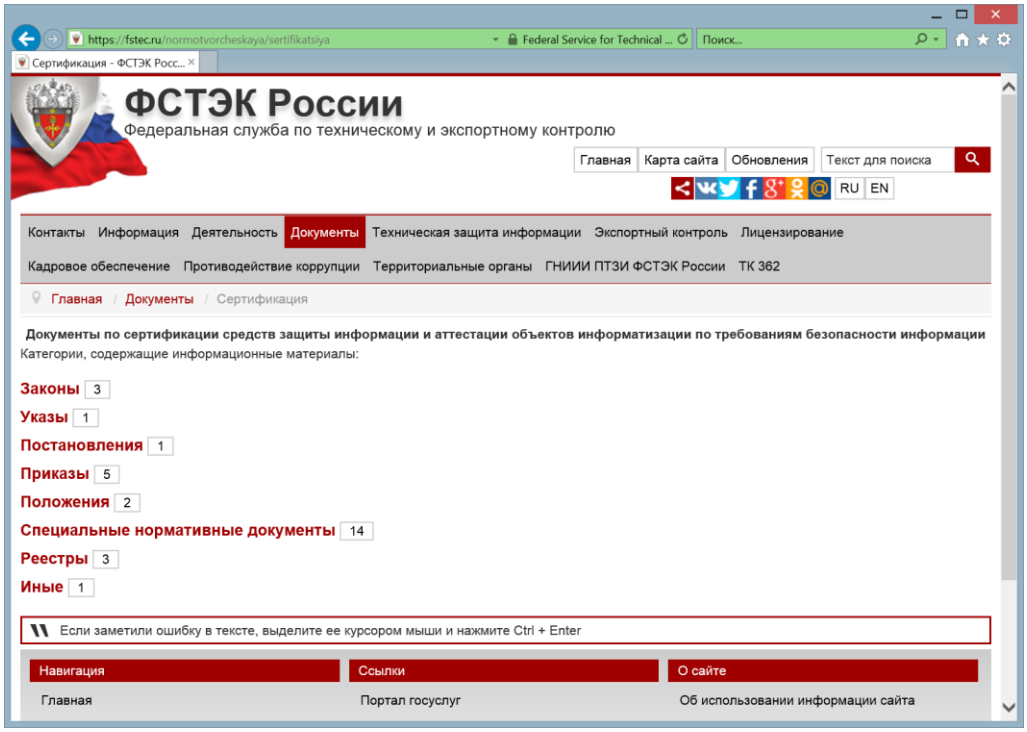


Рис. 7.1.3. **Сайт ФСТЭК России / Документы / Сертификация**

5. Перейдите в категорию *Постановления* (рис. 7.1.3).

5. Откройте *Положение о сертификации средств защиты информации*, перейдя по ссылке **Постановление Правительства Российской Федерации от 26 июня 1995 г. N 608** (рис. 7.1.4).

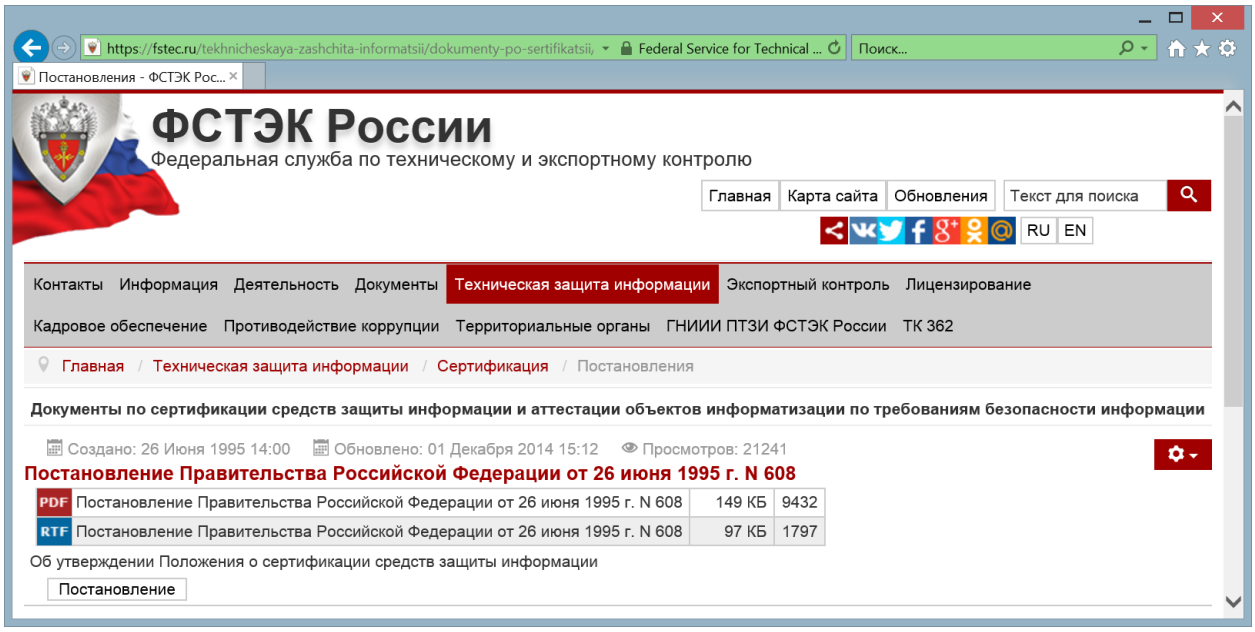


Рис. 7.1.4. **Сайт ФСТЭК России / Техническая защита информации / Сертификация / Постановления**

Зафиксируйте копию открывшейся страницы в своем отчете.

6. Отобразите в своем отчете ответы на вопросы:

– Что устанавливает *Положение о сертификации средств защиты информации*?

– Какие средства подлежат обязательной сертификации в соответствии с данным *Положением*?

7. Вернитесь к списку документов по сертификации средств защиты информации, перейдя к пункту *Сертификация* (рис. 7.1.4).

8. Перейдите в категорию *Положения* (рис. 7.1.3).

9. Откройте *Положением о системе сертификации средств защиты информации*, перейдя по ссылке **Положение. Утверждено приказом ФСТЭК России от 3 апреля 2018 г. N 55** (рис. 7.1.5).

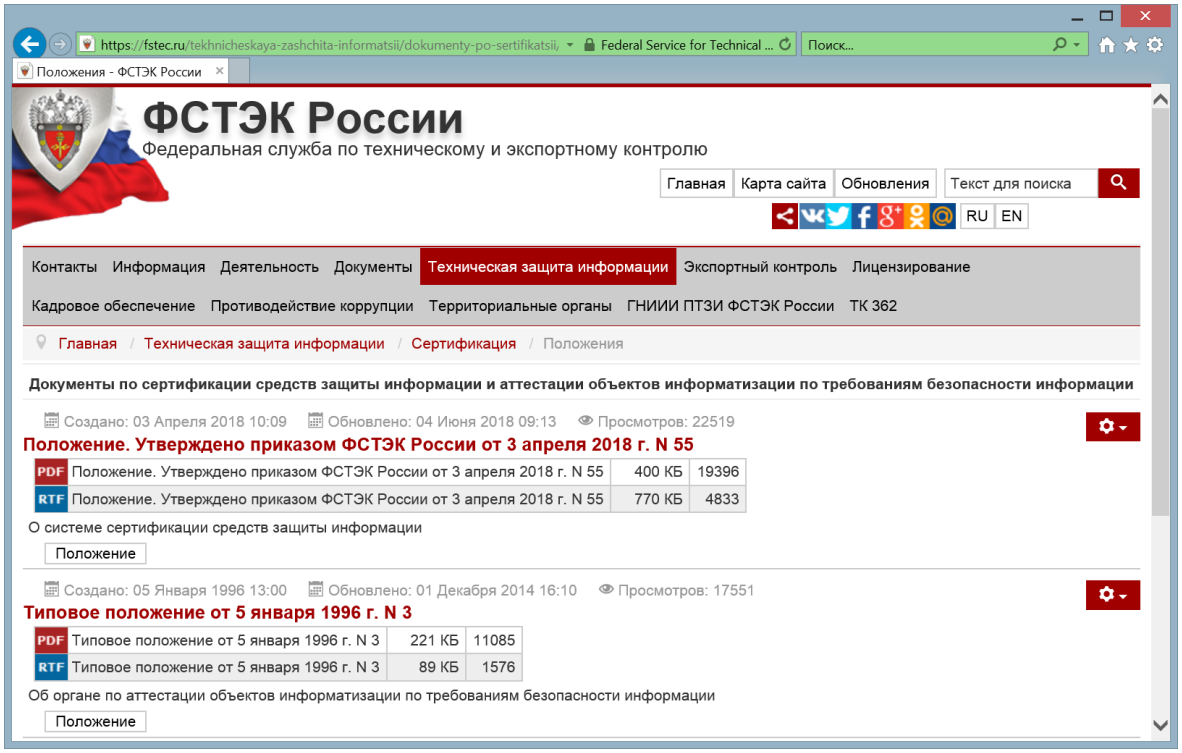


Рис. 7.1.5. **Сайт ФСТЭК России / Техническая защита информации / Сертификация / Положения**

Зафиксируйте копию открывшейся страницы в своем отчете.

10. Отобразите в своем отчете ответы на вопросы:

– В соответствии с какими законодательными и нормативными актами разработано *Положением о системе сертификации средств защиты информации*?

– Какие средства подлежат сертификации в системе сертификации ФСТЭК России в соответствии с данным *Положением*?

11. Вернитесь к списку документов по сертификации средств защиты информации, перейдя к пункту *Сертификация* (рис. 7.1.5).

12. Перейдите в категорию *Реестры* (рис. 7.1.3).

13. Откройте и изучите Государственный реестр сертифицированных средств защиты информации, *зафиксируйте копию страницы в своем отчете* (рис. 7.1.6).

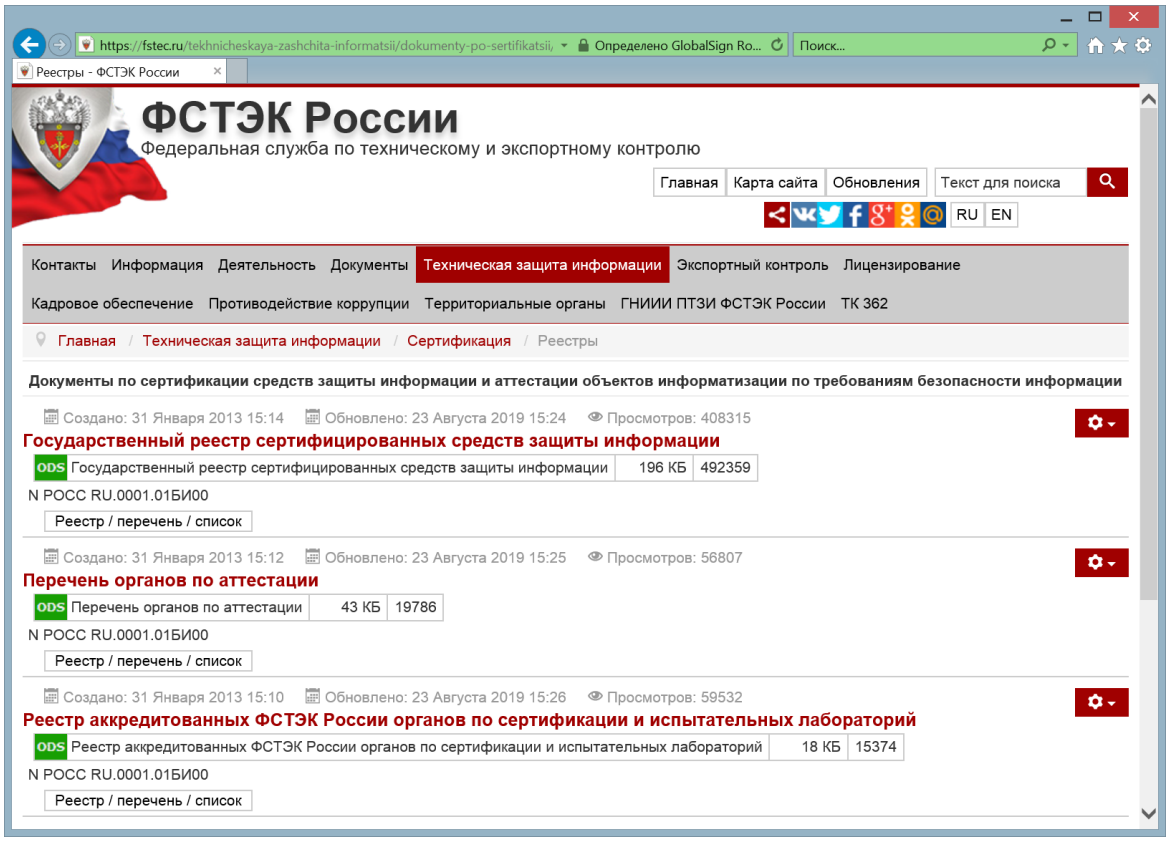


Рис. 7.1.6. **Сайт ФСТЭК России / Техническая защита информации / Сертификация / Реестры**

14. Откройте и изучите Реестр аккредитованных ФСТЭК России органов по сертификации и испытательных лабораторий, *зафиксируйте копию страницы в своем отчете* (рис. 7.1.6).

15. Ответьте на вопросы для изучения в файле отчета. Номера вопросов определяются по начальной букве фамилии студента (табл. 7.1.1).

Таблица 7.1.1

Варианты к работе 7.1

Начальная буква фамилии студента	Номера вопросов	Начальная буква фамилии студента	Номера вопросов
А, И, С, Щ	1, 9, 17, 25	Д, Н, Х	5, 13, 21, 29
Б, К, Т	2, 10, 18, 26	Е, О, Ц, Ю	6, 14, 22, 30
В, Л, У, Э	3, 11, 19, 27	Ж, П, Ч	7, 15, 23, 31
Г, М, Ф	4, 12, 20, 28	З, Р, Ш, Я	8, 16, 24, 32

16. Представьте оформленный отчет по выполненной работе преподавателю на проверку.

Вопросы для изучения

1. Какие средства являются средствами защиты информации в соответствии с Положением о сертификации средств защиты информации?
2. Как определено понятие «Система сертификации средств защиты информации» в Положении о сертификации средств защиты информации?
3. Какими органами создаются системы сертификации средств защиты информации?
4. На основе каких требований осуществляется сертификация средств защиты информации?
5. Какая комиссия осуществляет координацию работ по организации сертификации средств защиты информации?
6. Кто является участниками сертификации средств защиты информации в соответствии с Положением о сертификации средств защиты информации?
7. Каковы функции центральные органы системы сертификации, органы по сертификации средств защиты информации и испытательные лаборатории?
8. Какие функции выполняет Федеральный орган по сертификации?
9. Какие функции выполняет центральный орган системы сертификации?
10. Какие функции выполняет органы по сертификации средств защиты информации?
11. Какие функции выполняют испытательные лаборатории?
12. Какие функции выполняет изготовители в соответствии с Положением о сертификации средств защиты информации?
13. Каков срок действия сертификата в соответствии с Положением о сертификации средств защиты информации?
14. Как проводят испытания сертифицируемых средств защиты информации?
15. В каких случаях Федеральный орган по сертификации и органы по сертификации средств защиты информации имеет право приостанавливать или аннулировать действие сертификата?
16. Какой орган осуществляет инспекционный контроль за сертифицированными средствами защиты информации?
17. На основании каких требований осуществляется Сертификация средств защиты информации?
18. Кто является участниками системы сертификации ФСТЭК России являются в соответствии с Положением о системе сертификации средств защиты информации?
19. Какие органы осуществляют сертификацию средств защиты информации, оформляют сертификаты соответствия средств защиты информации требованиям по безопасности информации?
20. Какие мероприятия проводит испытательные лаборатории в соответствии с Положением о системе сертификации средств защиты информации?

21. Какие лицензии должны иметь изготовители средств защиты информации?

22. Каков срок действия сертификата в соответствии с Положением о системе сертификации средств защиты информации?

23. Кто может являться заявителями на осуществление сертификации?

24. Какие требования должны выполнить заявители на осуществление сертификации?

25. Какие процедуры включает сертификация средства защиты информации?

26. В какой срок ФСТЭК России принимает решение о выдаче сертификата соответствия?

27. В каких случаях сертификат соответствия подлежит переоформлению?

28. Каковы основания для отказа в переоформлении сертификата соответствия?

29. В каких случаях действие сертификата соответствия приостанавливается?

30. На какой срок действие сертификата соответствия может быть приостановлено?

31. В каких случаях действие сертификата соответствия возобновляется?

32. В каких случаях действие сертификата соответствия прекращается?

Тестовые задания

1. Какая информация подлежит защите *(выберите несколько вариантов ответа)*?

1) информация, которая не подлежит разглашению;
2) секретная информация;
3) важная информация;
4) оперативная информация;
5) конфиденциальная информация.

2. Какая информация относится к секретной?

1) информация, содержащая коммерческую тайну;
2) информация, содержащая банковскую тайну;
3) информация, содержащая персональные данные;
4) информация, содержащая врачебную тайну;
5) информация, содержащая государственную тайну.

3. Что относится к первоочередным задачам защиты информации *(выберите несколько вариантов ответа)*?

1) обеспечение качества информационных ресурсов и поддерживающей инфраструктуры;
2) обеспечение целостности информационных ресурсов и поддерживающей инфраструктуры;
3) обеспечение доступности информационных ресурсов и поддерживающей инфраструктуры;
4) обеспечение надежности информационных ресурсов и поддерживающей инфраструктуры;
5) обеспечение конфиденциальности информационных ресурсов и поддерживающей инфраструктуры.

4. В соответствии с Федеральным законом «Об информации, информационных технологиях и защите информации» информация делится на (*выберите несколько вариантов ответа*) …

1) конфиденциальную;
2) общедоступную;
3) государственную тайну;
4) ограниченного доступа.

5. В отношении информации, доступ к которой ограничен федеральными законами, необходимо соблюдать следующее требование:

1) обеспечение доступности;
2) обеспечение неотказуемости;
3) обеспечение конфиденциальности;
4) обеспечение целостности.

6. Информация, к которой нельзя ограничить доступ (*выберите несколько вариантов ответа*) — это:

1) информация о работе государственных органов;
2) информация об окружающей среде;
3) персональные данные субъекта;
4) информация о здоровье субъекта.

7. Какая информация подлежит защите?

1) информация, циркулирующая в системах и сетях связи;
2) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;
3) только информация, составляющая государственные информационные ресурсы;
4) любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

8. Базовый федеральный закон, регулирующий информационные отношения — это Федеральный закон:

1) «Об информации, информационных технологиях и защите информации»;
2) «О коммерческой тайне»;
3) «Об архивном деле в Российской Федерации»;
4) «О связи».

9. Классификация и виды информационных ресурсов определены:

1) Федеральным законом «Об информации, информатизации и защите информации»;
2) Гражданским кодексом РФ;
3) Конституцией РФ;
4) всеми перечисленными документами.

10. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам, — это …

1) обладатель информации;
2) создатель информации;
3) источник информации;
4) распространитель информации.

11. Защита от несанкционированного доступа к информации обеспечивает:

1) качество информации;
2) актуальность информации;
3) недоступность информации;

4) конфиденциальность информации;
5) неделимость информации.

12. Перечислите организации, входящие в состав системы государственного регулирования и контроля в области информационной безопасности *(выберите несколько вариантов ответа)*:

1) СВР России;
2) ФАПСИ России;
3) ФСТЭК России;
4) ФСБ России;
5) МВД России;
6) Правительство РФ;
7) Государственная Дума Федерального Собрания РФ.

13. Какой орган государственной власти координирует работу по защите информации, обрабатываемой техническими средствами?

1) ФСТЭК России;
2) ФСБ России;
3) ФСО России;
4) МВД России;
5) СВР России;

14. Что относится к основным задачам ФСТЭК России в области обеспечения информационной безопасности?

1) разработка отраслевых документов по защите информации;
2) противодействия иностранным техническим разведкам на территории РФ;
3) разработка криптографических методов защиты информации;
4) обеспечение передачи шифрованной информации в Российской Федерации и ее учреждениях, находящихся за пределами Российской Федерации.

15. Какой орган государственной власти обеспечивает безопасность информационно-телекоммуникационных систем криптографическими и инженерно-техническими методами?

1) ФСО России;
2) Минобороны России;
3) ФСБ России;
4) СВР России;
5) ФСТЭК России.

16. Перечислите основные составляющие Государственной системы защиты информации Российской Федерации *(выберите несколько вариантов ответа)*:

1) совокупность органов (ФСБ, ФСТЭК России), сил и средств, осуществляющих деятельность в области защиты информации;

2) система лицензирования деятельности в области технической защиты информации;

3) система государственного контроля всей информации, циркулирующей на территории РФ;

4) ужесточение норм и правил циркуляции конфиденциальной информации в информационных системах различных учреждений;

5) система сертификации средств защиты информации;

6) система подготовки и переподготовки специалистов в области защиты информации.

17. Выделите основные виды защиты информации *(выберите несколько вариантов ответа)*:

1) физическая защита информации;
2) экономическая защита информации;
3) межгосударственная защита информации;
4) правовая защита информации;
5) техническая защита информации;
6) научно-исследовательская защита информации.

18. К основным организационным мероприятиям по защите информации можно отнести:

1) организацию режима и охраны; организацию работы с сотрудниками; организацию работы с документами; организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации; организацию работы по анализу внутренних и внешних угроз конфиденциальной информации; организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией;

2) организацию охраны подвижных объектов; организацию работы с партнерами; организацию работы с документами; организацию контрразведывательных мероприятий; организацию работы по анализу внутренних и внешних угроз конфиденциальной информации; организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией;

3) организацию пропускного режима; организацию работы с клиентами; организацию использования технических средств сбора и хранения конфиденциальной информации; организацию аналитической работы;

4) организацию использования технических средств сбора, обработки, накопления и хранения информации; организацию работы по анализу внутренних и внешних угроз информации; организацию работы по проведению систематического контроля за работой персонала с информацией.

19. Силы и средства защиты организации в зависимости от решаемых задач, условий, специфических особенностей подразделяются на следующие основные направления защиты:

1) правовая защита, техническая защита, специальная защита, информационно-коммерческая защита;

2) правовая защита, техническая защита, организационная защита;

3) физическая защита, специальная защита, информационно-коммерческая защита;

4) физическая защита, техническая защита, специальная защита, морально-психологическая защита.

20. Как называется мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений?

1) создание системы защиты информации;
2) административное мероприятие;
3) организационное мероприятие;
4) техническое мероприятие.

21. В ходе какого этапа построения системы защиты информации определяются основные направления защиты персональных данных и производится выбор способов защиты?

1) формирование замысла защиты;
2) построение частной модели угроз;
3) оценка обстановки;
4) решение вопросов управления защитой.

22. Каковы организационные требования к системе защиты информации?

1) управленческие и идентификационные;
2) административные и аппаратурные;
3) административные и процедурные;
4) аппаратурные и физические.

23. Какие различают способы доступа к информации *(выберите несколько вариантов ответа)*?

1) за счет разглашения;
2) за счет системной несогласованности;
3) за счет утечки;
4) за счет несанкционированного доступа;
5) за счет административной ошибки.

24. Какие средства входят в состав техники защиты информации *(выберите несколько вариантов ответа)*?

1) антивирусное программное обеспечение;

2) средство защиты информации от утечки по техническим каналам;
3) средство защиты информации от несанкционированного доступа;
4) средство защиты информации от кибератак;
5) межсетевой экран;
6) средство поиска закладочных устройств;
7) средство защиты информации от технической разведки.

25. Какие различают методы защиты информации *(выберите несколько вариантов ответа)*?
1) интерактивные;
2) пассивные;
3) активные;
4) статические.

26. Укажите основные средства защиты информации по виду исполнения *(выберите несколько вариантов ответа)*?
1) электромагнитные средства;
2) средства специального назначения;
3) технические средства;
4) программные средства;
5) программно-технические средства;
6) высокочастотные средства;
7) компьютерные средства.

27. Назовите основной принцип физической защиты информации:
1) территориальная согласованность защиты;
2) организационная обоснованность защиты;
3) универсальность защитных механизмов;
4) непрерывность защиты в пространстве времени;
5) открытость защитных механизмов.

28. Перечислите основные направления физической защиты информации *(выберите несколько вариантов ответа)*:
1) физическое управление доступом;
2) меры по обнаружению стратегических ресурсов;
3) противопожарные меры;
4) управление информационными потоками;
5) защита поддерживающей инфраструктуры.

29. К какой группе относятся мероприятия, направленные на применение организационных мер и программно-технических способов защиты информации на объекте информатизации?
1) организационно-технические мероприятия;
2) технические мероприятия;
3) организационные мероприятия;

4) нормативно-правовые мероприятия;
5) инженерно-технические мероприятия;
6) программно-технические мероприятия.

30. Проведение каких действий предусматривают организационные мероприятия по обеспечению защиты информации *(выберите несколько вариантов ответа)*?

1) создание активных помех техническим средствам злоумышленников;
2) определение границ контролируемой (охраняемой) зоны;
3) выявление возможных путей проникновения к источникам защищаемой информации со стороны злоумышленников;
4) организация ложной работы технических средств связи и обработки информации;
5) показ ложных демаскирующих признаков деятельности и опознавания;
6) реализация мер по обнаружению, выявлению и контролю за обеспечением защиты информации всеми доступными средствами.

31. Определите основные классы технических средств, используемых при проведении организационно-технических мероприятий *(выберите несколько вариантов ответа)*:

1) комплексные средства защиты;
2) средства пассивной защиты;
3) скрытые средства защиты;
4) средства активной защиты;
5) средства постоянной защиты.

32. К основным средствам защиты информации относят *(выберите несколько вариантов ответа)*:

1) технические средства, предназначенные или используемые для защиты информации;
2) программные средства, предназначенные или используемые для защиты информации;
3) скрытые средства защиты;
4) программно-технические средства, предназначенные или используемые для защиты информации;
5) вещество и материал, предназначенные или используемые для защиты информации:
6) электронные средства, предназначенные или используемые для защиты информации;
7) компьютерные средства, предназначенные или используемые для защиты информации;
8) аппаратные средства, предназначенные или используемые для защиты информации.

33. Что понимается под совокупностью информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов, в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров?

1) система защиты информации;
2) объект защиты информации;
3) объект информатизации;
4) автоматизированная информационная система в защищенном исполнении.

34. Что понимается под информацией (носителем информации, информационным процессом), которую необходимо защищать в соответствии с целью защиты информации?

1) система защиты информации;
2) объект защиты информации;
3) объект информатизации;
4) автоматизированная информационная система в защищенном исполнении.

35. Что понимается под информацией (носителем информации, информационным процессом), которую необходимо защищать в соответствии с целью защиты информации?

1) система защиты информации;
2) объект защиты информации;
3) объект информатизации;
4) автоматизированная информационная система в защищенном исполнении.

36. Какие средства защиты информации относят к технике защиты информации *(выберите несколько вариантов ответа)*?

1) средства физической защиты информации;
2) программно-технические средства, предназначенные или используемые для защиты информации
3) криптографические средства защиты информации;
4) технические средства, предназначенные или используемые для защиты информации;
5) программные средства, предназначенные или используемые для защиты информации;
6) средства контроля эффективности защиты информации;
7) средства и системы управления, предназначенные для обеспечения защиты информации.

37. Лицо, заинтересованное в получении возможности несанкционированного доступа к конфиденциальной информации, представляющей промышленную и коммерческую тайну, предпринимающее попытку такого доступа или совершившее его — это:

1) вредитель;
2) злоумышленник;
3) нарушитель;
4) хакер.

38. Слабое место в системном обеспечении информационной системы, которое может быть использовано для реализации угрозы безопасности информации, называется:

1) уязвимостью;
2) угрозой;
3) недостатком;
4) брешью.

39. Наличие межсетевого экрана необходимо при:

1) использовании изолированной локальной сети;
2) использовании сетей общего пользования;
3) использовании почтового ящика в сети Интернет;
4) использовании автономного автоматизированного рабочего места.

40. Лицо, преднамеренно использующее уязвимости технических и нетехнических мер и средств контроля и управления безопасностью с целью захвата или компрометации информационных систем и сетей, или снижения доступности ресурсов информационной системы и сетевых ресурсов для законных пользователей — это:

1) вредитель;
2) злоумышленник;
3) нарушитель;
4) хакер.

41. Количественная или качественная характеристика безопасности информации, определяющая уровень требований, предъявляемых к конфиденциальности, целостности и доступности этой информации и реализуемых при ее обработке — это:

1) допустимый риск;
2) уровень защищенности информации;
3) показатель защищенности информации;
4) вероятность защищенности информации.

42. Что понимается под совокупностью органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованной и функционирующей по правилам и нормам,

установленным соответствующими документами в области защиты информации?

1) система защиты информации;
2) объект защиты информации;
3) объект информатизации;
4) автоматизированная информационная система в защищенном исполнении.

43. Способом несанкционированного доступа к источникам конфиденциальной информации называется:

1) потенциальные или реальные действия, приводящие к моральному или материальному ущербу;
2) спонтанное не зависящее от воли людей обстоятельство, возникающее в информационной системе в процессе ее функционирования, приводящее к утечке информации;
3) совокупность приемов и порядок действий с целью получения (добывания) охраняемых сведений незаконным, противоправным путем;
4) негативное воздействие на систему в целом или отдельные ее элементы, оказываемое какими-либо явлениями, происходящими внутри системы или во внешней среде.

44. К основным способам несанкционированного доступа к защищаемой информации относят *(выберите несколько вариантов ответа)*?

1) авторизованный вход в информационную систему;
2) инициативное сотрудничество;
3) актуализация базы данных;
4) хищение;
5) перехват;
6) копирование.

45. Степень опасности источника информации определяется:

1) размером потенциальных затрат злоумышленника на проникновение к данному источнику информации;
2) количеством способов несанкционированного доступа к источнику информации;
3) величиной доступности данного источника, определяемой экспертной комиссией;
4) количеством информации, содержащимся в этом источнике;
5) размером ущерба, наносимого при использовании данного источника.

46. Что относится к источникам информации?

1) отдельные материальные объекты;
2) субъекты, обладающие генетической памятью;

3) субъекты и объекты, обладающие определенной информацией, которая представляет конкретный интерес для злоумышленников или конкурентов;

4) определенные субъекты;

5) материальные носители информации, представляющей интерес только для специалистов определенных сфер деятельности.

47. Как показывает практика, выявить злоумышленника очень сложно, в первую очередь следует заботиться:

1) об уменьшении ущерба;
2) увеличении срока действия средств обработки информации;
3) уменьшении срока хранения информации;
4) уменьшении криминогенной обстановки вокруг организации;
5) увеличении объемов защищаемой информации.

48. Из перечисленного:

а) степень прогнозируемости;
б) природа происхождения;
в) предпосылки появления;
г) источники угроз;
д) размер ущерба

являются параметрами классификации угроз безопасности информации.

1) а, д
2) в, г, д
3) б, в, г
4) а, б, в

49. Из перечисленного:

а) случайная;
б) преднамеренная;
в) стихийная;
г) детерминированная;
д) объективная;
е) субъективная

классифицируются как угрозы безопасности по природе происхождения.

1) а, б, в, г
2) д, е
3) в, г
4) а, б

50. Нормативный документ, регламентирующий все аспекты безопасности продукта информационных технологий, называется:

1) системой защиты
2) стандартом безопасности
3) профилем безопасности
4) профилем защиты.

51. Что понимается под разглашением информации?

1) несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации;

2) передача сведений конфиденциального характера их обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены данным договором;

3) бесконтрольный выход защищаемой информации за пределы организации или круга лиц, которым она была доверена;

4) ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя при условии сохранения конфиденциальности данной информации.

52. Что такое «утечка информации»?

1) противоправное преднамеренное овладение защищаемой информацией;

2) умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним;

3) неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками;

4) ознакомление определенных лиц с защищаемой информацией с согласия ее обладателя.

53. Что такое «несанкционированный доступ к информации»?

1) противоправное преднамеренное овладение защищаемой информацией;

2) умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним;

3) доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа;

4) изменение информации, осуществляемое с нарушением установленных прав и (или) правил.

54 Что такое «несанкционированное воздействие на информацию»?

1) противоправное преднамеренное овладение защищаемой информацией;

2) умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним;

3) доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа;

4) изменение информации, осуществляемое с нарушением установленных прав и (или) правил.

55. Посредством чего осуществляется утечка информации?

1) активных соединений;

2) организационных мероприятий;
3) формальных коммуникаций;
4) различных технических каналов;
5) неформальных коммуникаций.

56. Что понимают под каналом утечки информации?
1) физический путь от источника информации к ее получателю;
2) физический путь от источника защищаемой информации к злоумышленнику;
3) материальные объекты, в том числе физические поля, в которых защищаемая информация находит свое отображение;
4) часть пространства, в которой перемещается носитель защищаемой информации.

57. Перечислите основные способы несанкционированного доступа к информации *(выберите несколько вариантов ответа)*:
1) уничтожение носителей информации;
2) подслушивание телефонных переговоров;
3) порча технических средств;
4) кража документов;
5) проникновение в информационную систему.

58. Под угрозой безопасности информации понимают:
1) нестабильное состояние мировой экономики;
2) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;
3) совокупность условий и факторов, влияющих на циркуляцию информации в каналах связи;
4) такое состояние информационной системы, при котором она, с одной стороны, не способна противостоять дестабилизирующему воздействию внешних и внутренних факторов, а с другой — ее функционирование создает опасность для элементов самой системы и внешней среды.

59. Перечислите возможные последствия реализации той или иной угрозы безопасности информации *(выберите несколько вариантов ответа)*:
1) фиксация информации;
2) изменение информации;
3) уничтожение информации;
4) обновление информации;
5) хищение информации;
6) сокрытие информации;
7) блокирование информации.

60. Как называется попытка реализации угрозы безопасности информации?

1) нападение;
2) нарушение статичности;
3) атака;
4) обвал.

61. Одном их источников угрозы безопасности информации являются:
1) потенциальные злоумышленники;
2) компрометирующие ситуации;
3) благоприятные факторы;
4) непредсказуемые последствия;
5) сложные обстоятельства.

62. Перечислите основные виды реализации угроз безопасности информации *(выберите несколько вариантов ответа)*:
1) распространение источника защищаемой информации;
2) создание среды распространения защищаемой информации;
3) воздействие на источник защищаемой информации;
4) несанкционированное распространение носителя защищаемой информации;
5) хищение получателя защищаемой информации.

63. Угрозы, приводящие к несанкционированному распространению информации от носителя защищаемой информации к злоумышленнику, называют угрозами:
1) модификации информации;
2) утечки информации;
3) разрушения информации;
4) проявления стихии;
5) действия помех.

64. Действия, совершаемые злоумышленниками с корыстной целью, называют:
1) точечными;
2) разрушительными;
3) непреднамеренными;
4) преднамеренными;
5) спровоцированными;
6) губительными.

65. Действия, ошибочно совершаемые людьми, приводящие к угрозе безопасности информации, называют:
1) точечными;
2) разрушительными;
3) непреднамеренными;
4) спровоцированными;

5) преднамеренными;
6) губительными.

66. Физические процессы или стихийные природные явления, не зависящие от человека, приводящие к угрозе безопасности информации, называются:

1) точечными;
2) разрушительными;
3) стихийными;
4) естественными;
5) спровоцированными;
6) губительными.

67. Что можно отнести к естественным источникам угроз безопасности информации *(выберите несколько вариантов ответа)*?

1) проявление стихии;
2) атаки хакеров;
3) действия помех;
4) сбои аппаратуры;
5) ошибки программ;
6) деструктивное воздействие со стороны обиженных сотрудников.

68. Что образуют внешние воздействия (силы), которые могут изменить, уничтожить информацию или привести к ее хищению, при распространении от источника внешнего воздействия до источника информации?

1) технический канал утечки информации;
2) канал несанкционированного доступа;
3) среду распространения носителя информации;
4) канал преобразования информации;
5) опасный сигнал.

69. Какие действия пользователя информации и злоумышленника создают угрозу утечки информации *(выберите несколько вариантов ответа)*?

1) утеря источника информации (документа, продукции и др.);
2) разглашение сведений;
3) регулярная проверка помещений на наличие закладных устройств;
4) соблюдение режима коммерческой тайны в организации;
5) перехват электромагнитных полей и электрических сигналов, содержащих защищаемую информацию;
6) утилизация всех отходов дело- и промышленного производства.

70. Как называется прием оптических и иных сигналов от объектов и получение с их помощью изображений этих объектов?

1) подслушивание;
2) наблюдение;

3) перехват;
4) фиксация;
5) регистрация.

71. Как называется процесс приема и анализа акустических сигналов?
1) наблюдение;
2) перехват;
3) хищение;
4) фиксация;
5) подслушивание.

72. Как называется процесс обнаружения, приема и обработки информативных сигналов?
1) демодуляция;
2) консервация;
3) перехват;
4) преобразование;
5) регистрация.

73. Что понимается под совокупностью правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности?
1) информационная политика;
2) безопасность информации;
3) политика безопасности;
4) регламентация доступа;
5) профиль защиты;
6) организация защиты.

74. На чем основывается политика безопасности в организации?
1) на выявлении всех возможных угроз безопасности информации организации;
2) поиске уязвимостей информационной системы организации;
3) анализе рисков, признанных реальными для информационной системы организации;
4) закупке оборудования, предотвращающего утечку информации по техническим каналам;
5) регистрации всех действий персонала при работе с защищаемой информацией.

75. Что понимают под совокупностью типовых требований по обеспечению безопасности информации, которые должны быть реализованы в защищаемой автоматизированной информационной системе?
1) информационная политика;
2) безопасность информации;

3) политика безопасности;
4) регламентация доступа;
5) профиль защиты;
6) организация защиты.

76. Какие механизмы безопасности необходимо использовать в рамках современных информационных систем *(выберите несколько вариантов ответа)*?

1) квотирование;
2) идентификация и аутентификация пользователей;
3) управление доступом;
4) резервное копирование;
5) мониторинг и аудит безопасности информации;
6) обеспечение высокой производительности системы;
7) обновление программного обеспечения.

77. Что представляет собой уровень риска с количественной точки зрения *(выберите несколько вариантов ответа)*?

1) вероятность реализации определенной угрозы;
2) степень защищенности информационной системы организации;
3) показатель доступности защищаемых информационных ресурсов организации;
4) величину возможного ущерба;
5) величину надежности системы защиты информации.

78. Какие действия включает в себя управление рисками?

1) централизация рисков;
2) оценка рисков;
3) оптимизация рисков;
4) локализация рисков;
5) уменьшение рисков.

79. Что из нижеперечисленного можно отнести к этапам управления рисками *(выберите несколько вариантов ответа)*?

1) выбор анализируемых объектов и уровня детализации их рассмотрения;
2) выбор методологии оценки рисков;
3) инкапсуляция результатов оценки рисков;
4) идентификация активов;
5) идентификация пассивов;
6) выбор защитных мер;
7) деструктуризация существующей системы защиты;
8) реализация и проверка выбранных мер;
9) оценка остаточного риска.

80. Помимо всего прочего в отраслях промышленности и в регионах страны для обеспечения информационной безопасности создаются *(выберите несколько вариантов ответа)*:

1) лицензионные центры;
2) центры по эксплуатации информационных технологий;
3) органы по аттестации объектов информатизации;
4) органы по тестированию средств вычислительной техники;
5) центры по аудиту защиты информации.

81. Лицензиат — это:

1) специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю;
2) подтверждение соответствия продукции или услуг установленным требованиям или стандартам;
3) государственный орган, осуществляющий лицензирование в соответствии с законодательством РФ;
4) вид деятельности, на осуществление которого на территории РФ требуется получение лицензии;
5) юридическое лицо или индивидуальный предприниматель, имеющие лицензию.

82. Как называют специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности, которое подтверждается документом?

1) лицензия;
2) сертификат;
3) аттестат соответствия;
4) документ соответствия.

83. Что такое сертификация?

1) подтверждение соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров;
2) предоставление в органы государственной власти информации об используемых средствах защиты информации;
3) специальная проверка, по результатам которой выдается разрешение на осуществление определенного вида деятельности;
4) представление различной информации посредством штрих-кодов.

84. Какой документ подтверждает соответствие средства защиты информации требованиям по безопасности информации?

1) технический паспорт средства защиты информации;
2) лицензия на средство защиты информации;

3) спецификация средства защиты информации;
4) сертификат на средство защиты информации;

85. Перечислите государственные органы, уполномоченные на ведение лицензионной деятельности в области защиты информации *(выберите несколько вариантов ответа)*:

1) ФСБ России;
2) ФАПСИ России;
3) ФСО России;
4) ФСТЭК России;
5) МВД России.

86. На какие виды деятельности не распространяется действие Федерального закона «О лицензировании отдельных видов деятельности»?

1) деятельность, связанная с защитой государственной тайны;
2) деятельность, связанная с защитой конфиденциальной информации;
3) предоставление услуг в области шифрования информации;
4) деятельность кредитных организаций;
5) использование атомной энергии;
6) деятельность по выдаче сертификатов ключей электронных подписей.

87. Какие средства подлежат сертификации в системе сертификации ФСТЭК России?

1) средства иностранного производства, обеспечивающие защиту информации;
2) средства противодействия иностранным техническим разведкам;
3) средства технической защиты информации;
4) средства, обеспечивающие защиту государственной тайны различных степеней секретности;
5) средства обеспечения безопасности информационных технологий.

88. Укажите срок действия сертификата соответствия средства защиты информации:

1) не более 5 лет;
2) не более 6 лет;
3) не более 8 лет;
4) от 2 до 4 лет;
5) от 3 до 6 лет;

89. Укажите на какой срок может быть приостановлено действие сертификата соответствия средства защиты информации

1) на срок не более 90 календарных дней;
2) на срок не более 30 календарных дней;
3) на срок не менее 90 календарных дней;

4) на срок не менее 30 календарных дней;
5) на срок не более 45 календарных дней.

90. Какой участник процесса сертификации оформляет экспертное заключение по сертификации средств защиты информации?

1) органы по сертификации средств защиты информации;
2) заявитель;
3) федеральный орган по сертификации;
4) испытательные лаборатории.

Алфавитный указатель терминов

Приложение

ОТЧЕТ **о выполнении практической работы** **по дисциплине**		
Студент		
Группа		Дата
№	Содержание пункта работы / вопроса	Результат выполнения пункта работы (копии экрана) / Ответ на вопрос
1		
2		
3		
4		
5		

Рекомендуемые источники

1. Груздева, Л. М. Основы информационной безопасности: учеб. пособие / Л. М. Груздева. — М. : Юридический институт МИИТа, 2018.

2. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков. — 6-е изд. — М. : Академия, 2012.

3. Астахова, А. В. Информационные системы в экономике и защита информации на предприятиях — участниках ВЭД : учеб. пособие / А. В. Астахова. — СПб. : Троицкий мост, 2014.

4. Чеботарева, А. А. Информационное право : учеб. пособие / А. А. Чеботарева. — М. : Юридический институт МИИТа, 2014.

5. Информационные технологии в юридической деятельности / под ред. В. Д. Элькина. — М. : Издательство Юрайт, 2013.

6. Карпов, В. И Основы теории обеспечения безопасности личности, общества и государства : учеб. пособие / В. И. Карпов, О. Н. Новокшанов, Д. Б. Павлов. — М. : Юридический институт МИИТа, 2010.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»:

1. http://docs.cntd.ru — сайт консорциума Кодекс, электронный фонд правовой и нормативно-технической документации
2. http://www.consultant.ru — Консультант +: законодательство РФ
3. http://fstec.ru/ — официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России)
4. http://www.scrf.gov.ru/ — официальный сайт Совета безопасности Российской Федерации
5. http://fsb.ru — официальный сайт Федеральной службы безопасности Российской Федерации (ФСБ России)