МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«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.

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие
в двух частях

Часть I

МОСКВА—2017

УДК 001.1
ББК 32.81
Г—87

Груздева, Л. М. Основы информационной безопасности : учеб. пособие в двух частях. — Ч. 1 / Л. М. Груздева. — М. : Юридический институт МИИТа, 2017. — 101 с.

В учебном пособии изложены правовые основы обеспечения информационной безопасности, в том числе политика государства в области информатизации общества, отрасли информационных технологий и национальной безопасности. Особое внимание уделено рассмотрению классификации информации, подлежащей защите в соответствии с законодательством Российской Федерации, а также государственной системе защиты информации.

Учебное пособие предназначено для студентов Юридического института РУТ (МИИТ), обучающихся по программам бакалавриата 40.03.01 «Юриспруденция» и специалитета 40.05.01 «Правовое обеспечение национальной безопасности», 40.05.02 «Правоохранительная деятельность», 40.05.03 «Судебная экспертиза», 38.05.02 «Таможенное дело».

Пособие включает широкий перечень контрольных вопросов и тестовых заданий, может быть полезно преподавателям информационно-правого цикла, а также широкому кругу читателей, самостоятельно изучающих вопросы информационной безопасности.

При работе с изданием использовалась справочная правовая система КонсультантПлюс.

Изд. заказ 11	Подписано в печать 06.03.2018	Тираж 200 экз.
Усл.-печ. л. 6,3	Уч.-изд. л. 4,7	Формат $60\times90^{1}/_{16}$

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

Содержание

Введение

Важное место в подготовке специалистов юридического профиля занимают вопросы информационной безопасности, что обусловлено масштабами проникновения информационных технологий в повседневную жизнь граждан, организаций и органов власти всех уровней. При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз (совокупности действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере).

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

В результате освоения модуля «Основы информационной безопасности» студент должен овладеть следующими компетенциями:

- готовностью к выполнению должностных обязанностей по обеспечению законности и правопорядка, безопасности личности, общества, государства (ПК-8[1]);
- способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности (ПК-9[2], ПК-16[3], ПК-22[4]);
- способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1[5]).

[1] ФГОС ВО по направлению подготовки 40.03.01 Юриспруденция (уровень бакалавриата), утвержденный приказом Минобрнауки России от 1 декабря 2016 г. № 1511.

[2] ФГОС ВО по специальности 40.05.03 Судебная экспертиза (уровень специалитета), утвержденный приказом Минобрнауки России от 28 октября 2016 г. № 1342.

[3] ФГОС ВО по специальности 40.05.01 Правовое обеспечение национальной безопасности (уровень специалитета), утвержденный приказом Минобрнауки России от 19 декабря 2016 г. № 1614.

[4] ФГОС ВО по специальности 40.05.02 Правоохранительная деятельность (уровень специалитета), утвержденный приказом Минобрнауки России от 16 ноября 2016 г. № 1424.

[5] ФГОС ВО по специальности 38.05.02 Таможенное дело (уровень специалитета), утвержденный приказом Минобрнауки России от 17 августа 2015 г. № 850.

Тема 1. Политика государства в области информатизации общества и отрасли информационных технологий

Формирование и развитие информационного общества[1] в Российской Федерации обеспечит конкурентоспособность России, развитие экономической, социально-политической, культурной и духовной сфер жизни общества, а также совершенствование системы государственного управления на основе использования информационных технологий (ИТ).

Стратегия развития информационного общества в Российской Федерации на 2017—2030 годы, утвержденная Указом Президента РФ от 9 мая 2017 г. № 203, определяет цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики[2], обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Целью настоящей Стратегии является создание условий для формирования в Российской Федерации *общества знаний* — общества, в котором преобладающее значение для развития гражданина, экономики и государства имеют получение, сохранение, производство и распространение достоверной информации с учетом стратегических национальных приоритетов Российской Федерации. Обеспечение национальных интересов при развитии информационного общества осуществляется путем реализации следующих приоритетов:

а) формирование информационного пространства[3] с учетом потребностей граждан и общества в получении качественных и достоверных сведений;

б) развитие информационной и коммуникационной инфраструктуры Российской Федерации;

в) создание и применение российских информационных и коммуникационных технологий, обеспечение их конкурентоспособности на международном уровне;

г) формирование новой технологической основы для развития эконо-

[1] *Информационное общество* — общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан.

[2] *Цифровая экономика* — хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг.

[3] *Информационное пространство* — совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры.

мики и социальной сферы;

д) обеспечение национальных интересов в области цифровой экономики.

Для устойчивого функционирования информационной инфраструктуры Российской Федерации необходимо:

а) обеспечить единство государственного регулирования, централизованные мониторинг и управление функционированием информационной инфраструктуры Российской Федерации на уровне информационных систем и центров обработки данных, а также на уровне сетей связи;

б) обеспечить поэтапный переход государственных органов и органов местного самоуправления к использованию инфраструктуры электронного правительства[1], входящей в информационную инфраструктуру Российской Федерации;

в) обеспечить использование российских криптоалгоритмов и средств шифрования при электронном взаимодействии федеральных органов исполнительной власти, органов государственной власти субъектов РФ, государственных внебюджетных фондов, органов местного самоуправления между собой, а также с гражданами и организациями;

г) осуществить скоординированные действия, направленные на подключение объектов к информационной инфраструктуре Российской Федерации;

д) заменить импортное оборудование, программное обеспечение и электронную компонентную базу российскими аналогами, обеспечить технологическую и производственную независимость и информационную безопасность;

е) обеспечить комплексную защиту информационной инфраструктуры Российской Федерации, в том числе с использованием государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы и системы критической информационной инфраструктуры;

ж) проводить непрерывный мониторинг и анализ угроз, возникающих в связи с внедрением новых информационных технологий, для своевременного реагирования на них;

з) обеспечить единство сетей электросвязи Российской Федерации, в том числе развитие и функционирование сетей связи государственных органов и органов местного самоуправления, а также интегрированной сети связи для нужд обороны страны, безопасности государства и обеспечения правопорядка.

Основными направлениями развития российских информационных и коммуникационных технологий, перечень которых может быть изменен по

[1] *Инфраструктура электронного правительства* — совокупность размещенных на территории РФ государственных информационных систем, программно-аппаратных средств и сетей связи, обеспечивающих при оказании услуг и осуществлении функций в электронной форме взаимодействие органов государственной власти РФ, органов местного самоуправления, граждан и юридических лиц.

мере появления новых технологий, являются:

– конвергенция сетей связи и создание сетей связи нового поколения[1];

– обработка больших объемов данных[2];

– искусственный интеллект;

– доверенные технологии электронной идентификации и аутентификации, в том числе в кредитно-финансовой сфере;

– облачные[3] и туманные вычисления[4];

– интернет вещей[5] и индустриальный интернет[6];

– робототехника и биотехнологии;

– радиотехника и электронная компонентная база;

– информационная безопасность (ИБ).

Реализация настоящей Стратегии обеспечивается согласованными действиями следующих государственных органов, органов местного самоуправления и организаций:

а) Правительство РФ;

б) Администрация Президента РФ;

в) аппарат Совета Безопасности Российской Федерации;

г) федеральные органы исполнительной власти;

д) Центральный банк РФ;

е) органы исполнительной власти субъектов РФ;

---

[1] *Сети связи нового поколения* — технологические системы, предназначенные для подключения к сети «Интернет» пятого поколения в целях использования в устройствах интернета вещей и индустриального интернета.

[2] *Обработка больших объемов данных* — совокупность подходов, инструментов и методов автоматической обработки структурированной и неструктурированной информации, поступающей из большого количества различных, в том числе разрозненных или слабосвязанных, источников информации, в объемах, которые невозможно обработать вручную за разумное время.

[3] *Облачные вычисления* — информационно-технологическая модель обеспечения повсеместного и удобного доступа с использованием сети «Интернет» к общему набору конфигурируемых вычислительных ресурсов («облаку»), устройствам хранения данных, приложениям и сервисам, которые могут быть оперативно предоставлены и освобождены от нагрузки с минимальными эксплуатационными затратами или практически без участия провайдера.

[4] *Туманные вычисления* — информационно-технологическая модель системного уровня для расширения облачных функций хранения, вычисления и сетевого взаимодействия, в которой обработка данных осуществляется на конечном оборудовании (компьютеры, мобильные устройства, датчики, емарт-узлы и другое) в сети, а не в «облаке».

[5] *Интернет вещей* — концепция вычислительной сети, соединяющей вещи (физические предметы), оснащенные встроенными информационными технологиями для взаимодействия друг с другом или с внешней средой без участия человека.

[6] *Индустриальный интернет* — концепция построения информационных и коммуникационных инфраструктур на основе подключения к информационно-телекоммуникационной сети «Интернет» (далее — сеть «Интернет») промышленных устройств, оборудования, датчиков, сенсоров, систем управления технологическими процессами, а также интеграции данных программно-аппаратных средств между собой без участия человека.

ж) органы местного самоуправления;

з) государственные внебюджетные фонды;

и) фонды и институты развития (в соответствии с планом реализации Стратегии);

к) государственные корпорации, компании с государственным участием и частные компании.

Стратегия развития отрасли информационных технологий в Российской Федерации на 2014— 2020 годы и на перспективу до 2025 года, утвержденная распоряжением Правительства РФ от 1 ноября 2013 г. № 2036-р, разработана для формирования единого системного подхода государства к развитию отрасли информационных технологий (рис. 1.1).

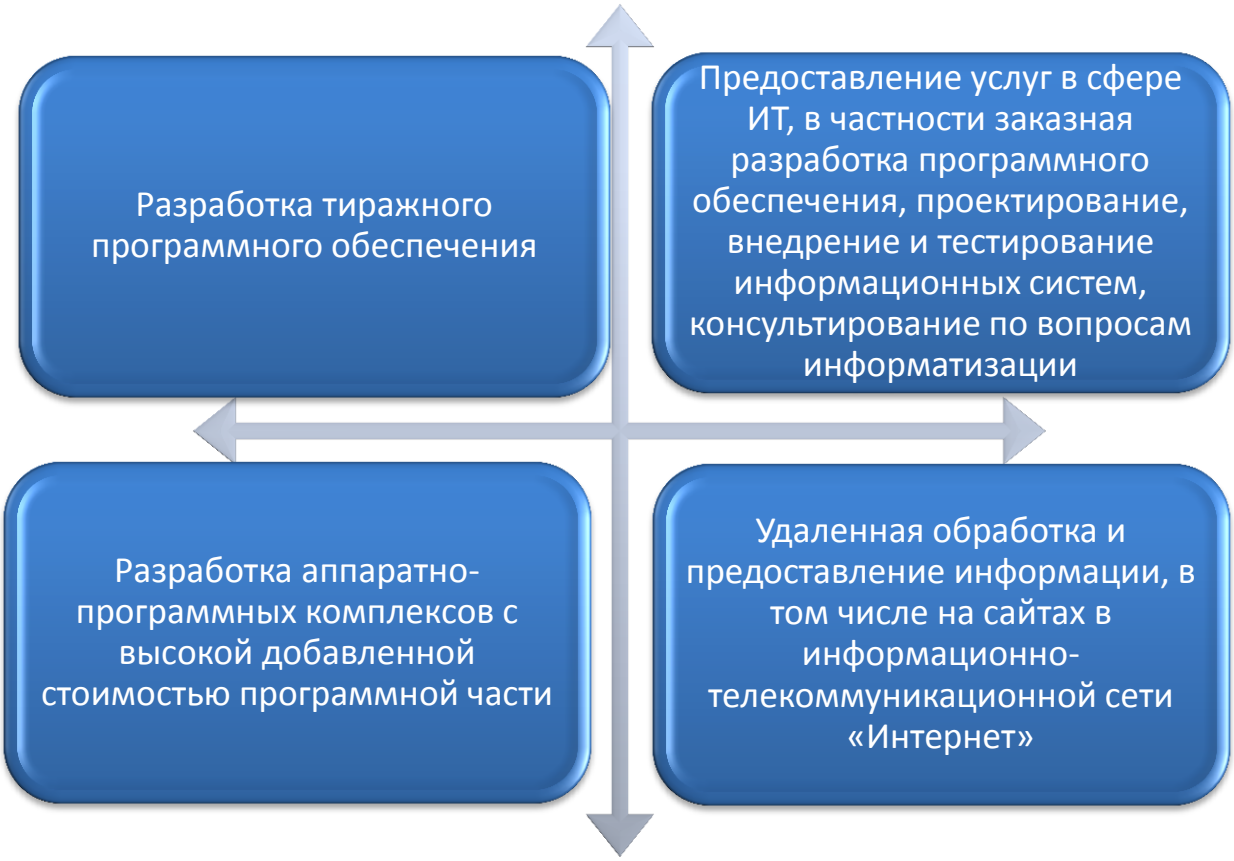


Рис. 1.1. **Виды деятельности российских компаний, занятых в отрасли информационных технологий**

Настоящая Стратегия определяет *цели* и *базовые принципы* развития отрасли информационных технологий (рис. 1.2), а также основные *направления* ее реализации (рис. 1.3).

Особенно актуальным является вопрос обеспечения должного уровня информационной безопасности страны в современном глобальном информационном мире, учитывая масштабы проникновения информационных технологий в повседневную жизнь граждан, организаций и органов власти всех уровней, а также высокий уровень зависимости создаваемых в стране информационных систем от импортной продукции.

Цели развития отрасли ИТ

- развитие сферы ИТ до полноценной отрасли российской экономики, создающей высокопроизводительные рабочие места и обеспечивающей выпуск высокотехнологичной и конкурентоспособной продукции;
- обеспечение различных сфер экономики качественными информационными технологиями с целью повышения производительности труда;
- обеспечение высокого уровня информационной безопасности государства, индустрии и граждан

Базовые принципы развития отрасли ИТ

- улучшение институциональных условий при минимальном прямом регулировании
- сохранение конкурентного характера развития отрасли;
- поддержка малого бизнеса в качестве приоритетного направления развития отрасли;
- определение приоритетов государственной поддержки среднего и крупного бизнеса на основе создаваемых компаниями высококвалифицированных рабочих мест, добавленной стоимости и потенциала глобальной конкурентоспособности компаний;
- обеспечение сбалансированной структуры российской отрасли, включающей крупные, средние и малые компании;
- сохранение интегрированности российской отрасли в глобальную индустрию информационных технологий;
- стимулирование капитализации компаний в России;
- стимулирование создания научно-технологического задела и новой высокотехнологичной продукции по перспективным направлениям развития отрасли;
- ориентация на государственно-частное партнерство при решении задач по развитию отрасли информационных технологий

Рис. 1.2. **Цели и базовые принципы развития отрасли информационных технологий в Российской Федерации на 2014— 2020 гг. и на перспективу до 2025 г.**

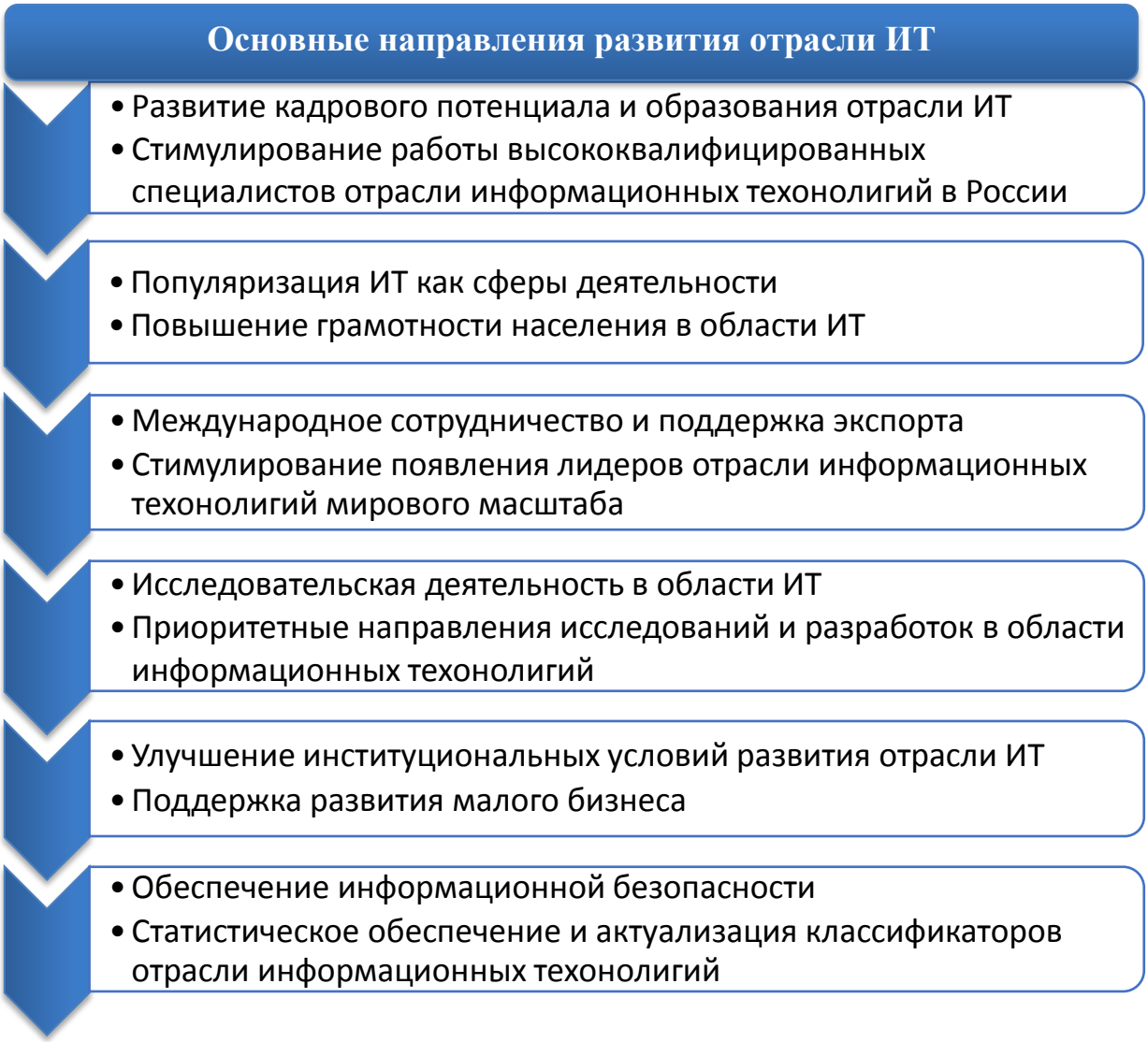


Рис. 1.3. **Основные направления реализации Стратегии развития отрасли информационных технологий в Российской Федерации на 2014—2020 гг. и на перспективу до 2025 г.**

Контрольные вопросы и задания

1. Какое общество называют информационным?
2. Какова цель действующей Стратегии развития информационного общества в Российской Федерации?
3. Что такое «общество знаний»?
4. Каковы основные принципы действующей Стратегии развития информационного общества в Российской Федерации?
5. Дайте определение понятию «цифровая экономика».
6. Сформулируйте определение понятия «информационное пространство».
7. Определите понятие «инфраструктура электронного правительства».
8. Дайте определение понятию «безопасные программное обеспечение и сервис».

9. Определите понятия «индустриальный интернет» и «интернет вещей».

10. Дайте определение понятию «критическая информационная инфраструктура Российской Федерации». Перечислите ее объекты.

11. Определите понятие «Национальная электронная библиотека».

12. Что такое «облачные вычисления»?

13. Какие мероприятия необходимо реализовать для формирования информационного пространства знаний?

14. Сформулируйте цель развития информационной и коммуникационной инфраструктуры Российской Федерации.

15. Каковы основные направления развития российских информационных и коммуникационных технологий?

16. Каковы ключевые направления повышения конкурентоспособности российских информационных и коммуникационных технологий?

17. Какими принципами должны руководствовать разработчики при создании российских информационных и коммуникационных технологий?

18. Какие основные задачи должны быть выполнены при применении информационных и коммуникационных технологий для развития социальной сферы, системы государственного управления, взаимодействия граждан и государства?

19. Сформулируйте основные задачи применения информационных технологий в сфере взаимодействия государства и бизнеса, формирования новой технологической основы в экономике.

20. Какие национальные интересы в области цифровой экономики определены в действующей Стратегии развития информационного общества в Российской Федерации?

21. Какие мероприятия необходимы для реализации национальных интересов в области цифровой экономики?

22. Условия и принципы сотрудничества российских организаций с иностранными организациями в сфере цифровой экономики?

23. На какие органы и организации возложена реализация Стратегии развития информационного общества в Российской Федерации?

24. Что понимается под отраслью информационных технологий?

25. Перечислите базовые принципы развития отрасли информационных технологий.

26. Какие основные цели развития отрасли информационных технологий ставит перед собой Правительство РФ на 2014— 2020 гг. и на перспективу до 2025 г.?

27. Каковы основные направления реализации Стратегии развития отрасли информационных технологий в Российской Федерации на 2014— 2020 гг. и на перспективу до 2025 г.?

28. Какие меры долгосрочного характера, направленные на обеспечение информационной безопасности, необходимо предпринять государственным органам власти, организациям и гражданам, проживающим на территории РФ?

Тема 2. Место информационной безопасности в системе национальной безопасности Российской Федерации

Базовым документом стратегического планирования, определяющим национальные интересы и стратегические национальные приоритеты Российской Федерации, цели, задачи и меры в области внутренней и внешней политики, направленные на укрепление национальной безопасности Российской Федерации и обеспечение устойчивого развития страны на долгосрочную перспективу, является *Стратегия национальной безопасности Российской Федерации* (*утверждена Указом Президента РФ от 31 декабря 2015 г. № 683*). В настоящей Стратегии даны следующие определения:

национальная безопасность Российской Федерации — состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией РФ и законодательством РФ (рис. 2.1);

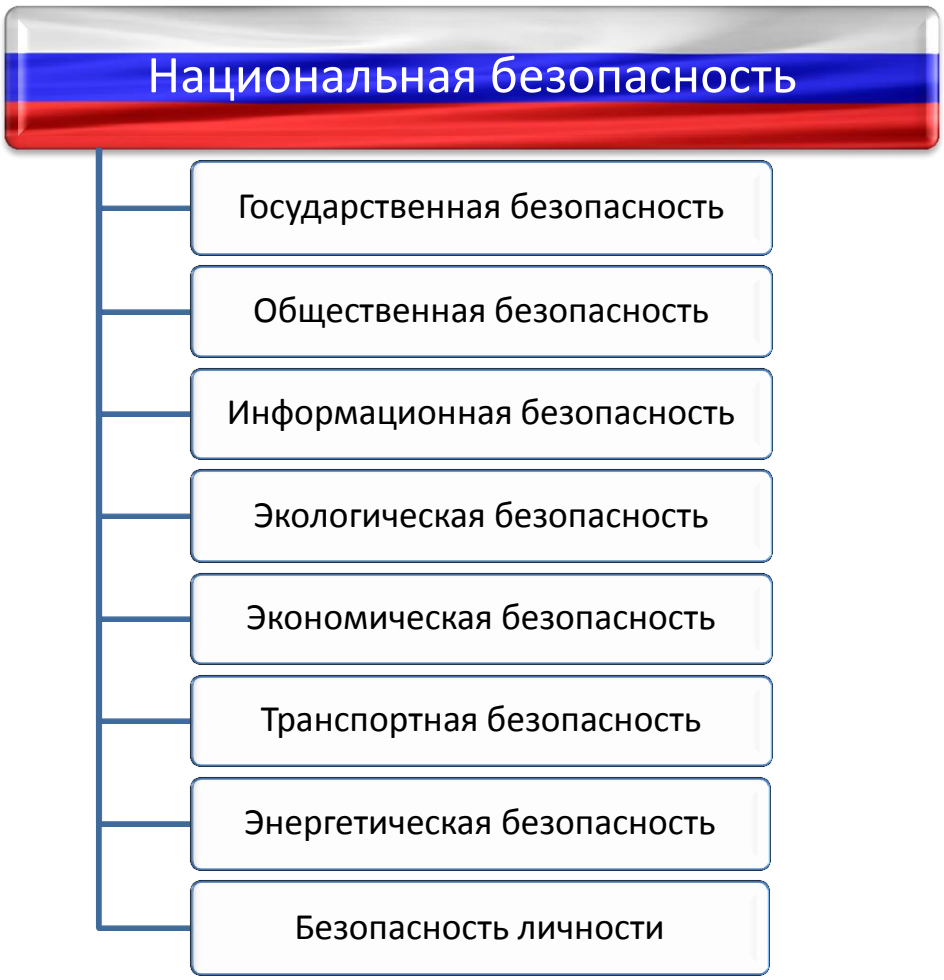


Рис. 2.1. **Взаимосвязь видов безопасности**

национальные интересы Российской Федерации — объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития;

угроза национальной безопасности — совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам;

обеспечение национальной безопасности — реализация органами государственной власти и органами местного самоуправления во взаимодействии с институтами гражданского общества политических, военных, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие угрозам национальной безопасности и удовлетворение национальных интересов;

стратегические национальные приоритеты Российской Федерации — важнейшие направления обеспечения национальной безопасности;

система обеспечения национальной безопасности — совокупность осуществляющих реализацию государственной политики в сфере обеспечения национальной безопасности органов государственной власти и органов местного самоуправления и находящихся в их распоряжении инструментов.

Государственная политика в области обеспечения безопасности является частью внутренней и внешней политики Российской Федерации и представляет собой совокупность скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер.

Все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории.

Появляются новые формы противоправной деятельности с использованием информационных и коммуникационных технологий. Среди основных угроз государственной и общественной безопасности выделяют деятельность, связанную с использованием информационных и коммуникационных технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, нанесения ущерба гражданскому миру, политической и социальной стабильности в обществе.

В целях обеспечения государственной и общественной безопасности совершенствуется система выявления и анализа угроз в информационной сфере, противодействия им. Принимаются меры для повышения защищенности граждан и общества от деструктивного информационного воздействия со стороны экстремистских и террористических организаций, иностранных специальных служб и пропагандистских структур.

Для противодействия угрозам качеству жизни граждан органы государственной власти и органы местного самоуправления во взаимодействии с институтами гражданского общества обеспечивают:

– развитие информационной инфраструктуры;

– доступность информации по различным вопросам социально-политической, экономической и духовной жизни общества;

– равный доступ к государственным услугам на всей территории РФ, в том числе с использованием информационных и коммуникационных технологий.

Для обеспечения экономической безопасности, кроме прочего, необходимы активные меры по государственной защите российских производителей, осуществляющих деятельность в области военной, продовольственной, информационной и энергетической безопасности.

Российская Федерация выступает за качественное развитие Организации Договора о коллективной безопасности, превращение ее в универсальную международную организацию, способную противостоять региональным вызовам и угрозам военно-политического и военно-стратегического характера, а также угрозам в информационной сфере.

При реализации Стратегии национальной безопасности Российской Федерации особое внимание уделяется обеспечению информационной безопасности с учетом стратегических национальных приоритетов. В целях сохранения стратегической стабильности Российская Федерация содействует формированию системы международной информационной безопасности.

Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством РФ, полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления в области безопасности, а также статус Совета Безопасности РФ.

Координацию деятельности по обеспечению безопасности осуществляют Президент РФ (рис. 2.2) и формируемый и возглавляемый им Совет Безопасности РФ, а также в пределах своей компетенции Правительство РФ, федеральные органы государственной власти, органы государственной власти субъектов РФ, органы местного самоуправления.

Доктрина информационной безопасности Российской Федерации (*утверждена Указом Президента РФ от 5 декабря 2016 г. № 646*) представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. В настоящей Доктрине определены следующие основные понятия:

информационная сфера — совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений;

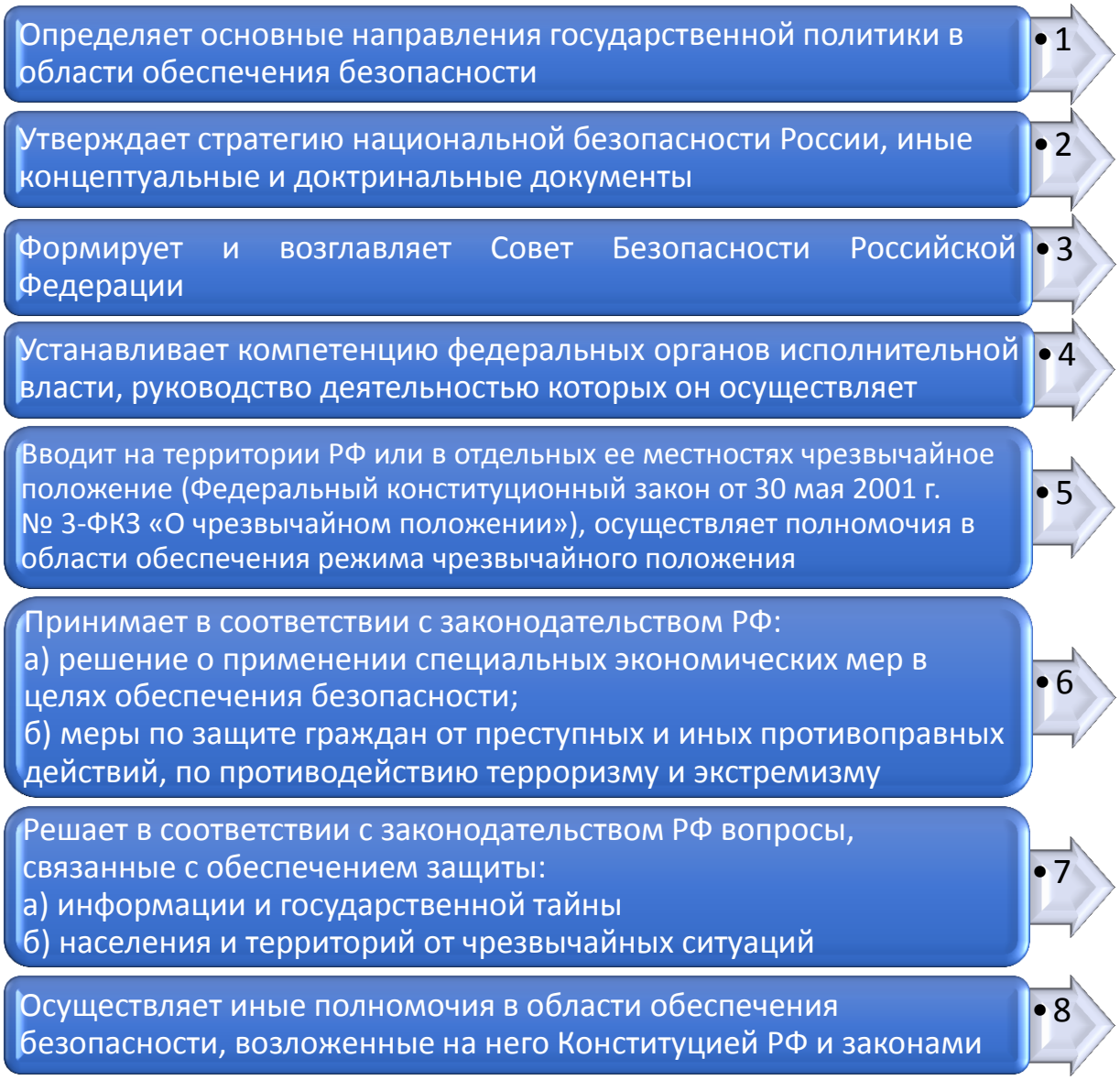


Рис. 2.2. **Полномочия Президента РФ в области обеспечения безопасности (ст. 8 Федерального закона «О безопасности»)**

национальные интересы Российской Федерации в информационной сфере — объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы;

угроза информационной безопасности Российской Федерации — совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере (рис. 2.3);

информационная безопасность Российской Федерации — состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

Рис. 2.3. **Основные информационные угрозы Российской Федерации**

обеспечение информационной безопасности — осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

силы обеспечения информационной безопасности — государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством РФ задач по обеспечению информационной безопасности (рис. 2.4);

средства обеспечения информационной безопасности — правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;

система обеспечения информационной безопасности — совокупность сил обеспечения информационной безопасности, осуществляющих

скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности;

информационная инфраструктура Российской Федерации — совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории РФ, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров РФ.

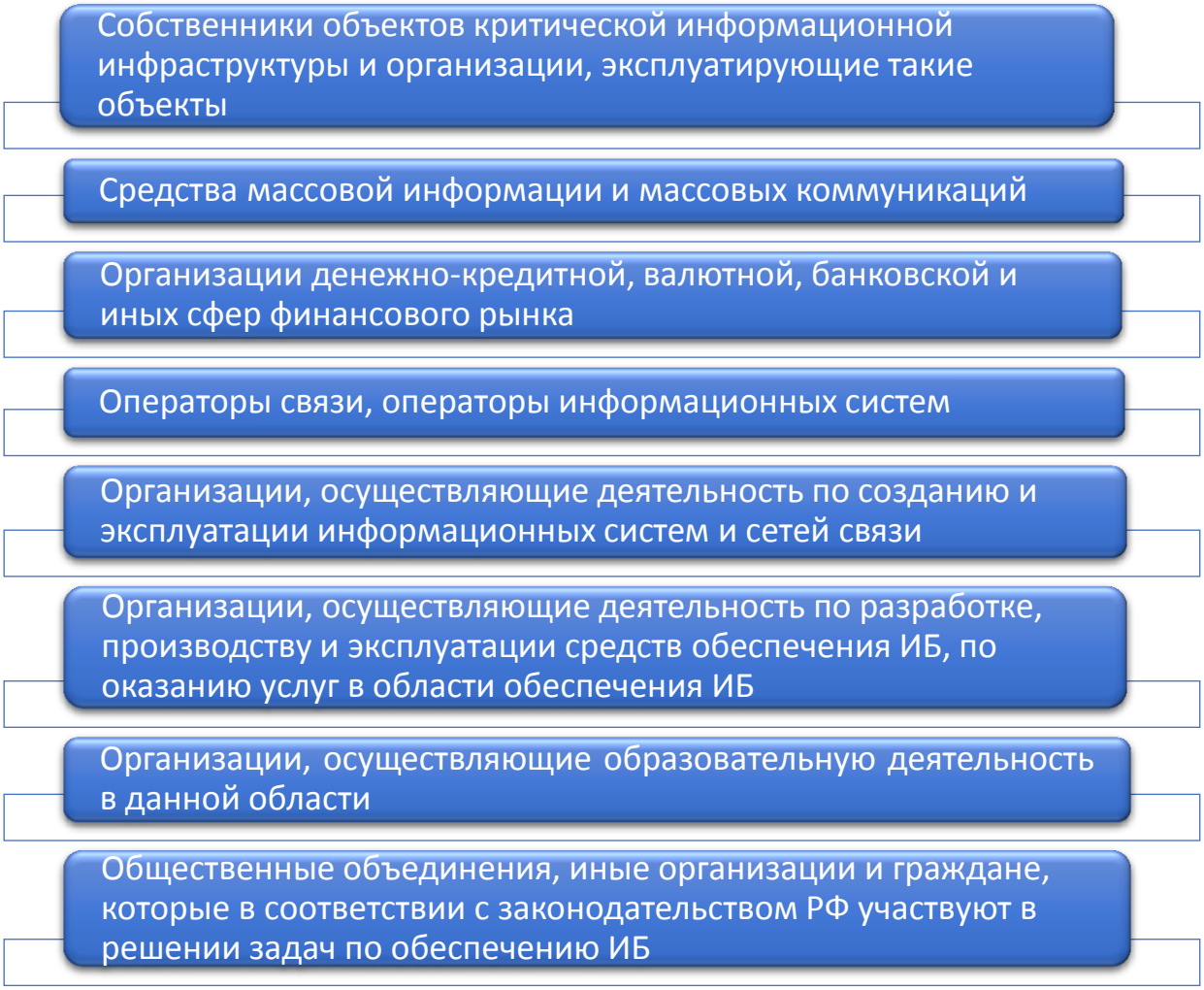


Рис. 2.4. **Участники системы обеспечения ИБ России**

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами (рис. 2.5).

Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

Рис. 2.5. **Организационная основа системы обеспечения ИБ России**

По *Указу Президента РФ от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации»* в целях противодействия угрозам информационной безопасности Российской Федерации при использовании информационно-телекоммуникационной сети «Интернет» на территории РФ *сегмент международной компьютерной сети «Интернет»* для федеральных органов государственной власти и органов государственной власти субъектов РФ, находящийся в ведении Федеральной службы охраны Российской Федерации (ФСО России), преобразован в *российский государственный сегмент информационно-телекоммуникационной сети «Интернет»* (сеть «Интернет»), являющийся элементом российской части сети «Интернет» и обеспечивающий:

а) подключение к сети «Интернет» предназначенных для взаимодействия с ней государственных информационных систем и информационно-телекоммуникационных сетей государственных органов, а также информационных систем и информационно-телекоммуникационных сетей организаций, созданных для выполнения задач, поставленных перед федеральными государственными органами;

б) размещение (публикацию) в сети «Интернет» информации государственных органов и названных в подп. «а» организаций.

Подключение информационных систем и информационно-телекоммуникационных сетей к сети «Интернет» через российский государственный сегмент сети «Интернет» осуществляется по каналам передачи данных, защищенным с использованием шифровальных (криптографических) средств.

Контрольные вопросы и задания

1. Каковы национальные интересы и стратегические национальные приоритеты в соответствии с действующей Стратегией национальной безопасности Российской Федерации?
2. Дайте определение понятию «национальная безопасность Российской Федерации».
3. Перечислите и охарактеризуйте виды безопасности, предусмотренные Конституцией РФ и законодательством РФ.
4. Дайте определение понятию «национальные интересы Российской Федерации».
5. Что понимается под угрозой национальной безопасности?
6. Определите понятие «обеспечение национальной безопасности».
7. Дайте определение понятию «стратегические национальные приоритеты Российской Федерации».
8. Что понимается под «системой обеспечения национальной безопасности»?
9. Сформулируйте основные угрозы государственной и общественной безопасности.
10. Какие мероприятия необходимо реализовать в целях обеспечения государственной и общественной безопасности?
11. Каковы стратегические цели обеспечения национальной безопасности в области науки, технологий и образования?
12. Какие мероприятия необходимо реализовать для решения задач национальной безопасности в области науки, технологий и образования?
13. Каковы принципы стратегической стабильности и равноправного стратегического партнерства Российской Федерации?
14. Перечислите организационные, нормативно-правовые и информационные основы реализации действующей Стратегией национальной безопасности Российской Федерации.
15. Дайте определение понятию «национальные интересы Российской Федерации в информационной сфере».
16. Какие основные принципы обеспечения безопасности определены в Федеральном законе «О безопасности»?
17. Перечислите основные задачи и функции Совета Безопасности Российской Федерации в соответствии с Федеральным законом «О безопасности»?
18. Как формируется Совет Безопасности Российской Федерации, и кто его возглавляет?
19. Каковы полномочия Президента РФ в области обеспечения безопасности?
20. Каковы полномочия палат Федерального Собрания РФ в области обеспечения безопасности?
21. Каковы полномочия Правительства РФ в области обеспечения безопасности?

22. Какие основные цели международного сотрудничества в области обеспечения безопасности сформулированы в Федеральном законе «О безопасности»?

23. Дайте определение понятию «угроза информационной безопасности Российской Федерации».

24. Дайте определение понятию «информационная безопасность Российской Федерации».

25. Определите понятие «обеспечение информационной безопасности».

26. Дайте определение понятию «силы обеспечения информационной безопасности».

27. Дайте определение понятию «средства обеспечения информационной безопасности».

28. Дайте определение понятию «система обеспечения информационной безопасности».

29. Дайте определение понятию «информационная инфраструктура Российской Федерации».

30. Какие национальные интересы в информационной сфере выделены в Доктрине информационной безопасности Российской Федерации?

31. Какие основные информационные угрозы выделены в Доктрине информационной безопасности Российской Федерации?

32. Охарактеризуйте состояние информационной безопасности в Российской Федерации.

33. Какие стратегические цели обеспечения информационной безопасности сформулированы в Доктрине информационной безопасности Российской Федерации?

34. Выделите основные направления обеспечения информационной безопасности в области обороны страны в соответствии с военной политикой Российской Федерации.

35. Выделите основные направления обеспечения информационной безопасности в области государственной и общественной безопасности.

36. Выделите основные направления обеспечения информационной безопасности в экономической сфере?

37. Выделите основные направления обеспечения информационной безопасности в области науки, технологий и образования.

38. Выделите основные направления обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства.

39. Определите организационную основу системы обеспечения информационной безопасности Российской Федерации.

Тема 3. Классификация информации, подлежащей защите в соответствии с законодательством Российской Федерации

В Конституции РФ, а также Декларации прав и свобод человека и гражданина Российской Федерации определено, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Ограничения этого права могут устанавливаться законом только в целях охраны личной, семейной, профессиональной, коммерческой и государственной тайны, а также нравственности.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» предусматривает разделение информации в зависимости от порядка ее предоставления или распространения (рис. 3.1).

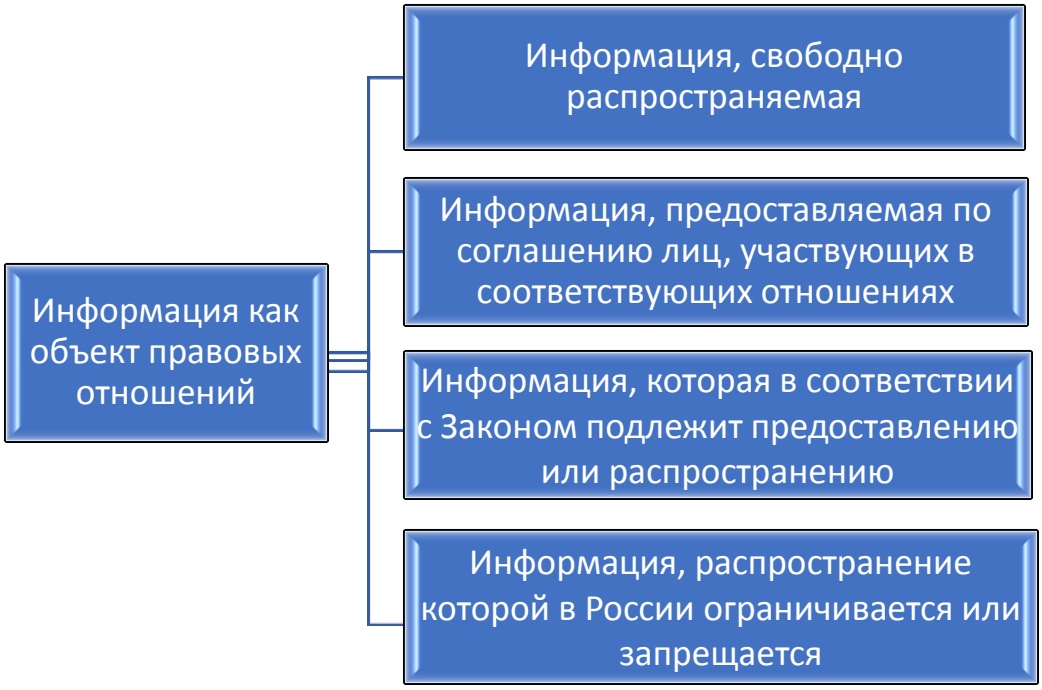


Рис. 3.1. **Классификация информации в зависимости от порядка ее представления или распространения**

Информация в зависимости от категории доступа к ней подразделяется на *общедоступную информацию*, а также на информацию, доступ к которой ограничен федеральными законами (***информация ограниченного доступа***).

В свою очередь информация ограниченного доступа подразделяется на информацию, отнесенную к *государственной тайне* и *конфиденциальную* (рис. 3.2). Отнесение информации к государственной тайне осуществляется в соответствии с Законом РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне». Условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение устанавливаются федеральными законами. Порядок доступа к

персональным данным граждан (физических лиц) устанавливается Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

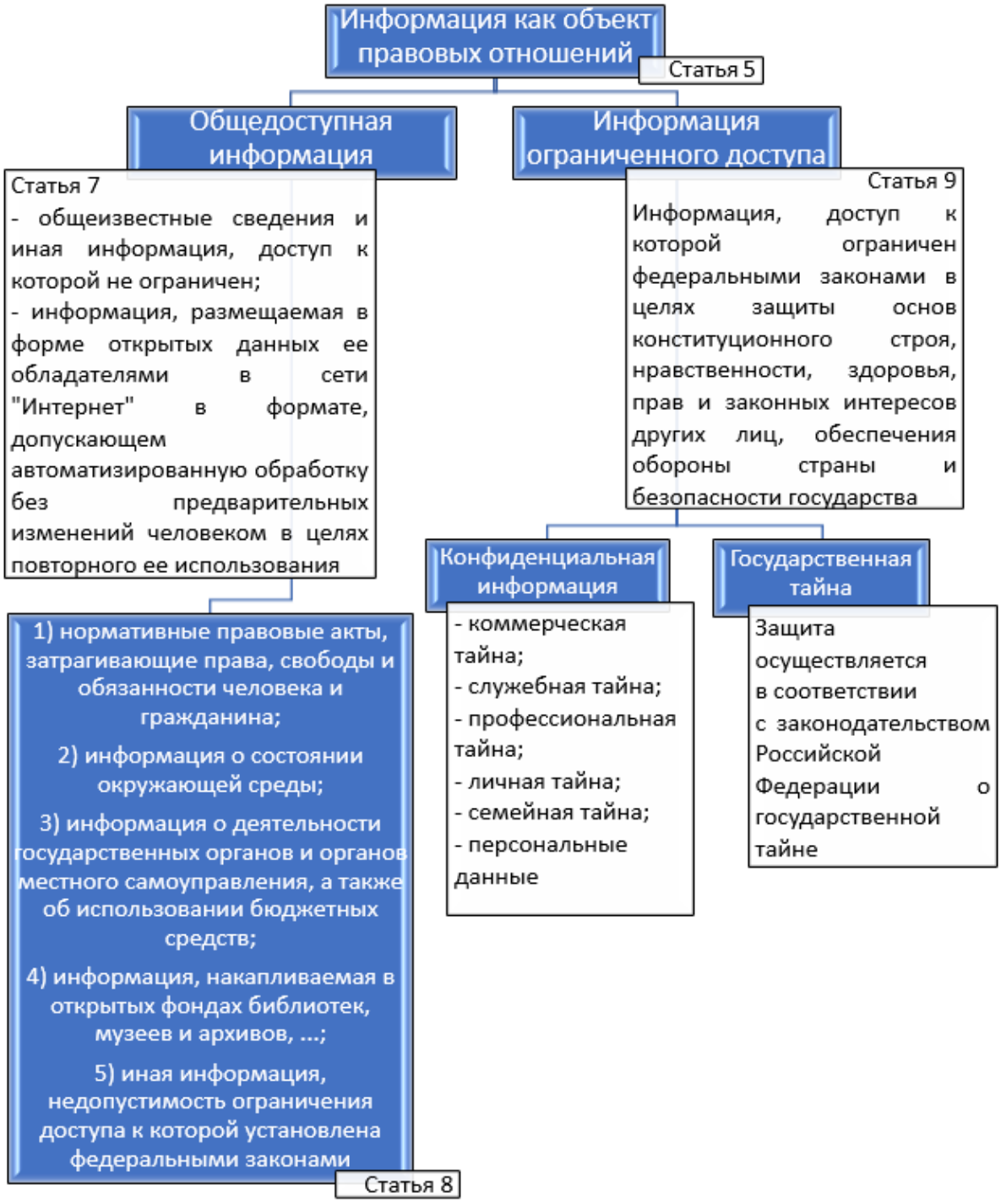


Рис. 3.2. **Классификация информации в зависимости от категории доступа согласно Федеральному закону «Об информации, информационных технологиях и о защите информации»**

В Федеральном законе «Об информации, информационных технологиях и о защите информации» даны следующие определения:

информация — сведения (сообщения, данные) независимо от формы их представления;

информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (рис. 3.3);

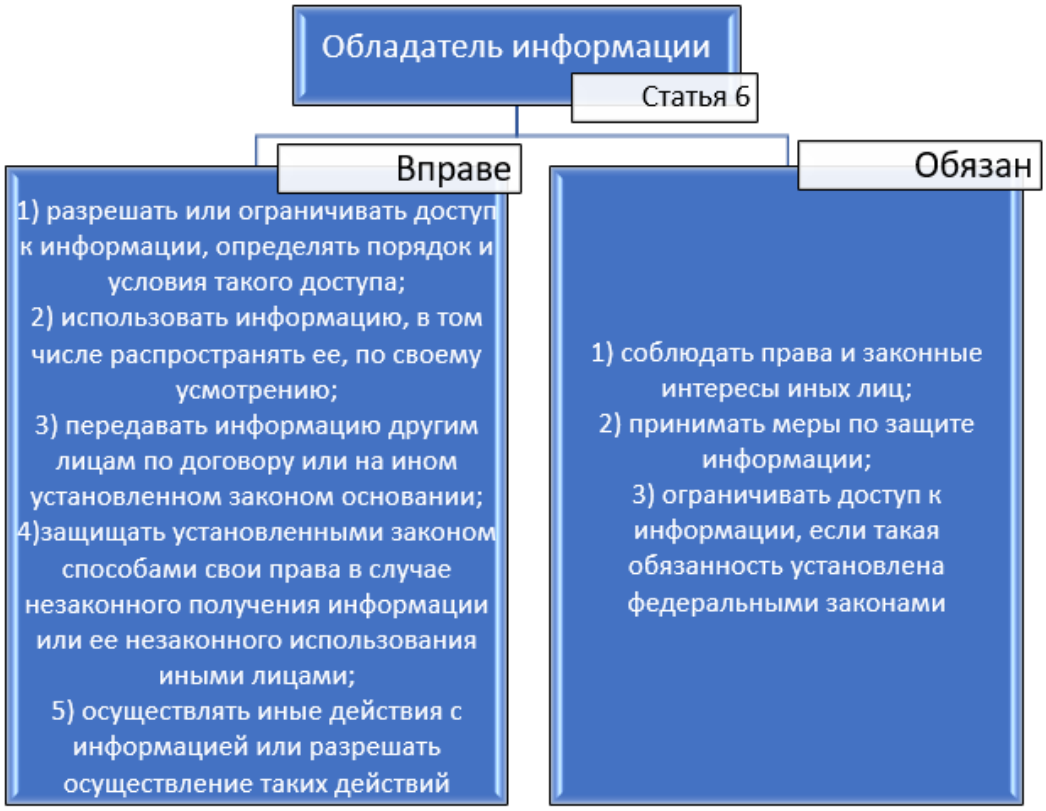


Рис. 3.3. **Права и обязанности обладателя информации согласно Федеральному закону «Об информации, информационных технологиях и о защите информации»**

доступ к информации — возможность получения информации и ее использования;

конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

электронное сообщение — информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

электронный документ — документированная информация, представленная в электронной форме, т.е. в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

сайт в сети «Интернет» — совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет»;

страница сайта в сети «Интернет» (интернет-страница) — часть сайта в сети «Интернет», доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети «Интернет»;

доменное имя — обозначение символами, предназначенное для адресации сайтов в сети «Интернет» в целях обеспечения доступа к информации, размещенной в сети «Интернет»;

сетевой адрес — идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему;

владелец сайта в сети «Интернет» — лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети «Интернет», в том числе порядок размещения информации на таком сайте;

провайдер хостинга — лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет»;

единая система идентификации и аутентификации — федеральная государственная информационная система, порядок использования которой устанавливается Правительством РФ, и которая обеспечивает в случаях, предусмотренных законодательством РФ, санкционированный доступ к информации, содержащейся в информационных системах;

поисковая система — информационная система, осуществляющая по запросу пользователя поиск в сети «Интернет» информации определенного содержания и предоставляющая пользователю сведения об указателе страницы сайта в сети «Интернет» для доступа к запрашиваемой информации, расположенной на сайтах в сети «Интернет», принадлежащих иным лицам, за исключением информационных систем, используемых для осуществления государственных и муниципальных функций, оказания государственных и муниципальных услуг, а также для осуществления иных публичных полномочий, установленных федеральными законами.

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

1) 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.

Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности (ФСБ России) и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России), 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.

Перечень сведений конфиденциального характера (табл. 3.1) определен в Указе Президента РФ от 6 марта 1997 г. № 188.

Таблица 3.1

Перечень сведений конфиденциального характера

№ п/п	Вид конфиденциальной информации	Определение (содержание)
1.	Персональные данные	Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях
2.	Тайна следствия и судопроизводства	Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении

		которых в соответствии с Федеральными законами от 20 апреля 1995 г. № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» и от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства», другими нормативными правовыми актами РФ принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством РФ такие сведения не отнесены к сведениям, составляющим государственную тайну
3.	Служебная тайна	Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами
4.	Профессиональная тайна	Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее)
5.	Коммерческая тайна	Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами
6.	Сведения о сущности изобретения	Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них
7.	Сведения, содержащиеся в личных делах осужденных	Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 2 октября 2007 г. № 229-ФЗ «Об исполнительном производстве»

3.1. Персональные данные

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти,

органами государственной власти субъектов РФ, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, т.е. позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

Целью указанного Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

В Законе даны следующие определения:

персональные данные — любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

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

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

автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники;

распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных — действия, направленные на

раскрытие персональных данных определенному лицу или определенному кругу лиц;

блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

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

Следует отметить, что в Законе установлены правила обработки персональных данных в общедоступных источниках персональных данных (ст. 8).

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Закона, является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи.

Нормативные документы в области обеспечения защиты персональных данных:

— постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

— постановление Правительства РФ от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персо-

нальных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

— постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

— постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом “О персональных данных” и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

— приказ Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

3.2. Коммерческая тайна

Федеральным законом от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» регулируются отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

В Законе даны следующие определения:

коммерческая тайна — режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

информация, составляющая коммерческую тайну, — сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

обладатель информации, составляющей коммерческую тайну, — лицо, которое владеет информацией, составляющей коммерческую тайну, на

законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;

доступ к информации, составляющей коммерческую тайну, — ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

передача информации, составляющей коммерческую тайну, — передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;

контрагент — сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

предоставление информации, составляющей коммерческую тайну, — передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;

разглашение информации, составляющей коммерческую тайну, — действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Согласно постановлению Правительства РСФСР от 5 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну» коммерческую тайну предприятия и предпринимателя не могут составлять:

– учредительные документы (решение о создании предприятия или договор учредителей) и Устав;

– документы, дающие право заниматься предпринимательской деятельностью (документы, подтверждающие факт внесения записей о юридических лицах в Единый государственный реестр юридических лиц, свидетельства о государственной регистрации индивидуальных предпринимателей, лицензии, патенты);

– сведения по установленным формам отчетности о финансово — хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РСФСР;

– документы о платежеспособности;

– сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

– документы об уплате налогов и обязательных платежах;

– сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства РСФСР и размерах причиненного при этом ущерба;

– сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

Нормативные документы в области обеспечения защиты коммерческой тайны:

— Трудовой кодекс Российской Федерации (ст. 57, 81, 238);

— Гражданский кодекс Российской Федерации (ст. 727, 771, 1027, гл. 75).

3.3. Служебная тайна

Служебная тайна является видом конфиденциальной информации, и право на служебную тайну выступает самостоятельным объектом права.

Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» определяет, что к ***служебной информации ограниченного распространения*** относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами.

К *основным объектам служебной тайны* можно отнести такие виды информации, как:

1) служебная информация о деятельности федеральных государственных органов, доступ к которой ограничен законом в целях защиты государственных интересов:

- *военная тайна*;
- *тайна следствия* (данные предварительного расследования либо следствия);
- *судебная тайна* (тайна совещания судей, содержание дискуссий и результатов голосования закрытого совещания Конституционного Суда РФ, материалы закрытого судебного заседания, тайна совещания присяжных заседателей или в силу служебной необходимости, порядок выработки и принятия решения, организация внутренней работы и т.д.);

2) охраноспособная конфиденциальная информация, ставшая известной в силу исполнения служебных обязанностей должностным лицам государственных органов и органов местного самоуправления: *коммерческая*

тайна, *банковская тайна*, *профессиональная тайна*, а также *конфиденциальная информация о частной жизни лица*.

Согласно указанному постановлению Правительства РФ к служебной информации ограниченного распространения *не могут быть отнесены*:

– акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

– сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;

– описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;

– порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;

– решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;

– сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения;

– документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

На документах (в необходимых случаях и на их проектах), содержащих служебную информацию ограниченного распространения, проставляется пометка «Для служебного пользования».

За разглашение служебной информации ограниченного распространения, а также нарушение порядка обращения с документами, содержащими такую информацию, государственный служащий (работник организации) может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

3.4. Профессиональные тайны

Профессиональная тайна — защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной.

Информация может считаться профессиональной тайной, если она отвечает следующим требованиям (критериям охраноспособности права):

– доверена или стала известна лицу лишь в силу исполнения им своих профессиональных обязанностей;

– лицо, которому доверена информация, не состоит на государственной или муниципальной службе (в противном случае информация считается служебной тайной) (например, вызов ветеринара на дом относится к служебной тайне);

– запрет на распространение доверенной или ставшей известной информации, которое может нанести ущерб правам и законным интересам доверителя, установлен федеральным законом;

– информация не относится к сведениям, составляющим государственную и коммерческую тайну.

В соответствии с этими критериями можно выделить следующие объекты профессиональной тайны:

Врачебная тайна — сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении (ст. 13 Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»). Основными принципами охраны здоровья являются:

1) соблюдение прав граждан в сфере охраны здоровья и обеспечение связанных с этими правами государственных гарантий;

2) приоритет интересов пациента при оказании медицинской помощи;

3) приоритет охраны здоровья детей;

4) социальная защищенность граждан в случае утраты здоровья;

5) ответственность органов государственной власти и органов местного самоуправления, должностных лиц организаций за обеспечение прав граждан в сфере охраны здоровья;

6) доступность и качество медицинской помощи;

7) недопустимость отказа в оказании медицинской помощи;

8) приоритет профилактики в сфере охраны здоровья;

9) соблюдение врачебной тайны.

Тайна связи. На территории РФ гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообще-

ний, передаваемых по сетям электросвязи и сетям почтовой связи (ст. 63 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»).

Ограничение права на тайну переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи, допускается только в случаях, предусмотренных федеральными законами.

Операторы связи обязаны обеспечить соблюдение тайны связи.

Осмотр почтовых отправлений лицами, не являющимися уполномоченными работниками оператора связи, вскрытие почтовых отправлений, осмотр вложений, ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи и сетям почтовой связи, осуществляются только на основании решения суда, за исключением случаев, установленных федеральными законами.

Сведения о передаваемых по сетям электросвязи и сетям почтовой связи сообщениях, о почтовых отправлениях и почтовых переводах денежных средств, а также сами эти сообщения, почтовые отправления и переводимые денежные средства могут выдаваться только отправителям и получателям или их уполномоченным представителям, если иное не предусмотрено федеральными законами.

Нотариальная тайна. Нотариусу при исполнении служебных обязанностей, лицу, замещающему временно отсутствующего нотариуса, а также лицам, работающим в нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и после сложения полномочий или увольнения (ст. 5 Основ законодательства Российской Федерации о нотариате» от 11 февраля 1993 г. № 4462-1).

Сведения (документы) о совершенных нотариальных действиях могут выдаваться только лицам, от имени или по поручению которых совершены эти действия, если иное не установлено законом.

Сведения о совершенных нотариальных действиях выдаются по требованию суда, прокуратуры, органов следствия в связи с находящимися в их производстве уголовными, гражданскими или административными делами, а также по требованию судебных приставов-исполнителей в связи с находящимися в их производстве материалами по исполнению исполнительных документов, по запросам органа, осуществляющего государственную регистрацию юридических лиц и индивидуальных предпринимателей, в связи с государственной регистрацией и по запросам органов, предоставляющих государственные и муниципальные услуги и исполняющих государственные и

муниципальные функции, и нотариусов в связи с совершаемыми нотариальными действиями. Справки о выдаче свидетельств о праве на наследство и о нотариальном удостоверении договоров дарения направляются в налоговый орган в случаях и в порядке, которые предусмотрены законодательством РФ о налогах и сборах. Справки о завещании выдаются только после смерти завещателя.

Адвокатская тайна — любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю (ст. 8 Федерального закона от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»).

Адвокат не может быть вызван и допрошен в качестве свидетеля об обстоятельствах, ставших ему известными в связи с обращением к нему за юридической помощью или в связи с ее оказанием.

Проведение оперативно-розыскных мероприятий и следственных действий в отношении адвоката (в том числе в жилых и служебных помещениях, используемых им для осуществления адвокатской деятельности) допускается только на основании судебного решения.

Полученные в ходе оперативно-розыскных мероприятий или следственных действий (в том числе после приостановления или прекращения статуса адвоката) сведения, предметы и документы могут быть использованы в качестве доказательств обвинения только в тех случаях, когда они не входят в производство адвоката по делам его доверителей. Указанные ограничения не распространяются на орудия преступления, а также на предметы, которые запрещены к обращению или оборот которых ограничен в соответствии с законодательством РФ.

Тайна усыновления. Судьи, вынесшие решение об усыновлении ребенка, или должностные лица, осуществившие государственную регистрацию усыновления, а также лица, иным образом осведомленные об усыновлении, обязаны сохранять тайну усыновления ребенка (ст. 139 Семейного кодекса Российской Федерации от 29 декабря 1995 г. № 223-ФЗ).

Статья 273 Гражданского процессуального кодекса Российской Федерации от 14 ноября 2002 г. № 138-ФЗ устанавливает, что для сохранения тайны усыновления судебное заседание проводится в закрытой форме; на него допускаются лишь лица, причастные к делу.

Статья 155 Уголовного кодекса Российской Федерации от 13 июня 1996 г. № 63-ФЗ устанавливает наказание за разглашение тайны усыновления. Данное деяние может быть совершено: гражданином, который обязан сохранить в секрете факт усыновления в качестве служебной/профессиональной тайны; иными лицами.

Тайна страхования. Страховщик не вправе разглашать полученные им в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с правилами, предусмотренными ст. 139 или 150 Гражданского кодекса Российской Федерации (часть вторая от 26 января 1996 г. № 14-ФЗ (ст. 946)).

Тайна исповеди — сведения, доверенные гражданином священнослужителю на исповеди. В Российской Федерации гарантируются свобода совести и свобода вероисповедания, в том числе право исповедовать индивидуально или совместно с другими любую религию или не исповедовать никакой, совершать богослужения, другие религиозные обряды и церемонии, осуществлять обучение религии и религиозное воспитание, свободно выбирать и менять, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними, в том числе создавая религиозные объединения. Священнослужитель не может быть привлечен к ответственности за отказ от дачи показаний по обстоятельствам, которые стали известны ему из исповеди (ст. 3 Федерального закона от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и о религиозных объединениях»).

Банковская тайна. Кредитная организация, Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов (ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»).

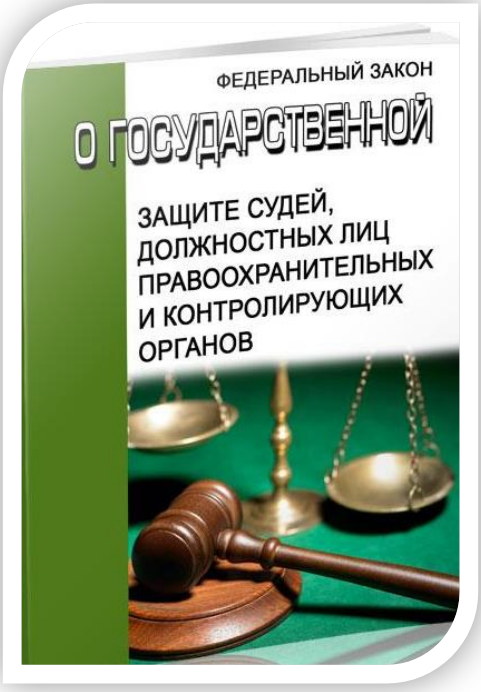
За разглашение банковской тайны Банк России, руководители (должностные лица) фе-

ральных государственных органов, перечень которых определяется Президентом РФ, высшие должностные лица субъектов РФ (руководители высших исполнительных органов государственной власти субъектов РФ), организация, осуществляющая функции по обязательному страхованию вкладов, кредитные, аудиторские и иные организации, уполномоченный орган, осуществляющий функции по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, орган валютного контроля, уполномоченный Правительством РФ, и агенты валютного контроля, а также должностные лица и работники указанных органов и организаций несут «ответственность», включая возмещение нанесенного ущерба, в порядке, установленном федеральным законом.

3.5. Процессуальные тайны

Следственная тайна связана с интересами законного производства предварительного расследования по уголовным делам (ст. 310 УК РФ). Разглашение данных предварительного расследования лицом, предупрежденным в установленном законом порядке о недопустимости их разглашения, если оно совершено без согласия следователя или лица, производящего дознание, — наказывается штрафом в размере до 80 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок до 480 часов, либо исправительными работами на срок до двух лет, либо арестом на срок до трех месяцев.

В целях обеспечения государственной защиты судей, должностных лиц правоохранительных и контролирующих органов, отдельных категорий военнослужащих, сотрудников органов государственной охраны, осуществляющих функции, выполнение которых может быть сопряжено с посягательствами на их безопасность, а также создания надлежащих условий для отправления правосудия, борьбы с преступлениями и другими правонарушениями Федеральный закон от 20 апреля 1995 г. № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» устанавливает систему мер государственной защиты жизни, здоровья и имущества указанных лиц и их близких. Государственной защите в соответствии с Законом подлежат:



1) судьи всех судов общей юрисдикции и арбитражных судов, арбитражные заседатели, присяжные заседатели;

2) прокуроры;

3) следователи;

4) лица, производящие дознание;

5) лица, осуществляющие оперативно-розыскную деятельность;

6) сотрудники федеральных органов внутренних дел, осуществляющие охрану общественного порядка и обеспечение общественной безопасности, а также исполнение приговоров, определений и постановлений судов (судей) по уголовным делам, постановлений органов расследования и прокуроров;

6.1) сотрудники учреждений и органов уголовно-исполнительной системы;

6.2) военнослужащие внутренних войск МВД России, органов военной полиции Вооруженных Сил РФ, принимавшие непосредственное участие в пресечении действий вооруженных преступников, незаконных вооруженных формирований и иных организованных преступных групп;

6.3) военнослужащие войск национальной гвардии Российской Федерации, принимавшие непосредственное участие в пресечении действий вооруженных преступников, незаконных вооруженных формирований и иных организованных преступных групп;

6.4) сотрудники Росгвардии, принимающие участие в осуществлении охраны общественного порядка и обеспечении общественной безопасности;

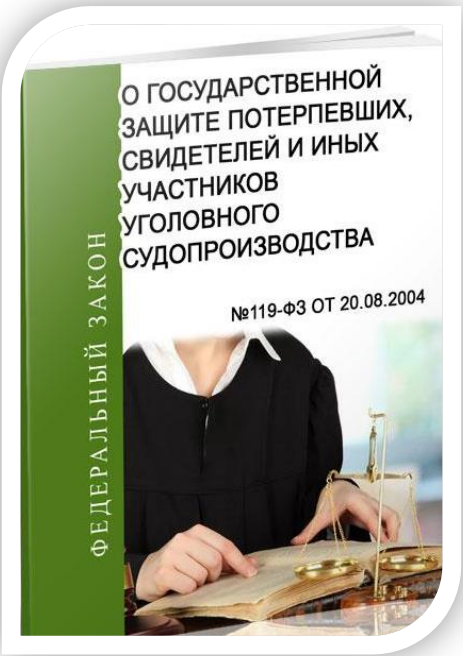
6.5) военнослужащие Вооруженных Сил РФ, принимавшие непосредственное участие в борьбе с терроризмом;

6.6) военнослужащие органов внешней разведки Российской Федерации, принимавшие непосредственное участие в специальных операциях или выполнявшие специальные функции по обеспечению безопасности Российской Федерации;

7) сотрудники органов федеральной службы безопасности;

8) сотрудники Следственного комитета РФ;

9) судебные исполнители;



10) работники контрольных органов Президента РФ, осуществляющие контроль за исполнением законов и иных нормативных правовых актов, выявление и пресечение правонарушений;

11) сотрудники органов государственной охраны;

12) работники таможенных и налоговых органов, антимонопольных органов, федеральных органов государственного контроля, Росфинмониторинга, Счетной палаты РФ, а также иные категории государственных и муниципальных служащих по перечню, устанавливаемому Правительством РФ;

13) близкие лиц, перечисленных выше.

Федеральный закон от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» устанавливает систему мер государственной защиты потерпевших, свидетелей и иных участников уголовного судопроизводства, включающую меры безопасности и меры социальной поддержки указанных лиц, а также определяет основания и порядок их применения. Государственной защите в соответствии с Законом подлежат следующие участники уголовного судопроизводства:

1) потерпевший;

2) свидетель;

3) частный обвинитель;

4) подозреваемый, обвиняемый, подсудимый, их защитники и законные представители, осужденный, оправданный, а также лицо, в отношении которого уголовное дело либо уголовное преследование было прекращено;

5) эксперт, специалист, переводчик, понятой, а также участвующие в уголовном судопроизводстве педагог и психолог;

6) гражданский истец, гражданский ответчик;

7) законные представители, представители потерпевшего, гражданского истца, гражданского ответчика и частного обвинителя.

Меры государственной защиты могут быть также применены до возбуждения уголовного дела в отношении заявителя, очевидца или жертвы преступления либо иных лиц, способствующих предупреждению или раскрытию преступления.

Меры государственной защиты в отношении защищаемых лиц могут быть применены после постановления приговора, вынесения постановления об освобождении лица от уголовной ответственности или наказания и о применении к нему принудительных мер медицинского характера.

Контрольные вопросы и задания

1. Как разделяется информация в зависимости от порядка ее предоставления или распространения в соответствии с Федеральным законом «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. Дайте определение понятию «информационные технологии».
5. Дайте определение понятию «информационная система».
6. Дайте определение понятию «информационно-телекоммуникационная сеть».
7. Дайте определение понятию «обладатель информации». Назовите его права и обязанности.
8. Определите понятия «доступ к информации» и «конфиденциальность информации».

9. Определите понятия «предоставление информации» и «распространение информации».

10. Определите понятия «электронное сообщение», «документированная информация» и «электронный документ».

11. Дайте определение понятию «оператор информационной системы».

12. Определите понятия «сайт в сети Интернет», «страница сайта в сети Интернет», «доменное имя», «сетевой адрес», «владелец сайта в сети Интернет» и «провайдер хостинга».

13. Дайте определение понятию «единая система идентификации и аутентификации».

14. Дайте определение понятию «поисковая система».

15. С какой целью осуществляется защита информации?

16. Какой перечень сведений конфиденциального характера определен в Указе Президента РФ от 6 марта 1997 г. № 188?

17. Какова цель Федерального закона «О персональных данных»?

18. Дайте определение понятию «персональные данные».

19. Дайте определение понятию «оператор».

20. Определите понятия «обработка персональных данных» и «автоматизированная обработка персональных данных».

21. Определите понятия «распространение персональных данных», «предоставление персональных данных», «блокирование персональных данных», «уничтожение персональных данных» и «обезличивание персональных данных».

22. Дайте определение понятию «информационная система персональных данных».

23. Дайте определение понятию «трансграничная передача персональных данных».

24. Какие правила обработки персональных данных в общедоступных источниках персональных данных установлены в Федеральном законе «О персональных данных»?

25. Назовите нормативные документы в области обеспечения защиты персональных данных.

26. Какие отношения регулируются в Федеральный закон «О коммерческой тайне»?

27. Дайте определение понятию «коммерческая тайна».

28. Дайте определение понятию «информация, составляющая коммерческую тайну».

29. Дайте определение понятию «обладатель информации, составляющей коммерческую тайну».

30. Определите понятия «доступ к информации» и «передача информации, составляющей коммерческую тайну».

31. Дайте определение понятию «контрагент».

32. Определите понятия «предоставление информации» и «разглашение информации, составляющей коммерческую тайну».

33. Какая информация не может являться коммерческой тайной предприятия согласно постановлению Правительства РСФСР от 5 декабря 1991 г. № 35?

34. Назовите нормативные документы в области обеспечения защиты коммерческой тайны.

35. Дайте определение понятию «служебная информация ограниченного распространения».

36. Какие виды информации можно отнести к основным объектам служебной тайны?

37. Какая информация не может быть отнесена к служебной информации ограниченного распространения?

38. Дайте определение понятию «профессиональная тайна».

39. Каким требованиям должна отвечать информация, чтобы считаться профессиональной тайной?

40. Дайте определение понятию «врачебная тайна».

41. Какие основные принципы охраны здоровья определены в Федеральном законе «Об основах охраны здоровья граждан в Российской Федерации»?

42. Определите понятие «тайна связи».

43. Определите понятие «нотариальная тайна».

44. Дайте определение понятию «адвокатская тайна».

45. Определите понятие «тайна усыновления».

46. Определите понятие «тайна страхования».

47. Дайте определение понятию «тайна исповеди».

48. Определите понятие «банковская тайна».

49. Кто подлежит государственной защите в соответствии с Федеральном законом «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов»?

50. Какие участники уголовного судопроизводства подлежат государственной защите в соответствии с Федеральным законом «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»?

Тема 4. Государственная тайна. Государственная система защиты информации

Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне» регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации. В настоящем Законе используются следующие основные понятия:

государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

носители сведений, составляющих государственную тайну, — материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

система защиты государственной тайны — совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;

допуск к государственной тайне — процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций — на проведение работ с использованием таких сведений;

доступ к сведениям, составляющим государственную тайну, — санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

гриф секретности — реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

средства защиты информации — 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.

К государственной тайне могут быть отнесены следующие сведения (ст. 5 Закона):

1) сведения в *военной* области:

– о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию войск, об их боеспособности и мобилизационной готовности, о создании и использовании мобилизационных ресурсов;

– о направлениях развития вооружения и военной техники, содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

– о количестве, устройстве и технологии производства ядерного и специального оружия, технических средствах и методах его защиты от несанкционированного применения;

– о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

– о дислокации, назначении, степени готовности и защищенности режимных и особо важных объектов, об их проектировании и строительстве, а также об отводе земель, недр и акваторий для этих объектов;

– о дислокации, действительных наименованиях, организационной структуре, вооружении и численности объединений, соединений и частей Вооруженных Сил Российской Федерации;

2) сведения в области *экономики, науки* и *техники*:

– о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, мобилизационных мощностях промышленности по изготовлению вооружения и военной техники, об объемах поставок и о запасах стратегических видов сырья и материалов, а также о размещении и фактических размерах государственных материальных резервов;

– об использовании инфраструктуры Российской Федерации в интересах обеспечения ее обороноспособности и безопасности;

– о силах и средствах гражданской обороны, дислокации, предназначении и степени защищенности объектов административного управления, обеспечения безопасности населения, о функционировании промышленности, транспорта и связи в целом по Российской Федерации;

– об объемах, планах (заданиях) государственного оборонного заказа, выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, связях предприятий по кооперации, разработчиках или изготовителях, указанных вооружения, военной техники и другой оборонной продукции;

– о научно-исследовательских, опытно-конструкторских и проектных работах, технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность Российской Федерации;

– о государственных запасах драгоценных металлов и драгоценных камней Российской Федерации, ее финансах и бюджетной политике (кроме обобщенных показателей, характеризующих общее состояние экономики и финансов);

3) сведения в области *внешней политики* и *экономики*:

– о внешнеполитической и внешнеэкономической (торговой, кредитной и валютной) деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб ее интересам;

4) сведения в области *разведывательной, контрразведывательной* и *оперативно-розыскной деятельности*:

– о силах, средствах, источниках, методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

– о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

– о системе правительственной и об иных видах специальной связи, о государственных шифрах, методах и средствах их анализа;

– о методах и средствах защиты секретной информации;

– о государственных программах и мероприятиях в области защиты государственной тайны.

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений (Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности, утвержденные постановлением Правительства РФ от 4 сентября 1995 г. № 870). Сведения, отнесенные к государственной тайне, по степени секретности подразделяются на сведения особой важности, совершенно секретные и секретные (табл. 4.1)

Таблица 4.1

Сведения, отнесенные к государственной тайне, по степени секретности

№ п/п	Степень секретности сведений	Определение (содержание)
1.	Сведения особой важности	Сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей
2.	Совершенно секретные сведения	Сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей
3.	Секретные сведения	Все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Рос-

		сийской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности

К *органам защиты государственной тайны* относятся (ст. 20 Закона РФ «О государственной тайне»):

– межведомственная комиссия по защите государственной тайны (коллегиальный орган, координирующий деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих реализацию законодательства РФ о государственной тайне);

– органы федеральной исполнительной власти (Минобороны России, СВР России) (организуют и обеспечивают защиту государственной тайны в соответствии с функциями, возложенными на них законодательством РФ);

– органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны (обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции).

Допуск должностных лиц и граждан Российской Федерации к государственной тайне осуществляется в добровольном порядке (рис. 4.1). Допуск лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне осуществляется в порядке, устанавливаемом Правительством РФ.

Допуск должностных лиц и граждан к государственной тайне предусматривает:

- принятие на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну;
- согласие на частичные, временные ограничения их прав в соответствии со ст. 24 Закона РФ «О государственной тайне»;
- письменное согласие на проведение в отношении их полномочными органами проверочных мероприятий;
- определение видов, размеров и порядка предоставления льгот, предусмотренных Законом;
- ознакомление с нормами законодательства РФ о государственной тайне, предусматривающими ответственность за его нарушение;
- принятие решения руководителем органа государственной власти, предприятия, учреждения или организации о допуске оформляемого лица к сведениям, составляющим государственную тайну.

Рис. 4.1. **Допуск к государственной тайне (ст. 21 Закона РФ «О государственной тайне»)**

Размер ежемесячной процентной надбавки к должностному окладу (тарифной ставке) граждан, допущенных к государственной тайне на постоянной основе[1], за работу со сведениями, имеющими степень секретности «*особой важности*», составляет 50— 75%, имеющими степень секретности «*совершенно секретно*», — 30— 50%, имеющими степень секретности «*секретно*» при оформлении допуска с проведением проверочных мероприятий, — 10— 15%, без проведения проверочных мероприятий, — 5— 10%[2].

Ежемесячная надбавка за работу со сведениями, составляющими государственную тайну, военнослужащим Вооруженных Сил РФ[3] установлена в следующих размерах:

– со сведениями, имеющими степень секретности «*особой важности*», — 25% оклада по воинской должности;

[1] За исключением военнослужащих, сотрудников органов внутренних дел РФ и уголовно-исполнительной системы.

[2] См.: Правила выплаты ежемесячных процентных надбавок к должностному окладу (тарифной ставке) граждан, допущенных к государственной тайне на постоянной основе, и сотрудников структурных подразделений по защите государственной тайны, утвержденные постановлением Правительства РФ от 18 сентября 2006 г. № 573.

[3] См.: Приказ Министра обороны РФ от 30 декабря 2011 г. № 2700 «Об утверждении Порядка обеспечения денежным довольствием военнослужащих Вооруженных Сил Российской Федерации».

– со сведениями, имеющими степень секретности «*совершенно секретно*», — 20% оклада по воинской должности;

– со сведениями, имеющими степень секретности «*секретно*», — 10% оклада по воинской должности.

Военнослужащим, проходящим военную службу по контракту на отдельных воинских должностях, за работу со сведениями, имеющими степень секретности «особой важности», может устанавливаться надбавка в размере до 65% оклада по воинской должности.

Сотрудникам уголовно-исполнительной системы (УИС) в зависимости от степени секретности сведений, составляющих государственную тайну, к которым они имеют документально подтвержденный доступ на законных основаниях, выплачивается ежемесячная надбавка к должностному окладу за работу со сведениями, составляющими государственную тайну[1]:

– 25% должностного оклада — за работу со сведениями, имеющими степень секретности «особой важности»;

– 20% должностного оклада — за работу со сведениями, имеющими степень секретности «совершенно секретно»;

– 10% должностного оклада — за работу со сведениями, имеющими степень секретности «секретно».

Сотрудникам УИС на отдельных должностях за работу со сведениями, имеющими степень секретности «особой важности», может устанавливаться надбавка в размере до 65% должностного оклада.

Решение об отказе должностному лицу или гражданину в допуске к государственной тайне принимается руководителем органа государственной власти, предприятия, учреждения или организации в индивидуальном порядке с учетом результатов проверочных мероприятий (рис. 4.2). Гражданин имеет право обжаловать это решение в вышестоящую организацию или в суд.

Надзор за соблюдением законодательства при обеспечении защиты государственной тайны и законностью принимаемых при этом решений осуществляют Генеральный прокурор РФ и подчиненные ему прокуроры.

Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам (утверждено постановлением Совета Министров — Правительства Российской Федерации от 15 сентября 1993 г. № 912-51) является документом, обязательным для выполнения при проведении работ по защите информации, содержащей сведения, составляющие государственную или служебную тайну, в органах (аппаратах, администрациях) представительной, исполнительной и судебной властей Российской Федерации, республик в со-

[1] См.: Приказ ФСИН России от 27 мая 2013 г. № 269 «Об утверждении Порядка обеспечения денежным довольствием сотрудников уголовно-исполнительной системы, Порядка выплаты премий за добросовестное выполнение служебных обязанностей сотрудникам уголовно-исполнительной системы и Порядка оказания материальной помощи сотрудникам уголовно-исполнительной системы».

ставе Российской Федерации, автономной области, автономных округов, краев, областей, городов Москвы, Санкт-Петербурга и в органах местного самоуправления, на предприятиях и в их объединениях, учреждениях и организациях независимо от их организационно-правовой формы и формы собственности.

Основаниями для отказа должностному лицу или гражданину в допуске к государственной тайне могут являться:

- признание его судом недееспособным, ограниченно дееспособным или особо опасным рецидивистом, нахождение его под судом или следствием за государственные и иные тяжкие преступления, наличие у него неснятой судимости за эти преступления;
- наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, согласно перечню, утверждаемому Минздравом России;
- постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства;
- выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности Российской Федерации;
- уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных.

Рис. 4.2. **Основания для отказа в допуске к государственной тайне (ст. 22 Закона РФ «О государственной тайне»)**

Защита информации (ЗИ) осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путем проведения специальных работ (рис. 4.3).

Целями ЗИ являются:

1) предотвращение утечки информации по техническим каналам;

2) предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в системах информатизации;

3) соблюдение правового режима использования массивов и программ обработки информации, а также обеспечение полноты, целостности и достоверности информации в системах обработки;

Организационно-технические мероприятия:

- лицензирование деятельности предприятий в области ЗИ;
- аттестование объектов по выполнению требований обеспечения ЗИ при проведении работ со сведениями соответствующей степени секретности;
- сертификация средств ЗИ и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам;
- категорирование вооружения и военной техники, предприятий (объектов) по степени важности ЗИ в оборонной, экономической, политической, научно-технической и других сферах деятельности;
- обеспечение условий ЗИ при подготовке и реализации международных договоров и соглашений;
- оповещение о пролетах космических и воздушных летательных аппаратов, кораблях и судах, ведущих разведку объектов (перехват информации, подлежащей защите), расположенных на территории РФ;
- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении;
- разработка и внедрение технических решений и элементов ЗИ при создании и эксплуатации вооружения и военной техники, при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи;
- разработка средств ЗИ и контроля за ее эффективностью (специального и общего применения) и их использование;
- применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи

Рис. 4.3. **Основные организационно-технические мероприятия по защите информации, содержащей сведения, составляющие государственную или служебную тайну**

4) сохранение возможности управления процессом обработки и пользования информацией.

Защита информации в системах и средствах информатизации и связи (рис. 4.4) является составной частью работ по их созданию, эксплуатации и осуществляется во всех органах государственной власти и на предприятиях, располагающих информацией, содержащей сведения, отнесенные к государственной или служебной тайне.

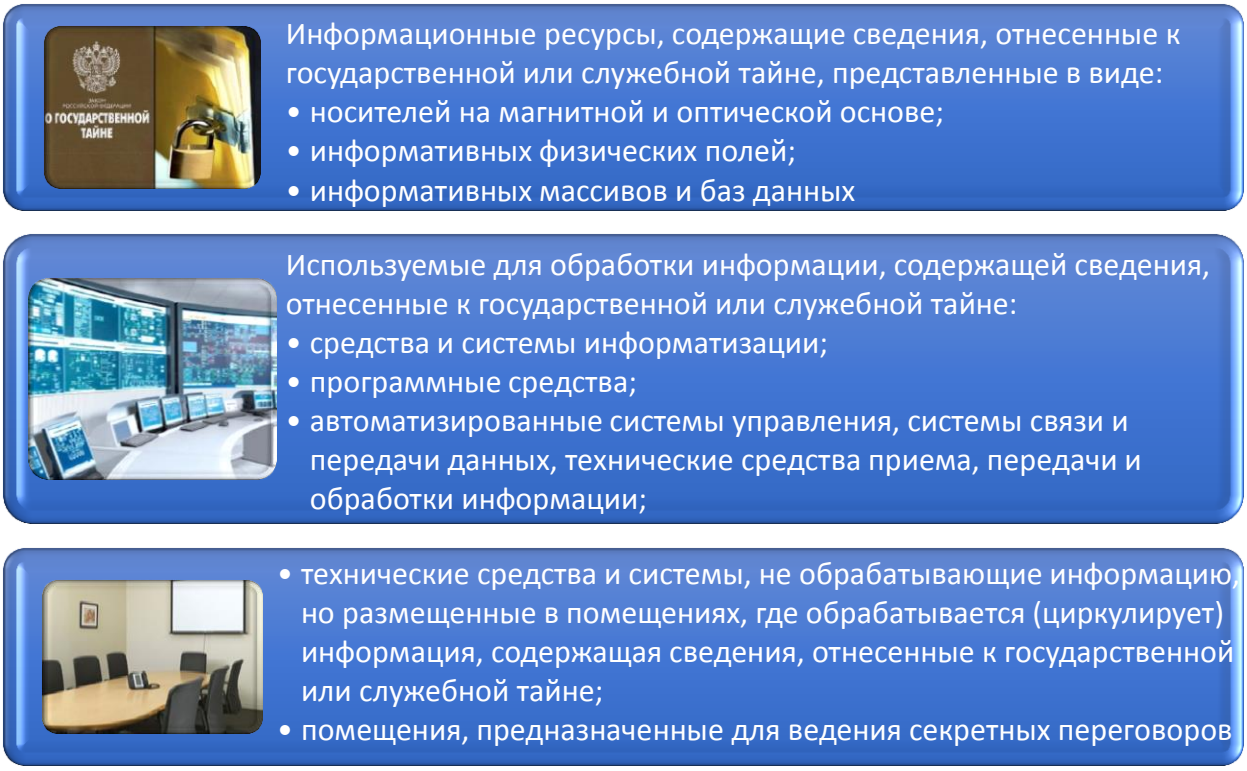


Рис. 4.4. **Объекты защиты в системах и средствах информатизации и связи**

Защита информации осуществляется путем:

1) предотвращения перехвата техническими средствами информации, передаваемой по каналам связи, — достигается применением криптографических и иных методов и средств защиты, а также проведением организационно-технических и режимных мероприятий;

2) предотвращения утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также электроакустических преобразований — достигается применением защищенных технических средств, аппаратных средств защиты, средств активного противодействия, экранированием зданий или отдельных помещений, установлением контролируемой зоны вокруг средств информатизации и другими организационными и техническими мерами;

3) исключения несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации — достигается применением специальных программно-технических средств защиты, использованием криптографических способов защиты, а также организационными и режимными мероприятиями;

4) предотвращения специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации, — достигается применением специальных программных и аппаратных средств защиты (антивирусных процес-

соров, антивирусных программ), организацией системы контроля безопасности программного обеспечения;

5) выявления возможно внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств) — достигается проведением специальных проверок по выявлению этих устройств;

6) предотвращения перехвата техническими средствами речевой информации из помещений и объектов — достигается применением специальных средств защиты, проектными решениями, обеспечивающими звукоизоляцию помещений, выявлением специальных устройств подслушивания и другими организационными и режимными мероприятиями.

Защита информации считается *эффективной*, если принимаемые меры соответствуют установленным требованиям или нормам.

Несоответствие мер установленным требованиям или нормам по защите информации является *нарушением* (рис. 4.5). При обнаружении нарушений первой категории руководители органов государственной власти и предприятий обязаны:

1) немедленно прекратить работы на участке (рабочем месте), где обнаружены нарушения, и принять меры по их устранению;

2) организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц;

3) сообщить в Государственную техническую комиссию при Президенте РФ, руководству органа государственной власти, федеральному органу государственной безопасности и заказчику о вскрытых нарушениях и принятых мерах.

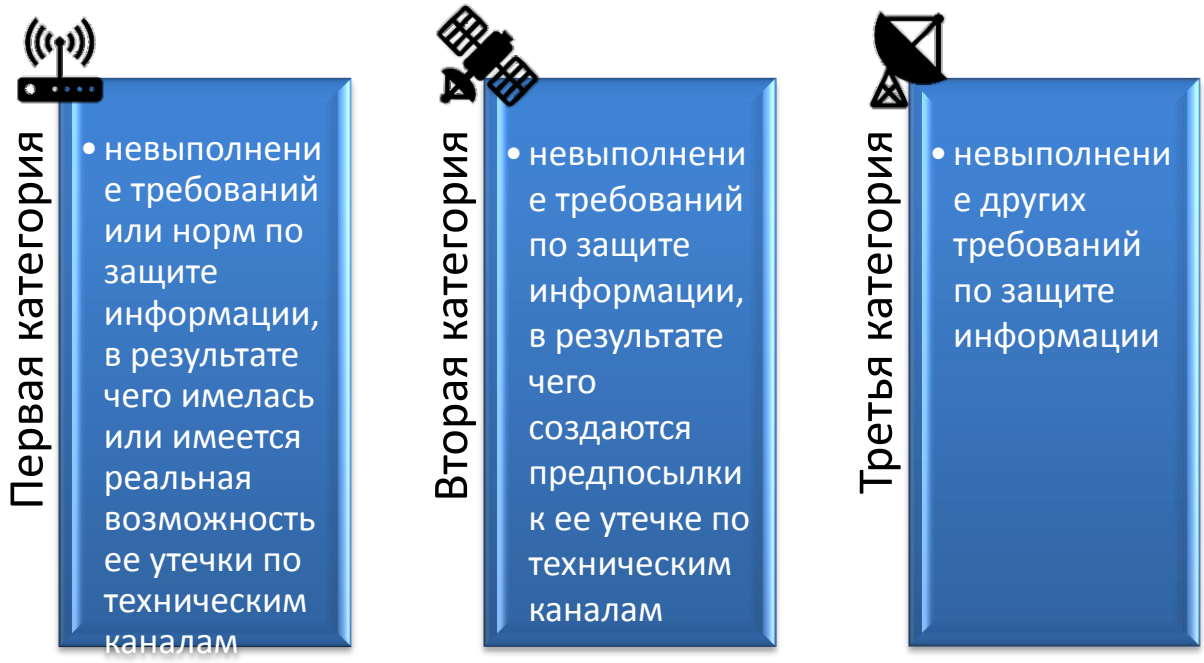


Рис. 4.5. **Нарушения по степени важности**

Возобновление работ разрешается после устранения нарушений и проверки достаточности и эффективности принятых мер, проводимой ФСТЭК России или по ее поручению подразделениями по защите информации органов государственной власти.

При обнаружении нарушений второй и третьей категорий руководители проверяемых органов государственной власти и предприятий обязаны принять необходимые меры по их устранению в сроки, согласованные с органом, проводившим проверку, или заказчиком (представителем заказчика). Контроль за устранением этих нарушений осуществляется подразделениями по защите информации этих органов государственной власти и предприятий.

Финансирование мероприятий по защите информации, содержащей сведения, отнесенные к государственной или служебной тайне, а также подразделений по защите информации в органах государственной власти и на бюджетных предприятиях предусматривается в сметах расходов на их содержание.

Создание технических средств зашиты информации, не требующее капитальных вложений, осуществляется в пределах средств, выделяемых заказчикам на научно-исследовательские и опытно-конструкторские работы, связанные с разработкой продукции. Расходы по разработке технических средств защиты включаются в стоимость разработки образца продукции.

Создание технических средств защиты информации, требующее капитальных вложений, осуществляется в пределах средств, выделяемых заказчикам на строительство (реконструкцию) сооружений или объектов.

Контрольные вопросы и задания

1. Какие отношения регулирует Закон РФ «О государственной тайне»?
2. Дайте определение понятию «государственная тайна».
3. Дайте определение понятию «носители сведений, составляющих государственную тайну».
4. Дайте определение понятию «система защиты государственной тайны».
5. Определите понятия «допуск к государственной тайне» и «доступ к сведениям, составляющим государственную тайну».
6. Дайте определение понятию «гриф секретности».
7. Дайте определение понятию «средства защиты информации».
8. Какие сведения в военной области могут быть отнесены к государственной тайне в соответствии с Законом РФ «О государственной тайне»?
9. Какие сведения в области экономики, науки и техники могут быть отнесены к государственной тайне в соответствии с Законом РФ «О государственной тайне»?
10. Какие сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности могут быть отнесены к государственной тайне в соответствии с Законом РФ «О государственной тайне»?

11. Как подразделяются сведения, отнесенные к государственной тайне, по степени секретности?

12. Какие органы относятся к органам защиты государственной тайны?

13. Что предусматривает допуск должностных лиц и граждан к государственной тайне?

14. Каков размер ежемесячной процентной надбавки к должностному окладу (тарифной ставке) граждан, допущенных к государственной тайне на постоянной основе?

15. Что может служить основанием для отказа должностному лицу или гражданину в допуске к государственной тайне?

16. Кем осуществляется надзор за соблюдением законодательства при обеспечении защиты государственной тайны и законностью принимаемых при этом решений?

17. Какие основные организационно-технические мероприятия по защите информации, содержащей сведения, составляющие государственную или служебную тайну, определены в Положении о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам (утверждено постановлением Совета Министров — Правительства РФ от 15 сентября 1993 г. № 912-51)?

18. Определите объекты защиты в системах и средствах информатизации и связи во всех органах государственной власти и на предприятиях, располагающих информацией, содержащей сведения, отнесенные к государственной или служебной тайне.

19. С помощью каких мероприятий с применением технических средств осуществляется защита информации, содержащей сведения, отнесенные к государственной тайне?

20. Какие могут быть зафиксированы нарушения по степени важности в органах государственной власти и на предприятиях, располагающих информацией, содержащей сведения, отнесенные к государственной или служебной тайне?

Тема 5. Основные нормативные документы в области обеспечения безопасности информации

Необходимой составляющей государственной системы обеспечения информационной безопасности являются: национальные стандарты Российской Федерации (утверждаются приказами Росстандарта), руководящие, нормативно-технические и методические документы по безопасности информации[1].

[1] *Безопасность информации* [данных] — состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность [ГОСТ Р 50922-2006].

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0-2012 «Стандартизация в Российской Федерации. Основные положения» (взамен ГОСТ Р 1.0-2004).

Основные национальные стандарты РФ:

— ГОСТ Р 50922-2006. Защита информации. Основные термины и определения (взамен ГОСТ Р 50922-96). В настоящем стандарте 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». Настоящий стандарт устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации[1];

— ГОСТ Р 52069.0-2013. Защита информации. Система стандартов. Основные положения (взамен ГОСТ Р 52069.0-2003). Настоящий стандарт устанавливает цель, задачи и структуру системы стандартов по защите (некриптографическими методами) информации[2], объекты и аспекты стандартизации в данной области. Положения настоящего стандарта применяются при проведении работ по стандартизации в области противодействия техническим разведкам, технической защиты информации[3] некриптографическими методами, обеспечения (некриптографическими методами) безопасности информации в ключевых системах информационной инфраструктуры. Настоящий стандарт является основополагающим национальным стандартом Российской Федерации в области защиты (некриптографическими методами) информации;

— ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения (взамен ГОСТ Р 51275-99) (URL: http://docs.cntd.ru/document/1200057516). Настоящий стандарт устанавливает классификацию и перечень факторов, воздействующих на безопасность защищаемой информации[4], в целях обоснования угроз безопас-

---

[1] *Защита информации,* ЗИ — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [ГОСТ Р 50922-2006].

[2] *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 [ГОСТ Р 52069.0-2013].

[3] *Техническая защита информации*, ТЗИ — защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств [ГОСТ Р 50922-2006].

[4] *Защищаемая информация* — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации [ГОСТ Р 50922-2006].

ности информации[1] и требований по защите информации на объекте информатизации[2];

— ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении (URL: http://docs.cntd.ru/document/1200108858). Общие положения. Настоящий стандарт распространяется на создаваемые (модернизируемые) информационные автоматизированные системы, в отношении которых законодательством или заказчиком установлены требования по их защите, и устанавливает содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении, содержание и порядок выполнения работ по защите информации о создаваемой (модернизируемой) автоматизированной системе в защищенном исполнении;

— ГОСТ Р 56093-2014. Защита информации. Автоматизированные системы в защищенном исполнении средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования (URL: http://docs.cntd.ru/document/1200112853). Настоящий стандарт устанавливает требования к средствам обнаружения факта преднамеренных силовых электромагнитных воздействий[3] на автоматизированные системы в защищенном исполнении с выдачей извещения о его воздействии, а также к средствам обнаружения, которые обеспечивают формирование данных об амплитудных, временных и иных характеристиках преднамеренных силовых электромагнитных воздействий, необходимых для их обработки в системах более высокого уровня, требования к которым настоящим стандартом не устанавливаются;

— ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей (URL: http://docs.cntd.ru/document/1200123701). Настоящий стандарт устанавливает общие требования к структуре описания уязвимости и правилам описания уязвимости информационной системы[4] (ИС). В настоящем стандарте принята

---

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

[2] *Объект информатизации* — 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 [ГОСТ Р 51275-2006].

[3] *Преднамеренное силовое электромагнитное воздействие на информацию* — несанкционированное воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения (генерирования) в автоматизированных информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем [ГОСТ Р 50922-2006].

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

структура описания уязвимости, использование которой позволит обеспечить достаточность информации для идентификации уязвимости ИС и выполнения работ по анализу уязвимостей ИС. Стандарт не распространяется на уязвимости ИС, связанные с утечкой информации по техническим каналам, в том числе уязвимостями электронных компонентов технических (аппаратных и аппаратно-программных) средств информационных систем;

— ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем (URL: http://docs.cntd.ru/document/1200123702). Настоящий стандарт устанавливает классификацию уязвимостей информационных систем и направлен на совершенствование методического обеспечения определения и описания угроз безопасности информации при проведении работ по защите информации в ИС;

— ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель (URL: http://docs.cntd.ru/document/1200071694) (взамен ГОСТ Р ИСО/МЭК 15408-1-2002). ИСО/МЭК 15408 предназначен для использования в качестве основы при оценке характеристик безопасности продуктов или систем информационных технологий (ИТ). Устанавливая общую базу критериев, ИСО/МЭК 15408 позволяет сделать результаты оценки безопасности ИТ значимыми для более широкой аудитории;

— ГОСТ Р ИСО/МЭК 15408-2-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (URL: http://docs.cntd.ru/document/1200069465) (взамен ГОСТ Р ИСО/МЭК 15408-2-2002). Настоящий стандарт устанавливает структуру и содержание компонентов функциональных требований безопасности для оценки безопасности. Он также включает в себя каталог функциональных компонентов, отвечающих общим требованиям к функциональным возможностям безопасности многих продуктов и систем ИТ;

— ГОСТ Р ИСО/МЭК 15408-3-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности (URL: http://docs.cntd.ru/document/1200069464) (взамен ГОСТ Р ИСО/МЭК 15408-3-2002). Настоящий стандарт устанавливает требования доверия ИСО/МЭК 15408 и включает в себя оценочные уровни доверия (ОУД), определяющие шкалу для измерения доверия, собственно компоненты доверия, из которых составлены уровни доверия, и критерии для оценки профиля защиты (ПЗ) и задания по безопасности (ЗБ);

— ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Настоящий стандарт представляет собой руководство по управлению безопасностью информационных и телекоммуникационных тех-

нологий (ИТТ), устанавливает концепцию и модели, лежащие в основе базового понимания безопасности ИТТ, и раскрывает общие вопросы управления, которые важны для успешного планирования, реализации и поддержки безопасности ИТТ. Целью настоящего стандарта является формирование общих понятий и моделей управления безопасностью ИТТ. Приведенные в нем положения носят общий характер и применимы к различным методам управления и организациям. Настоящий стандарт разработан так, что позволяет приспосабливать его положения к потребностям организации и свойственному ей стилю управления. Настоящий стандарт не разрабатывает конкретных подходов к управлению безопасностью;

— ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. В настоящем стандарте содержатся рекомендации по менеджменту инцидентов информационной безопасности[1] в организациях для руководителей подразделений по обеспечению информационной безопасности (ИБ) при применении информационных технологий (ИТ), информационных систем, сервисов и сетей;

— ГОСТ Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология (URL: http://docs.cntd.ru/document/1200102762/). Настоящий стандарт содержит: обзор семейства стандартов системы менеджмента информационной безопасности (СМИБ)[2]; введение в СМИБ; краткое описание процесса «План (Plan) — Осуществление (Do) — Проверка (Check) — Действие (Act)» (PDCA); термины и определения для использования в семействе стандартов СМИБ. Настоящий стандарт применим ко всем типам организаций (например, коммерческие предприятия, правительственные учреждения, некоммерческие организации);

— ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (URL: http://docs.cntd.ru/document/1200058325/). Настоящий стандарт предназначен для применения организациями любой формы собственности (например, коммерческими, государственными и некоммерческими организациями). Настоящий стандарт устанавливает требования по разработке, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению документированной системы менеджмента информационной безопасности (СМИБ) среди общих бизнес-

[1] *Инцидент информационной безопасности* (information security incident) — появление одного или нескольких нежелательных, или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ [ГОСТ Р ИСО/МЭК ТО 18044-2007].

[2] *Система менеджмента информационной безопасности* (СМИБ) (information security management system (ISMS)) — часть общей системы менеджмента, основанная на подходе бизнес-рисков по созданию, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению информационной безопасности [ГОСТ Р ИСО/МЭК 27000-2012].

рисков организации. Кроме этого, стандарт устанавливает требования по внедрению мер управления информационной безопасностью и ее контроля, которые могут быть использованы организациями или их подразделениями в соответствии с установленными целями и задачами обеспечения информационной безопасности (ИБ). Целью построения СМИБ является выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон;

— ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности (URL: http://docs.cntd.ru/document/1200103619/) (взамен ГОСТ Р ИСО/МЭК 17799-2005). Настоящий национальный стандарт предлагает рекомендации и основные принципы введения, реализации, поддержки и улучшения менеджмента информационной безопасности в организации. Цели, изложенные в данном национальном стандарте, обеспечивают полное руководство по общепринятым целям менеджмента информационной безопасности. Реализация целей управления, а также мер и средств контроля и управления настоящего национального стандарта направлена на удовлетворение требований, определенных оценкой рисков. Настоящий национальный стандарт может служить практическим руководством по разработке стандартов безопасности организации, для эффективной практики менеджмента безопасности организаций и способствует укреплению доверия в отношениях между организациями;

— ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности (URL: http://docs.cntd.ru/document/1200084141) (взамен ГОСТ Р ИСО/МЭК ТО 13335-3-2007 и ГОСТ Р ИСО/МЭК ТО 13335-4-2007). Настоящий стандарт представляет руководство по менеджменту риска информационной безопасности. Настоящий стандарт поддерживает общие концепции, определенные в ИСО/МЭК 27001, и предназначен для содействия адекватного обеспечения информационной безопасности на основе подхода, связанного с менеджментом риска. Знание концепций, моделей, процессов и терминологии, изложенных в ИСО/МЭК 27001 и ИСО/МЭК 27002, важно для полного понимания настоящего стандарта;

— ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи (URL: http://docs.cntd.ru/document/1200095034) (взамен ГОСТ Р 34.10-2001). Настоящий стандарт определяет схему электронной цифровой подписи (ЭЦП, цифровая подпись), процессы формирования и проверки цифровой подписи под заданным сообщением (документом), передаваемым по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения. Внедрение цифровой подписи на основе настоящего стандарта повышает по сравнению с ранее действовавшей схемой цифровой подписи уровень защищенности передаваемых сообщений от подделок и искажений. Настоящий стандарт

рекомендуется применять при создании, эксплуатации и модернизации систем обработки информации различного назначения;

— ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования (URL: http://docs.cntd.ru/document/1200095035) (взамен ГОСТ Р 34.11-94). Настоящий стандарт определяет алгоритм и процедуру вычисления хэш-функции для любой последовательности двоичных символов, которые применяются в криптографических методах обработки и защиты информации, в том числе для реализации процедур обеспечения целостности, аутентичности, электронной цифровой подписи (ЭЦП) при передаче, обработке и хранении информации в автоматизированных системах;

— ГОСТ Р 34.13-2015. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров (URL: http://docs.cntd.ru/document/1200121984) (взамен ГОСТ Р ИСО/МЭК 10116-93). Режимы работы блочных шифров, определенные в настоящем стандарте, рекомендуется использовать при разработке, производстве, эксплуатации и модернизации средств криптографической защиты информации в системах обработки информации различного назначения. Настоящим стандартом следует руководствоваться, если информация конфиденциального характера подлежит защите в соответствии с законодательством РФ и др.

Перечень технической документации, национальных стандартов и методических документов, необходимых для выполнения работ и оказания услуг, установленных положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79, утв. директором ФСТЭК России 24 июля 2017 г.

— Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992;

— Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден решением председателя Гостехкомиссии России от 30.03.1992;

— Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Утвержден решением председателя Гостехкомиссии России от 30.03.1992;

— Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992;

— Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизи-

рованных систем и требования по защите информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992;

— Положение о сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом председателя Гостехкомиссии России от 27.10.1995 № 199;

— Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом Гостехкомиссии России от 04.06.1999 № 114;

— Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 02.03.2001 № 282. ДСП;

— Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП;

— Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП;

— Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП;

— Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электро-акустических преобразований во вспомогательных технических средствах и системах. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001. ДСП;

— Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15.02.2008. ДСП;

— Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 06.12.2011 № 638. ДСП;

— Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи. Утвержден приказом ФСТЭК России от 15.03.2012 № 27. ДСП;

— Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 № 28. ДСП;

— Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11.02.2013 №17;

— Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информа-

ционных системах персональных данных. Утверждены приказом ФСТЭК России от 18.02.2013 № 21;

— Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27.09.2013 № 119. ДСП;

— Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11.02.2014;

— Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. Утверждены приказом ФСТЭК России от 14.03.2014 № 31;

— Требования к средствам контроля съемных машинных носителей информации. Утверждены приказом ФСТЭК России от 28.07.2014 № 87. ДСП;

— Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 09.02.2016 № 9. ДСП;

— Требованиям безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19.08.2016 № 119. ДСП и др.

Основные акты, нормативные и методические документы ФСТЭК России в области защиты персональных данных:

— Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России 14 февраля 2008 г.;

— Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России 15 февраля 2008 г.;

— приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

— приказ ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

— Методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 г. и др.

Основные документы ФСБ России:

— приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)». Положение регулирует отношения, возникающие при разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержа-

щей сведений, составляющих государственную тайну (информация конфиденциального характера);

— Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденные ФСБ России 31 марта 2015 г. № 149/7/2/6-432;

— приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности». Настоящий документ определяет состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации (СКЗИ), необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности и др.

Контрольные вопросы и задания

1. Опишите сферу применения Федерального закона «О техническом регулировании».
2. Как Федеральный закон «О техническом регулировании» определяет «стандарт иностранного государства»?
3. Как Федеральный закон «О техническом регулировании» определяет «региональный стандарт»?
4. Назовите цели и задачи стандартизации в Российской Федерации.
5. С какими принципами осуществляют национальную стандартизацию в Российской Федерации?
6. Каковы основные задачи международного сотрудничества в области стандартизации?
7. Как ГОСТ Р 50922-2006 определяет термин «защита информации»?
8. Как ГОСТ Р 50922-2006 определяет термины, относящиеся к видам защиты информации (правовая защита информации, техническая защита информации, криптографическая защита информации, физическая защита информации)?
9. Как ГОСТ Р 50922-2006 определяет термины, относящиеся к способам защиты информации (способ защиты информации, защита информации от утечки, защита информации от несанкционированного воздействия, защита информации от непреднамеренного воздействия, защита информации от разглашения, защита информации от несанкционированного доступа, защита

информации от преднамеренного воздействия, защита информации от [иностранной] разведки)?

10. Как ГОСТ Р 50922-2006 определяет термины, относящиеся к замыслу защиты информации (замысел защиты информации, цель защиты информации, система защиты информации, политика безопасности (информации в организации), безопасность информации [данных]?

11. Как ГОСТ Р 50922-2006 определяет термины, относящиеся к объекту защиты информации (объект защиты информации, защищаемая информация, носитель защищаемой информации, защищаемый объект информатизации, защищаемая информационная система)?

12. Как ГОСТ Р 50922-2006 определяет термины, относящиеся к угрозам безопасности информации (угроза (безопасности информации), фактор, воздействующий на защищаемую информацию, источник угрозы безопасности информации, уязвимость (информационной системы), вредоносная программа, несанкционированное воздействие на информацию преднамеренное силовое электромагнитное воздействие на информацию, модель угроз (безопасности информации))?

13. Как ГОСТ Р 50922-2006 определяет термины, относящиеся к технике защиты информации (техника защиты информации, средство защиты информации, средство контроля эффективности защиты информации, средство физической защиты информации, криптографическое средство защиты информации)?

14. Как ГОСТ Р 50922-2006 определяет термины, относящиеся к способам оценки соответствия требованиям по защите информации (оценка соответствия требованиям по защите информации, лицензирование в области защиты информации, сертификация на соответствие требованиям по безопасности информации, специальное исследование (объекта защиты информации), специальная проверка, аудиторская проверка информационной безопасности в организации, мониторинг безопасности информации, экспертиза документа по защите информации, анализ информационного риска, оценка информационного риска)?

15. Как ГОСТ Р 50922-2006 определяет термины, относящиеся к эффективности защиты информации (эффективность защиты информации, требование по защите информации, показатель эффективности защиты информации, норма эффективности защиты информации)?

Тесты

1. Что из ниже перечисленного относится к проблемам информации (*выберите несколько вариантов ответа*)?

1) обеспечение целостности;
2) обеспечение неделимости;
3) обеспечение достоверности;
4) обеспечение чистоты;
5) обеспечение защиты от различного вида угроз.

2. Процесс обеспечения информационных потребностей общества на основе применения новейших информационных технологий — это…

1) компьютеризация;
2) информатика;
3) информатизация;
4) информационная индустрия;
5) автоматизация.

3. Информационная система — это…

1) посредник между потребителем информации и информационным массивом;
2) ряд компьютеров, объединенных в локальную сеть;
3) совокупность технических средств обработки информации;
4) группа людей, ответственная за обработку, накопление, хранение и выдачу информации;
5) средства массовой информации, функционирующие на территории определенного государства.

4. Какие свойства информации являются наиболее важными в практическом применении (*выберите несколько вариантов ответа*)?

1) ценность;
2) популярность;
3) достоверность;
4) чистота;
5) своевременность.

5. Что является основной причиной старения информации?

1) физическая изношенность носителя;
2) появление новой информации, с поступлением которой прежняя информация оказывается неверной;
3) устаревание знаковой системы, посредством которой выражена информация;
4) уменьшение потребности в информации;
5) величина длительности хранения информации: чем больше длительность, тем информация старее.

6. Совокупность взаимосвязанных и взаимообусловленных процессов выявления, анализа, ввода и отбора информации, выдачи с помощью различных средств ее потребителю для принятия управленческого решения — это…

1) процессы обработки информации;
2) циркуляция информации;
3) информационные процессы;
4) процессы перераспределения информации;
5) вычислительные процессы.

7. Организационно-упорядоченная совокупность людей, информационных ресурсов, технических средств и технологий обработки информации, имеющая своей целью сбор, обработку, накопление, хранение, актуализацию, поиск и выдачу информации — это…

1) автоматизированная инфраструктура;
2) информационная система;
3) информационная структура;
4) автоматизированная система;
6) информационный ресурс.

8. Что понимается под безошибочностью данных?

1) свойство данных не иметь явных ошибок;
2) свойство данных полностью соответствовать области их применения;
3) свойство данных не иметь скрытых случайных ошибок;
4) свойство данных соответствовать нескольким областям человеческой деятельности;
5) свойство данных не иметь противоречий в собственной структуре;

9. Назовите свойство данных, которое заключается в том, что время их сбора и переработки соответствует динамике изменения ситуации:

1) идентичность;
2) оперативность;
3) динамичность;
4) адаптивность;
5) актуальность.

10. Каким свойством обладают данные, соответствующие состоянию объекта (явления)?

1) идентичность;
2) объективность;
3) эквивалентность;
4) неотрывность;
5) целостность.

11. Что является источником информации, обладающей свойством «общественная природа»?

1) живые организмы, несущие в своем строении определенную биологическую информацию;
2) структура и состояние современного общества;
3) отношения между людьми;
4) познавательная деятельность людей, общества;
5) состояние окружающей среды.

12. Что подразумевается под целостностью информации (*выберите несколько вариантов ответа*)?

1) принадлежность информации одному источнику;
2) неделимость информации;
3) актуальность информации;
4) непротиворечивость информации;
5) защищенность информации от разрушения и несанкционированного изменения.

13. Меры каких уровней необходимо принимать при обеспечении защиты интересов субъектов информационных отношений?

1) социального;
2) законодательного;
3) исполнительного;
4) административного;
5) экономического;
6) процедурного;
7) функционального;
8) программно-технического;
9) программно-аппаратного.

14. Что относится к основным составляющим информационной безопасности (*выберите несколько вариантов ответа*)?

1) защита информации;
2) компьютерная безопасность;
3) экологическая безопасность;
4) защищенность информации и поддерживающей инфраструктуры;
5) защита от информации;
6) защищенность потребностей граждан.

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

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

16. Обозначьте основные направления деятельности на законодательном уроне в сфере обеспечения информационной безопасности (*выберите несколько вариантов ответа*)?

1) разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;
2) ориентация на созидательные законы;
3) ориентация на карательные законы;
4) создание уникальных стандартов и сертификационных нормативов, актуальных только в России;
5) интеграция в мировое правовое пространство;
6) учет современного состояния информационных технологий;
7) использование исключительно собственного опыта при создании нормативно-правовой базы в области информационной безопасности.

17. Выделите основные группы процедурных мер, направленных на обеспечение информационной безопасности (*выберите несколько вариантов ответа*).

1) программная защита;
2) управление персоналом;
3) управление ресурсами;
4) аппаратная защита;
5) физическая защита;
6) поддержание работоспособности;
7) реагирование на нарушения режима безопасности;
8) обеспечение стабильности;
9) планирование восстановительных работ.

18. На чем основывается политика информационной безопасности в организации*?*

1) на выявлении всех возможных угроз информационной безопасности организации;
2) на поиске уязвимостей информационной системы организации;
3) на анализе рисков, признанных реальными для информационной системы организации;
4) на закупке оборудования, предотвращающего утечку информации по техническим каналам;
5) на регистрации всех действий персонала при работе с защищаемой информацией.

19. Уполномоченными лицами считаются … (*выберите несколько вариантов ответа*)

1) собственники информации;
2) владельцы информации;
3) пользователи информации;

4) пользователи, получившие право работы с информацией от ее владельца;

5) государственные служащие;

6) работники силовых структур.

20. Уязвимость — это …

1) наличие узких мест в системе защиты информации;

2) слабость системы информационной безопасности;

3) незащищенность или ошибка в объекте, которая может привести к возникновению угрозы;

4) наличие угроз информационной безопасности;

5) незащищенность объектов информационной системы.

21. Неумышленное происшествие с деструктивным воздействием на объект — это …

1) ошибка;

2) катастрофа;

3) авария;

4) повреждение;

5) поломка.

22. Для чего предназначены информационные способы работы с информационными потоками (*выберите несколько вариантов ответа*)?

1) сбор информации;

2) качественное, своевременное и достоверное удовлетворение информационных потребностей пользователей;

3) перераспределение информации;

4) передача информации;

5) уничтожение информации.

23. Основные компоненты информатизации включают в себя (*выберите несколько вариантов ответа*) …

1) оборудование;

2) вычислительные сети;

3) информационные системы;

4) каналы связи;

5) информационные ресурсы.

24. Информационные ресурсы — это…

1) документ, входящий в информационную систему;

2) массивы документов;

3) файлы, хранящиеся в памяти компьютера;

4) документы и массивы документов в разных формах и видах, содержащие информацию по всем направлениям жизнедеятельности общества;

5) все существующие знания.

25. Что из нижеперечисленного относится к свойствам информации (*выберите несколько вариантов ответа*)?

1) неотрывность от языка носителя;
2) дискретность;
3) периодичность;
4) независимость от создателей;
5) латентность.

26. Фиксированные информационные ресурсы — это…

1) некоторые сведения, которые не могут менять свое содержание со временем;
2) информация, закрепленная на каком-нибудь физическом носителе;
3) набор символов, имеющий смысл и определенную размерность;
4) фиксированный массив документов, необходимый для удовлетворения информационных потребностей общества в определенной сфере деятельности;
5) документы определенного вида.

27. Информация — это…

1) входные данные;
2) фиксированный набор символов естественного языка;
3) сведения о лицах, предметах, событиях, явлениях и процессах, хранящиеся в памяти ЭВМ;
4) сведения о лицах, предметах, событиях, явлениях и процессах, отраженные на материальных носителях, используемые в целях получения знаний и практических решений;
5) признаковая структура объектов.

28. Чем определяется ценность информации*?*

1) рыночной стоимостью;
2) обеспечением возможности достижения цели, поставленной перед получателем;
3) стоимостью носителя;
4) степенью доверия к источнику;
5) количеством заинтересованных в ней лиц.

29. Что такое защита информации?

1) создание защищенных банков данных конфиденциальной информации;
2) комплекс мероприятий по обеспечению конфиденциальности, целостности, доступности, учета и неотрекаемости информации;
3) набор аппаратных и программных средств для обеспечения конфиденциальности, целостности, доступности, учета и неотрекаемости информации;

4) комплекс мероприятий по обеспечению сохранности, доступности и конфиденциальности данных в компьютерных сетях;

5) обеспечение кодирования информации, передаваемой в локальной сети организации.

30. Возможность за приемлемое время получить требуемую информационную услугу определяет …

1) отказоустойчивость информационной системы;
2) время отклика системы;
3) пропускную способность канала;
4) качество сервиса;
5) степень доступности информации.

31. Что подразумевается под комплексом организационных, технических и технологических мер по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе?

1) информационная защищенность;
2) информационная стабильность;
3) стойкость информационной системы;
4) национальная безопасность;
5) информационная безопасность.

32. Что такое «угроза»?

1) возможность реализации несанкционированных действий в отношении информационной системы;
2) невосполнимый ущерб, нанесенный государственной организации;
3) предотвращенное деструктивное воздействие на информационную систему;
4) непоправимый вред, наносимый окружающей среде;
5) уязвимость информационной системы.

33. Назовите основные средства защиты информации (*выберите несколько вариантов ответа*):

1) электромеханические;
2) физические;
3) аппаратные;
4) виброакустические;
5) программные;
6) криптографические;
7) идентификационные.

34. Назовите свойство данных сохранять ценность для потребителя с течением времени, т.е. не подвергаться моральному старению:

1) актуальность;
2) значимость;

3) неизменность;
4) срочность;
5) постоянность.

35. Что понимается под совокупностью документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов*?*

1) информационная политика;
2) безопасность информации;
3) политика безопасности;
4) регламентация доступа;
5) организация защиты.

36. 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) протоколирование и аудит;
6) обеспечение высокой производительности системы;
7) обновление;
8) криптография;
9) межсетевое экранирование;
10) обеспечение высокой доступности.

37. Перечислите основные группы мер, которые необходимо реализовывать на законодательном уровне для обеспечения информационной безопасности (*выберите несколько вариантов ответа*);

1) меры, направленные на увеличение количества аппаратно-программных продуктов иностранного производства на отечественном рынке;

2) меры, направленные на создание и поддержание в обществе негативного отношения к нарушениям и нарушителям информационной безопасности;

3) меры, направленные на снижение использования средств вычислительной техники (СВТ) во всех сферах человеческой деятельности;

4) меры, направленные на ограничение доступа рядовых граждан к механизмам информационной безопасности;

5) меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности.

38. Фиксация и анализ всех действий уполномоченных лиц, выполняемых ими в рамках, контролируемых системой информационной безопасности — это …

1) контроль;
2) учет;
3) база знаний;
4) слежка;
5) регистрация.

39. Попытка практической реализации угрозы — это …

1) взлом;
2) атака;
3) кража;
4) нападение;
5) удаленная атака.

40. Каким свойством обладают данные, характеризующие текущую ситуацию?

1) адаптивность;
2) корректность;
3) непротиворечивость;
4) целостность;
5) актуальность.

41. Субъект, преследующий корыстные или деструктивные цели, противоречащие целям системы, — это …

1) вредитель;
2) хакер;
3) агент конкурирующей системы;
4) правонарушитель;
5) злоумышленник.

42. Что понимается под истинностью данных?

1) свойство данных не иметь скрытых случайных ошибок;
2) свойство данных постоянно соответствовать текущей ситуации;
3) свойство данных противостоять деструктивному воздействию;
4) свойство данных не иметь явных ошибок;
5) свойство данных не иметь преднамеренные искажения человеком — источником сведений или искажения, вносимые средствами обработки информации.

43. Что представляет собой «информационная безопасность» в соответствии с Доктриной информационной безопасности Российской Федерации?

1) состояние системы, при котором она способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз;

2) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

3) состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства;

4) состояние информационной системы предприятия, при котором невозможно деструктивное воздействие на элементы данной системы со стороны сотрудников организации;

5) состояние защищенности информационных ресурсов от дестабилизирующего воздействия внешних и внутренних злоумышленников.

44. Что представляет собой объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы*?*

7) государственная информационная политика;

8) информационная безопасность Российской Федерации;

9) национальные интересы Российской Федерации в информационной сфере;

10) информационные интересы Российской Федерации;

11) национальная безопасность Российской Федерации в информационной сфере.

45. Что представляет собой совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства*?*

1) мировую экологическую обстановку;

2) злоумышленные действия вражеской разведки;

3) потенциальный вред;

4) угрозу;

5) промышленный шпионаж с привлечением разведывательных и специальных служб.

46. Что можно отнести к важнейшим принципам деятельности государственных органов по обеспечению информационной безопасности (*выберите несколько вариантов ответа*)?

1) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений;

2) предоставление гражданам информации по работе государственных органов на всех уровнях;

3) конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

4) соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями;

5) развитие систем массовой информации Российской Федерации.

47. Что можно отнести к внутренним угрозам информационной безопасности в соответствии с Доктриной информационной безопасности Российской Федерации (*выберите несколько вариантов ответа*)?

1) расширение областей применения информационных технологий;

2) информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей;

3) возрастающие масштабы компьютерной преступности;

4) целенаправленное вмешательство и проникновение в деятельность и развитие информационных систем Российской Федерации;

5) высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи.

48. Что является стратегической целью обеспечения информационной безопасности в области обороны страны согласно Доктрине информационной безопасности Российской Федерации?

1) защита суверенитета;

2) поддержание обороноспособности Российской Федерации;

3) защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях;

4) поддержание территориальной целостности Российской Федерации;

5) обеспечение основных прав и свобод человека и гражданина.

49. Перечислите организации, которые входят в состав организационной основы системы обеспечения информационной безопасности Российской Федерации (*выберите несколько вариантов ответа*);

1) ФСБ России;

2) Совет Федерации Федерального Собрания РФ;

3) Совет Безопасности Российской Федерации;

4) ФСТЭК России;

5) Государственная Дума Федерального Собрания РФ;

6) МВД России;

7) Правительство РФ.

50. Основным органом, координирующим действия государственных структур по вопросам защиты государственной тайны, является;

1) Совет Безопасности Российской Федерации;
2) ФСБ России;
3) Межведомственная комиссия по защите государственной тайны;
4) СВР России;
5) Минобороны России;
6) Роскомнадзор.

51. Назовите организацию, координирующую деятельность государственной системы противодействия техническим разведкам и технической защиты информации:

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

52. Что относится к основной деятельности Минобороны России в области обеспечения информационной безопасности*?*

1) разработка криптографических средств защиты информации;
2) организация деятельности по обеспечению информационной безопасности, защите государственной тайны в Вооруженных Силах РФ;
3) организационно-техническое обеспечение деятельности Межведомственной комиссии по защите государственной тайны;
4) организация деятельности государственной системы противодействия техническим разведкам на федеральном уровне;
5) техническая защита информации в аппаратах федеральных органов государственной власти.

53. К угрозам информационной безопасности для личности можно отнести … (*выберите несколько вариантов ответа*)

1) препятствия в построении информационного общества;
2) манипулирование массовым сознанием;
3) лишение права граждан на неприкосновенность частной жизни;
4) противодействие защите интересов личности и общества;
5) нарушение права граждан на защиту своего здоровья от неосознаваемой человеком вредной информации.

54. К угрозам информационной безопасности для государства можно отнести … (*выберите несколько вариантов ответа*)

1) лишение права граждан на неприкосновенность частной жизни;
2) противодействие защите интересов личности и общества;
3) посягательства на объекты интеллектуальной собственности;

4) противодействие защите единого информационного пространства страны;

5) противодействие построению правового государства.

55. Что представляет собой «информационная сфера» в соответствии с Доктриной информационной безопасности Российской Федерации?

1) системообразующий фактор жизни общества, активно влияющий на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации;

2) совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений;

3) федеральная государственная информационная система, порядок использования которой устанавливается Правительством РФ и которая обеспечивает в случаях, предусмотренных законодательством РФ, санкционированный доступ к информации, содержащейся в информационных системах;

4) совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений;

5) совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории РФ, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров РФ.

56. Национальными интересами Российской Федерации в информационной сфере являются (*выберите несколько вариантов ответа*):

1) защита государственных информационных ресурсов от несанкционированного доступа;

2) развитие в Российской Федерации отрасли информационных технологий и электронной промышленности;

3) обеспечение свободного сбора, хранения, использования и распространения информации о частной жизни граждан Российской Федерации;

4) обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации;

5) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности.

57. Какие бывают уровни воздействия информационной безопасности (*выберите несколько вариантов ответа*)?

1) для личности;
2) для организации;
3) для государства;
4) для предприятия;
5) для общества;
6) для субъекта РФ.

58. Что можно отнести к важнейшим задачам государственных органов в рамках деятельности по обеспечению информационной безопасности (*выберите несколько вариантов ответа*)?

1) организация разведывательной деятельности для обеспечения информационной безопасности личности, общества и государства;
2) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;
3) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;
4) государственная поддержка разработки, производства и эксплуатации средств информационного взаимодействия;
5) планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности.

59. Что можно отнести к внешним угрозам информационной безопасности в соответствии с Доктриной информационной безопасности Российской Федерации (*выберите несколько вариантов ответа*)?

1) наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях;
2) отставание России от ведущих стран мира по уровню информатизации;
3) увеличение в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации;
4) отсутствие четко сформулированной информационной политики, отвечающей национальным целям, ценностям и интересам;
5) информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

60. Что можно отнести к стратегическим целями обеспечения информационной безопасности в области государственной и общественной безопасности согласно Доктрине информационной безопасности Российской Федерации (*выберите несколько вариантов ответа*)?

1) защита суверенитета;
2) поддержание обороноспособности Российской Федерации;
3) обеспечение секретности информационной структуры Российской Федерации;
4) поддержание территориальной целостности Российской Федерации;
5) обеспечение основных прав и свобод человека и гражданина.

61. Перечислите участников системы обеспечения информационной безопасности Российской Федерации согласно Доктрине информационной безопасности Российской Федерации (*выберите несколько вариантов ответа*);
1) федеральные и муниципальные органы власти;
2) собственники объектов критической информационной инфраструктуры;
3) средства массовой информации и массовых коммуникаций;
4) организации, осуществляющие образовательную деятельность;
5) организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка;
6) организации и граждане Российской Федерации;
7) операторы связи.

62. Какие государственные органы Российской Федерации контролируют деятельность в области информационной безопасности (*выберите несколько вариантов ответа*)?
1) СВР России;
2) Совет Безопасности Российской Федерации;
3) Государственная Дума Федерального Собрания РФ;
4) ФСТЭК России;
5) ФСБ России;
6) МВД России;
7) Правительство РФ.

63. Что относится к задачам ФСТЭК России в области обеспечения информационной безопасности (*выберите несколько вариантов ответа*)?
1) разработка отраслевых документов по защите информации;
2) противодействие добыванию информации техническими средствами разведки, техническая защита информации;
3) разработка криптографических методов защиты информации;
4) осуществление нормативно-правового регулирования вопросов технической защиты информации;
5) прогнозирование развития сил, средств и возможностей технических разведок, выявление угроз безопасности информации.

64. Назовите организацию, обеспечивающую безопасность информационно-телекоммуникационных систем криптографическими и инженерно-техническими методами;

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

65. К угрозам информационной безопасности для общества можно отнести … (*выберите несколько вариантов ответа*)

1) нарушение права граждан на защиту своего здоровья от неосознаваемой человеком вредной информации;
2) препятствия в построении информационного общества;
3) манипулирование массовым сознанием;
4) препятствие формированию институтов общественного контроля органов государственной власти;
5) противодействие защите государственных информационных систем и государственных информационных ресурсов.

66. По происхождению угрозы информационной безопасности бывают … (*выберите несколько вариантов ответа*)

1) сторонние;
2) внезапные;
3) внутренние;
4) ожидаемые;
5) внешние.

67. 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.

68. 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».

69. Информация ограниченного доступа — это …

1) информация, доступ к которой ограничен федеральными законами;
2) информация, доступ к которой ограничен законами субъекта РФ;
3) информация, доступ к которой ограничен в силу указа Президента РФ;
4) информация, доступ к которой ограничен Конституцией РФ.

70. 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.

71. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя — это:
1) конфиденциальность информации;
2) недоступность информации;
3) засекреченность информации;
4) защита информации.

72. К информации ограниченного доступа не относятся;
1) санитарно-эпидемиологическая информация;
2) коммерческая тайна;
3) персональные данные;
4) сведения о мерах безопасности в отношении судьи и участников уголовного процесса.

73. Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации, — это;
1) секретная информация;
2) государственная тайна;
3) конфиденциальная информация;
4) совершенно секретная информация;
5) межгосударственная тайна.

74. Какой гриф секретности в соответствии с постановлением Правительства РФ от 4 сентября 1995 г. № 870 присваивается информации, распространение которой может нанести ущерб интересам министерства (федеральной службы) или отрасли экономики Российской Федерации?
1) секретная информация;
2) строго конфиденциальная информация;

3) совершенно секретная информация;
4) конфиденциальная информация;
5) информация особой важности.

75. 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.

76. Какую информацию относят к конфиденциальной (*выберите несколько вариантов ответа*)?
1) коммерческую тайну;
2) персональные данные;
3) государственную тайну;
4) тайну переписки;
5) ведомственную тайну;
6) тайну переговоров.

77. Как различается информация, относящаяся к разным степеням секретности?
1) временем получения данной информации;
2) степенью тяжести ущерба, наносимого утечкой данной информации;
3) объемом сведений;
4) количеством средств, затрачиваемых на ее получение потенциальным злоумышленником;
5) вычислительной мощностью, требующейся для ее декодирования.

78. Кто имеет право засекречивать информацию (*выберите несколько вариантов ответа*)?
1) органы власти;
2) должностные лица;
3) органы управления;
4) любой гражданин Российской Федерации;
5) Правительство РФ.

79. Сведения, не подлежащие засекречиванию (*выберите несколько вариантов ответа*):
1) о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

2) о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию войск, об их боеспособности и мобилизационной готовности, о создании и использовании мобилизационных ресурсов;

3) о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

4) научно-исследовательских, опытно-конструкторских и проектных работах, технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность Российской Федерации;

5) о методах и средствах защиты секретной информации;

6) о состоянии здоровья высших должностных лиц Российской Федерации;

7) о фактах нарушения законности органами государственной власти и их должностными лицами.

80. На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные… (*выберите несколько вариантов ответа*)

1) о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данных учреждении и организации перечня сведений, подлежащих засекречиванию;

2) гриф секретности информации;

3) об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;

4) о регистрационном номере;

5) об инвентарном номере;

6) список должностных лиц, допущенных к ознакомлению с содержащимися в этом носителе сведениями;

7) о дате или условии рассекречивания сведений либо о событии, после наступления которого сведения будут рассекречены.

81. Основанием рассекречивания сведений, составляющих государственную тайну, не является:

1) изменение срока засекречивания;

2) взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими государственную тайну;

3) истечение установленного срока засекречивания;

4) изменение объективных обстоятельств.

82. Целью защиты информации не является:

1) обеспечение использования информации;

2) предотвращение хищения, утечки, искажения, утраты и подделки информации;

3) предотвращение несанкционированных действий по уничтожению, модификации, копированию и блокированию информации;

4) реализация права на государственную тайну и конфиденциальную информацию.

83. Степенью секретности информации не является:

1) ограниченность в доступе;

2) особая важность;

3) совершенно секретно;

4) секретно.

84. Каким требованиям отвечает информация, отнесенная к коммерческой тайне (*выберите несколько вариантов ответа*)?

1) имеет действительную или потенциальную ценность в силу ее неизвестности третьим лицам;

2) ее утечка может нанести ущерб безопасности Российской Федерации;

3) не подпадает под перечень сведений, доступ к которым не может быть ограничен, и перечень сведений, отнесенных к государственной тайне;

4) ее цена не должна превышать 16 минимальных размеров оплаты труда (МРОТ);

5) к ней нет свободного доступа на законном основании;

6) ее ценность со временем не меняется;

7) обладатель принимает меры по охране ее конфиденциальности.

85. Что относится к основным объектам банковской тайны (*выберите несколько вариантов ответа*)?

1) тайна банковского счета;

2) тайна банковской деятельности;

3) тайна операций по банковскому счету;

4) тайна банковской структуры;

5) тайна банковской политики;

6) тайна частной жизни клиента или корреспондента.

86. Какие сведения не могут быть отнесены к служебной тайне (*выберите несколько вариантов ответа*)?

1) сведения, содержащие коммерческую тайну;

2) сведения, содержащие профессиональную тайну;

3) сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, необходимые для обеспечения безопасного существования граждан Российской Федерации;

4) описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;

5) сведения об исполнении бюджета и использовании других государственных ресурсов;

6) сведения, содержащие тайну личной жизни граждан Российской Федерации.

87. 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.

88. Гриф секретности или конфиденциальности на носителе информации представляет собой …

1) обязательный атрибут носителя любой информации;
2) условный знак, указывающий на то, что на носителе присутствует информация, содержащая государственную тайну;
3) условный знак полезности содержащейся на носителе информации;
4) условный знак, указывающий на то, что на носителе присутствует информация, содержащая коммерческую тайну;
5) условное обозначение того, что носитель по своей физической структуре ненадежен, и частое его использование может привести к потере всех данных, содержащихся на нем.

89. Какой гриф секретности, в соответствии с постановлением Правительства РФ № 870 от 4 сентября 1995 г. присваивается информации, распространение которой может нанести ущерб интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности?

1) секретная информация;
2) строго конфиденциальная информация;
3) совершенно секретная информация;
4) конфиденциальная информация;
5) информация особой важности.

90. Что из нижеперечисленного можно отнести к источникам конфиденциальной информации (*выберите несколько вариантов ответа*)?

1) различные документы;
2) слухи;
3) людей;
4) публикации;
5) художественную литературу;
6) технические носители информации;
7) технические средства обработки информации;

8) указы Президента РФ;
9) выпускаемую продукцию;
10) производственные и промышленные отходы.

91. В каком случае нельзя засекречивать информацию как имеющую статус государственной тайны (*выберите несколько вариантов ответа*)?
1) если ее утечка не влечет ущерба национальной безопасности страны;
2) если эта информация принадлежит определенному предприятию;
3) если сокрытие информации будет нарушать конституционные и законодательные права граждан;
4) если сокрытие данной информации не нанесет ущерб окружающей среде;
5) если ее утечка нанесет ущерб безопасности Российской Федерации.

92. Совокупность организационно-правовых мер, регламентированных законами и другими нормативными актами, по введению ограничений на распространение и использование информации в интересах ее собственника (владельца) — это…
1) ограничение информации;
2) блокировка информации;
3) засекречивание информации;
4) изоляция информации;
5) кодирование информации.

93. Приведите основные принципы засекречивания информации (*выберите несколько вариантов ответа*):
1) надежность засекречивания;
2) законность засекречивания;
3) внезапность засекречивания;
4) обоснованность засекречивания;
5) оперативность засекречивания;
6) своевременность засекречивания.

94. Органы государственной власти и должностные лица, на которых возложено отнесение сведений к государственной тайне и их защита (*выберите несколько вариантов ответа*):
1) Государственная Дума Федерального Собрания РФ;
2) Президент РФ;
3) Министр внутренних дел РФ;
4) Правительство РФ;
5) органы судебной власти.

95. Должностные лица, принявшие решения о засекречивании сведений либо о включении их в этих целях в носители сведений, составляющих госу-

дарственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от … (*выберите несколько вариантов ответа*)

1) причиненного обществу, государству и гражданам материального и морального ущерба;
2) причиненного ущерба, нанесенного экономике государства;
3) причиненного ущерба, нанесенного международному имиджу Российской Федерации;
4) причиненного ущерба инфраструктуре по обеспечению обороноспособности и безопасности Российской Федерации;
5) причиненного личности, обществу и государству материального ущерба.

96. Какая информация не может быть отнесена к коммерческой тайне (*выберите несколько вариантов ответа*)?

1) содержащая технологию производства;
2) содержащаяся в учредительных документах;
3) содержащая персональные данные граждан Российской Федерации;
4) содержащая сведения о задолженностях работодателей по выплате заработной платы и другим выплатам социального характера;
5) содержащая сведения о численности и кадровом составе работающих;
6) содержащая маркетинговую политику руководителя.

97. Что относится к основным объектам профессиональной тайны (*выберите несколько вариантов ответа*)?

1) тайна страхования;
2) тайна связи;
3) тайна контрагента;
4) тайна проповеди;
5) нотариальная тайна;
6) тайна покупателя.

98. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленном федеральными законами случаях, — это …

1) опознавательные признаки;
2) персональные данные;
3) открытые сведения;
4) биометрический паспорт;
5) база данных.

99. Что представляют собой угроза?

1) нестабильное состояние мировой экономики;

2) совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию информационных технологий или его собственнику;

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.

100. Перечислите все 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.

101. Источниками угрозы информационной безопасности являются… (*выберите несколько вариантов ответа*)

1) потенциальные злоумышленники;
2) компрометирующие ситуации;
3) благоприятные факторы;
4) непредсказуемые последствия;
5) сложные обстоятельства.

102. К активным угрозам относятся:

1) попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания;
2) копирование информации;
3) разрушение или радиоэлектронное подавление линий связи, вывод из строя компьютера или операционной системы;
4) анализ графика.

103. Какие угрозы безопасности информации являются преднамеренными?

1) некомпетентное использование средств защиты;
2) поджог;
3) неумышленное повреждение каналов связи;
4) ошибки в программном обеспечении.

104. Что не относится к угрозам информационной безопасности?

1) классификация уязвимостей;
2) сбои и отказы оборудования (технических средств);
3) преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов);
4) хищение производственных отходов.

105. К посторонним лицам нарушителей информационной безопасности относятся:
1) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
2) персонал, обслуживающий технические средства;
3) технический персонал, обслуживающий здание;
4) пользователи;
5) сотрудники службы безопасности;
6) представители конкурирующих организаций;
7) лица, нарушившие пропускной режим.

106. Искусственные угрозы безопасности информации вызваны:
1) деятельностью человека;
2) ошибками при проектировании компьютерных систем, ее элементов или разработке программного обеспечения;
3) воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
4) корыстными устремлениями злоумышленников;
5) ошибками при действиях персонала.

107. К внутренним нарушителям информационной безопасности относится (*выберите несколько вариантов ответа*):
1) клиенты;
2) пользователи системы;
3) посетители;
4) любые лица, находящиеся внутри контролируемой территории;
5) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
6) персонал, обслуживающий технические средства;
7) сотрудники отделов разработки и сопровождения программного обеспечения;
8) технический персонал, обслуживающий здание.

108. Что можно отнести к угрозам случайных воздействий на источник 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.

109. 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.

110. В каком случае возникает реальный ущерб?
1) при появлении угрозы;
2) при уничтожении уязвимости;
3) при реализации угрозы;
4) при организации защиты конфиденциальной информации;
5) при оценке вреда, наносимого той или иной угрозой.

111. Как называется попытка реализации угрозы безопасности информации?
1) нападение;
2) нарушение статичности;
3) атака;
4) обвал.

112. Какие угрозы безопасности информации являются преднамеренными?
1) ошибки персонала;
2) не авторизованный доступ;
3) открытие электронного письма, содержащего вирус;
4) любопытство.

113. К пассивным угрозам не относятся;
1) попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания;
2) копирование информации;
3) разрушение или радиоэлектронное подавление линий связи, вывод из строя компьютера или операционной системы;
4) анализ графика сети.

114. Какие угрозы безопасности информации являются непреднамеренными?
1) внедрение агентов в число персонала системы;

2) поджог;
3) умышленное повреждение каналов связи;
4) ошибки в программном обеспечении.

115. Что не относится к угрозам информационной безопасности?
1) классификация угроз;
2) вскрытие шифров криптозащиты информации;
3) нелегальное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
4) ввод ошибочных данных.

116. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
1) сотрудники;
2) хакеры;
3) атакующие;
4) контрагенты (лица, работающие по договору);
5) хактевисты;
6) кибершпионы.

117. Естественные угрозы безопасности информации вызваны…
1) деятельностью человека;
2) ошибками при проектировании компьютерной системы, ее элементов или разработке программного обеспечения;
3) воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;
4) корыстными устремлениями злоумышленников;
5) ошибками при действиях персонала.

118. Воздействия, которые создаются злоумышленниками, являются…
1) точечными;
2) разрушительными;
3) преднамеренными;
4) спровоцированными;
5) губительными.

119. Угрозы, приводящие к несанкционированному распространению носителя с защищаемой информацией к злоумышленнику, называются…
1) угрозами модификации информации;
2) угрозами утечки информации;
3) угрозами разрушения информации;
4) угрозами проявления стихии;
5) угрозами действия помех.

120. В каком случае возникает потенциальный ущерб?

1) при реализации угрозы;
2) при появлении угрозы;
3) при уничтожении уязвимости;
4) при организации защиты конфиденциальной информации;
5) при оценке вреда, наносимого той или иной угрозой.

121. В каком случае реализуется угроза утечки информации?

1) происходит утеря источника информации;
2) происходит частичная модификация защищаемой информации;
3) защищаемая информация полностью уничтожена;
4) информация попадает к злоумышленнику;
5) защищаемая информация теряет актуальность.

122. Из нижеперечисленного выделите возможные способы получения информации (выберите несколько вариантов ответа):

1) изучение порядка сдачи налоговой отчетности предприятия;
2) изучение продукции предприятия;
3) ознакомление с правилами пожарной безопасности предприятия;
4) использование сведений, распространяемых служащими предприятия;
5) непосредственное наблюдение, осуществляемое скрытно.

123. Перечислите способы несанкционированного доступа к конфиденциальной информации (выберите несколько вариантов ответа):

1) авторизованный вход в систему;
2) хищение;
3) перехват;
4) актуализация базы данных;
5) копирование.

124. Перехват, который осуществляется путем использования оптической техники, называется…

1) активный перехват;
2) пассивный перехват;
3) аудиоперехват;
4) видеоперехват;
5) просмотр мусора.

125. Что понимается под «разглашением» конфиденциальной информации?

1) умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним;
2) передача сведений конфиденциального характера их обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены данным договором;

3) бесконтрольный выход конфиденциальной 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.

126. Что относится к формальным каналам распространения информации (*выберите несколько вариантов ответа*)?

1) деловые встречи;
2) совещания;
3) личная переписка;
4) интернет;
5) телевидение.

127. «Утечка» конфиденциальной информации — это…

1) противоправное преднамеренное овладение конфиденциальной информацией;

2) умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним;

3) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена;

4) ознакомление определенных лиц с конфиденциальной информацией с согласия ее обладателя.

128. 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.

129. Перечислите основные виды каналов утечки информации (*выберите несколько вариантов ответа*):

1) визуально-оптические;
2) магнитоконтактные;
3) акустические;
4) электромеханические;
5) электромагнитные;
6) материально-вещественные;
7) оптико-электронные.

130. Что подразумевается под «несанкционированным доступом» к конфиденциальной информации?

1) умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним;

2) противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам;

3) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена;

4) ознакомление определенных лиц с конфиденциальной информацией с согласия ее обладателя.

131. Как называется процесс приема и анализа акустических сигналов?

1) наблюдение;
2) перехват;
3) хищение;
4) фиксация;
5) подслушивание.

132. Как называется процесс приема и анализа радио- и электрических сигналов?

1) демодуляция;
2) консервация;
3) перехват;
4) преобразование;
5) регистрация.

133. Как называются сигналы, содержащие секретную или конфиденциальную информацию, которые могут быть перехвачены злоумышленником и с которых может быть снята данная информация?

1) модулированные сигналы;
2) дискретные сигналы;
3) полезные сигналы;
4) опасные сигналы;
5) секретные сигналы.

134. Активный перехват информации — это перехват, который…

1) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

2) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

3) неправомерно использует технологические отходы информационного процесса;

4) осуществляется путем использования оптической техники;

5) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

135. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций, называется…

1) активный перехват;
2) пассивный перехват;
3) аудиоперехват;
4) видеоперехват;
5) просмотр мусора.

136. 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.

137. Что относится к неформальным каналам распространения информации (*выберите несколько вариантов ответа*)?

1) обмен официальными деловыми документами;
2) конференции;
3) выставки;
4) газеты;
5) средства передачи официальной информации.

138. Посредством чего осуществляется утечка конфиденциальной информации?

1) посредством активных соединений;
2) посредством организационных мероприятий;
3) посредством формальных коммуникаций;
4) посредством различных технических каналов;
5) посредством неформальных коммуникаций.

139. Что подразумевается под каналом утечки информации?

1) физический путь от источника информации к ее получателю;
2) физический путь от источника конфиденциальной информации к злоумышленнику;
3) материальные объекты, в том числе физические поля, в которых конфиденциальная информация находит свое отображение;
4) часть пространства, в которой перемещается носитель информации.

140. Перечислите основные способы несанкционированного доступа (*выберите несколько вариантов ответа*);

1) уничтожение носителей информации;
2) подслушивание телефонных переговоров;
3) порча средств вычислительной техники;
4) кража документов;
5) проникновение в компьютер.

141. Что из нижеперечисленного относится к условиям, способствующим неправомерному овладению конфиденциальной информацией (*выберите несколько вариантов ответа*)?

1) создание в организации должностной инструкции о порядке работы с конфиденциальной информацией;
2) излишняя болтливость сотрудников;
3) жесткий контроль обеспечения информационной безопасности в организации;
4) традиционный обмен производственным опытом;
5) бесконтрольное использование информационных систем;
6) случайный подбор кадров;
7) введение в организации режима коммерческой тайны.

142. 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) регистрации.

143. Как называется технический канал утечки информации, организованный злоумышленником установкой на объекте закладного устройства?

1) случайным;
2) потенциальным;
3) спонтанным;
4) опасным;
5) организованным.

144. Какие технические средства из нижеперечисленных создают опасные сигналы (*выберите несколько вариантов ответа*)?

1) электрические розетки;
2) средства телефонной проводной связи;
3) лампы накаливания;
4) средства электронной вычислительной техники;
5) видеоаппаратура.

145. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации, называется…

1) активный перехват;
2) пассивный перехват;
3) аудиоперехват;
4) видеоперехват;
5) просмотр мусора.

146. Способ несанкционированного доступа к источникам конфиденциальной информации называется — это:

1) потенциальные или реальные действия, приводящие к моральному или материальному ущербу;
2) спонтанное не зависящее от воли людей обстоятельство, возникающее 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.

147. Какая информация добывается посредством подслушивания (*выберите несколько вариантов ответа*)?

1) информация об излучениях, модулированных звуковой волной;
2) информация о координатах источника звука;
3) речевая информация;
4) демаскирующие признаки сигналов различных источников звуков;
5) информация о направлении звуковой волны.

148. Назовите основной недостаток визуально-оптического наблюдения в видимом и инфракрасных диапазонах;

1) невозможность сохранения изображения для последующего анализа специалистами;
2) невозможность распознавания объекта в темное время суток;
3) невозможность наблюдения скрытых объектов через отверстия или щели;
4) недопустимо малое возможное расстояние до объекта.

149. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации — …

1) защищаемая информация;
2) конфиденциальная информация;
3) секретная информация;
4) информация ограниченного доступа.

150. 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 — …

1) объект информатизации;
2) информационная система;
3) комплексная защита объектов информатизации;
4) аттестованная информационная система.

Алфавитный указатель терминов

Рекомендуемые источники

1. 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.
2. Астахова, А.В. Информационные системы в экономике и защита информации на предприятиях — участниках ВЭД : учеб. пособие / А. В. Астахова. — СПб. : Троицкий мост, 2014..
3. Чеботарева, А. А. Информационное право : учеб. пособие / А. А. Чеботарева. — М. : Юридический институт МИИТа, 2014.
4. Груздева, Л. М. Информационные технологии в профессиональной деятельности : метод. указания по выполнению практических работ / Л. М. Груздева, С. Л. Лобачев, А. А. Чеботарева. — М. : Юридический институт МИИТа, 2015.
5. Информационные технологии в юридической деятельности / под ред. В. Д. Элькина. — М. : Издательство Юрайт, 2013.
6. Информационные технологии в юриспруденции : учеб. пособие / под ред. С. Я. Казанцев. — 2-е изд., перераб. и доп. — М. : Академия, 2012.
7. 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://www.inside-zi.ru — сайт журнала «Защита информации»
2. http://www.inside-zi.ru — сайт журнала «Инсайд»
3. http://www.xakep.ru — сайт журнала «Хакер»
4. http://garant.ru — Гарант: законодательство РФ
5. http://www.consultant.ru — Консультант +: законодательство РФ
6. http://fstec.ru/ — официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России)
7. http://www.scrf.gov.ru/ — официальный сайт Совета безопасности Российской Федерации
8. http://fsb.ru — официальный сайт Федеральной службы безопасности Российской Федерации (ФСБ России)