МИНИТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОСТОВСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ
УНИВЕРСИТЕТ (РИНХ)»

«УТВЕРЖДАЮ»
Ректор ФГБОУ ВО «РГЭУ (РИНХ)»
д.э.н., профессор
_____ Е.Н.Макаренко

«__09__» ___октября___ 2023 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ И ПРАВИЛА ПРОВЕДЕНИЯ В ФГБОУ ВО «РГЭУ (РИНХ)» НА 2024/2025 УЧЕБНЫЙ ГОД

Ростов-на-Дону

2023 год

Настоящая программа предназначена для лиц, поступающих в магистратуру по направлению подготовки 10.04.01 «Информационная безопасность».

Программа содержит темы, включённые в междисциплинарный экзамен по направлению и собеседование, рекомендуемую литературу для подготовки к вступительным испытаниям, а также примерный вариант теста проверки знаний поступающих на данную магистерскую программу.

Контактная информация:
344002, Россия, г. Ростов-на-Дону, ул. Б. Садовая, 69
www.rsue.ru

Приемная комиссия:
г. Ростов-на-Дону, ул. Б. Садовая, 69, каб. 108, 110, тел. (863) 237-02-60, 240-55-48

Кафедра «Информационных технологий и защиты информации», ауд. 306а,
тел. (863) 240-21-23

СОДЕРЖАНИЕ

Требования к вступительному испытанию

Цель вступительного испытания заключается в комплексном определении практической и теоретической подготовленности поступающего в магистратуру бакалавра (специалиста) и соответствия его знаний, умений и навыков требованиям обучения в магистратуре по направлению подготовки. Испытания носят дисциплинарный характер и включают темы базовых дисциплин направления бакалавриата (специалитета) «Информационная безопасность».

К сдаче вступительного экзамена допускаются лица, имеющие законченное высшее профессиональное образование со степенями «бакалавр», «специалист».

Вступительные испытания в магистратуру проводятся в форме письменного тестирования.

Основные задачи тестирования:

- проверить уровень знаний поступающего;
- определить склонности к научно-исследовательской деятельности;
- определить уровень научных интересов;
- определить уровень научно-технической эрудиции поступающего.

Ориентировочная продолжительность процедуры вступительных испытаний – 60 минут.

В основу программы вступительных испытаний положены квалификационные требования, предъявляемые к бакалаврам (специалистам) по направлению «Информационная безопасность».

Каждый экзаменационный билет состоит из вопросов тестового типа. Результаты вступительного испытания оцениваются по 100 бальной шкале. Минимальный проходной балл 30.

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ

РАЗДЕЛ 1. ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Законодательно – правовые и организационные основы обеспечения защиты информации. Структура законодательства РФ в области защиты информации. Источники конфиденциальной информации. Угрозы безопасности информации. Роль и место организационно-правовой защиты информации в структуре системы защиты информации. Организационные каналы утечки конфиденциальной информации. Организация защиты информации на предприятии. Политика безопасности предприятия. Информация как объект правового регулирования. Виды информации, защищаемой законодательством РФ. Государственная тайна как особый вид защищаемой информации. Принципы, механизм и процедура отнесения сведений к государственной тайне. Порядок засекречивания сведений, документов и продукции. Порядок рассекречивания сведений, документов и продукции. Система контроля за состоянием защиты государственной тайны. Органы защиты государственной тайны и их полномочия. Юридическая ответственность за нарушения правового режима защиты государственной тайны. Объекты защиты. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну. Обязанности персонала организации по сохранению коммерческой тайны. Состав и структура системы безопасности предприятия. Правовые основы деятельности службы безопасности. Организационное обеспечение информационной безопасности при проведении закрытых мероприятий. Организация информационно – аналитической работы.

РАЗДЕЛ 2. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Сущность и понятие информационной безопасности. Место информационной безопасности в системе национальной безопасности. Национальные интересы РФ в информационной сфере. Сущность и понятие информационной безопасности. Виды угроз информационной безопасности РФ. Источники угроз информационной безопасности РФ. Основные задачи по обеспечению информационной безопасности РФ. Обеспечение информационной безопасности РФ в информационных и телекоммуникационных системах. Система обеспечения информационной безопасности РФ. Основные свойства информации. Виды представления информации. Система защиты информации. Виды угроз безопасности информации. Органы добывания информации. Источники и носители информации. Источники функциональных сигналов. Источники ПЭМИН. Классификация

акустоэлектрических преобразователей. Излучатели низкочастотных сигналов. Излучатели высокочастотных сигналов. Паразитные связи и наводки. Формы ЗИ. Объекты защиты информации. Понятия: ОТСС, ВТСС и их состав; ВП(ЗП); КЗ; зона 1; зона 2. Характеристика ТКУИ. Причины возникновения ТКУИ. Классификация ТКУИ. Телекоммуникационные каналы утечки информации. Акустические каналы утечки информации. Организационные мероприятия по защите информации от утечки по техническим каналам. Технические мероприятия по защите информации от утечки по техническим каналам.

РАЗДЕЛ 3. ЛИЦЕНЗИРОВАНИЕ, СЕРТИФИКАЦИЯ, АТТЕСТАЦИЯ.

Структура системы государственного лицензирования. Порядок проведения лицензирования. Лицензирование в области защиты информации. Перечень видов деятельности в области защиты информации, подлежащих лицензированию. Порядок оформления запроса на лицензирование по видам деятельности. Государственная аттестация руководителей предприятий. Основные лицензионные требования и условия. Структура системы сертификации в области защиты информации. Порядок проведения аттестации и контроля объектов информатизации.

РАЗДЕЛ 4. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

История развития криптографии. Понятие о традиционных методах шифрования. Классические методы шифрования. Стандарт шифрования данных DES. Управление ключами в симметричных криптосистемах. Криптосистемы с открытым ключом. Основные понятия теории чисел. Алгоритм шифрования RSA. Управление ключами в асимметричных криптосистемах. Хэш-функции. Электронная цифровая подпись. Протоколы аутентификации. Имитостойкость и помехоустойчивость криптосистем. Методы генерации случайных чисел. Криптографические шифраторы. Особенности программно-аппаратной реализации криптографической защиты компьютерных сетей и сетей связи.

РАЗДЕЛ 5. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕТЕЙ И ТЕЛЕКОММУНИКАЦИЙ

Топологии физических сетей. Защищенные протоколы и уровни сетевого взаимодействия. Иерархия защищенных протоколов сетевого взаимодействия. Эталонная модель сетевого взаимодействия OSI. Протоколы и стандарты локальных сетей. Технология Ethtrnet. Технологии Fast Ethernet. Типы линий связи. Методы коммутации. Коммутация каналов. Коммутация пакетов. Коммутация сообщений. Структура глобальных сетей.

Компьютерные глобальные сети с коммутацией пакетов. Принципы коммутации пакетов с использованием техники виртуальных каналов. Сети X.25. Сети Frame Relay.

ПРИМЕР ТЕСТОВОГО ЗАДАНИЯ

1. Носители защищаемой информации (*выберите все правильные ответы*):

1. элементарные частицы
2. линии связи
3. электромагнитные поля
4. акустические поля

2. Контролируемая зона:

1. зона, в которой исключено появление посторонних лиц и транспортных средств

2. зона, в которой исключено появление лиц и транспортных средств, не имеющих постоянных или временных пропусков.

3. зона, в которой исключено появление лиц и транспортных средств, не имеющих допуска к защищаемой информации

3. Зона 2 – пространство вокруг ОТСС:

1.на границе и за пределами которого напряженность электромагнитного поля информативного сигнала не превышает нормированного значения.

2.за пределами которого напряженность электромагнитного поля информативного сигнала не превышает нормированного значения.

3. в пределах которого напряженность электромагнитного поля информативного сигнала не превышает нормированного значения.

4. Зона 1 – пространство вокруг ОТСС:

1. на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в ВТСС, а также в посторонних проводах и линиях передачи информации, не превышает нормированного значения.

2. за пределами которого уровень наведенного от ОТСС информативного сигнала в ВТСС, а также в посторонних проводах и линиях передачи информации, имеющих выход за пределы КЗ, не превышает нормированного значения.

3.на границе и за пределами которого уровень наведенного от ОТСС информативного сигнала в ВТСС, а также в посторонних проводах и линиях передачи информации, имеющих выход за пределы КЗ, не превышает нормированного значения.

5. Что входит в технический канал утечки информации? (*выберите все правильные ответы):*

1. Физическая среда распространения информационного сигнала
2. Объект разведки
3. Субъект разведки
4. Техническое средство разведки

6. Технические каналы утечки информации, обрабатываемой ТСОИ (*выберите все правильные ответы*):

1.электрический
2.электромагнитный
3.индукционный
4.виброакустический
5.параметрический

7. Источники ПЭМИН (*выберите все правильные ответы*):

1. Вычислительная техника
2. Вибрация оконных стёкол
3. Монитор видеоконтроля
4. Проводка электропитания

8. Технические каналы утечки акустической речевой информации (*выберите все правильные ответы*):

1.оптико-электронный
2.электромагнитный
3.индукционный
4.виброакустический
5.электрический

9. Цель аттестации объектов информатизации:

1. обнаружить технические каналы утечки информации
2. выявить персонал, способный распространять защищаемую информацию.
3. выявить средства негласного съема информации.
4. подтвердить, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

10. Обязательной аттестации подлежат объекты информатизации (*выберите все правильные ответы*):

1.предназначенные для обработки информации, составляющей государственную тайну

2.ведения конфиденциальных переговоров

3.управления экологически опасными объектами

11. К ОТСС относятся (*выберите все правильные ответы*):

1.средства изготовления и размножения документов

2.системы охранной сигнализации

3.системы пожарной сигнализации

4.средства и системы открытой телефонной связи;

5.аппаратура звукоусиления в выделенных помещениях

12. К ОТСС относятся технические средства, обрабатывающие:

1.экономическую информацию

2.техническую информацию

3.информацию ограниченного доступа

4.информацию о поставщиках

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

1. Организационное
2. Организационно-техническое
3. Техническо-организационное
4. Техническое

14. В каком документе изложены основные составляющие национальных интересов РФ в информационной сфере:

1. Конституция РФ.

2. Указ Президента РФ №537 «О Стратегии национальной безопасности РФ до 2020 года»

3. №149-ФЗ «Об информации, информационных технологиях и о защите информации»

4. «Доктрина информационной безопасности РФ». №646 от 5.12.2016 г.

5. «Стратегия развития информационного общества в РФ». № Пр-212, 2008 г.

15. В каком законе определен правовой режим информатизации, правила, процедуры и распределение ответственности в области защиты информации в системах ее обработки, установлен порядок правовой защиты и гарантии реализации прав и ответственности субъектов информационных взаимоотношений:

1. Федеральный закон от 28.12.2010 № 390-ФЗ "О безопасности".

2. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных

технологиях и о защите информации".

3. Федеральный закон от 27.12.2002 № 184-ФЗ "О техническом регулировании".
4. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных".

16. Все нормативно-правовые акты в РФ не могут противоречить…:

1. Уголовному кодексу РФ
2. Административному кодексу РФ
3. Конституции РФ
4. Законам, утвержденным ГД РФ
5. Указам Президента РФ

17. Исполнение Закона «О персональных данных» организует:

1. Государственная Дума РФ
2. Президент РФ
3. Правительство РФ
4. ФСТЭК совместно с ФСБ

18. Свойства информации как объекта защиты (*выберите все правильные ответы*):

1. Конфиденциальность
2. Ознакомление.
3. Доступность
4. Модификация.
5. Достоверность
6. Уничтожение.
7. Целостность
8. Блокирование.

19. Что такое разглашение информации (*выберите все правильные ответы*):

1. Умышленные действия приведшие к ознакомлению сведениями лиц, не допущенных к ним.

2. Неосторожные действия приведшие к ознакомлению сведениями лиц, не допущенных к ним.

3. Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц

4. Противоправное преднамеренное овладение конфиденциальной информацией

20. Перечень сведений конфиденциального характера по видам тайны (*выберите все правильные ответы*):

1. служебные сведения

2. сведения об организационной структуре организации

3. сведения, связанные с коммерческой деятельности

4. сведения, распространение которых нанесут ущерб интересам министерства (ведомства) или отрасли экономики РФ.

5. сведения о содержании Устава предприятия

21. Лицензирование деятельности по технической защите конфиденциальной информации осуществляют:

1.ФСБ РФ

2.ФСТЭК

3 СВР РФ

4. МО РФ

22. Допуск предприятий к проведению работ, связанных с использованием сведений, составляющих ГТ, осуществляют:

1.ФСБ РФ

2.ФСТЭК

3 СВР РФ

1. МО РФ

23. С какой целью в России защищаются персональные данные?

1. для обеспечения условий вхождения России в ВТО
2. для обеспечения прав на неприкосновенность частной жизни, личную и семейную тайну
3. для защиты государственной тайны
4. для обеспечения интересов бизнеса

24. Какие из перечисленных сведений не входят в состав персональных данных?

1. год рождения
2. место рождения
3. семейное положение
4. сведения о средствах обеспечения безопасности персональных данных
5. социальное положение
6. национальность
7. состояние здоровья
8. судимость

25. Что предписано сделать с персональными данными после достижения целей, с которыми они обрабатывались? (*выберите все правильные ответы*):

1. хранить в течение установленного срока

2. передать в уполномоченный орган по защите прав субъектов персональных данных

3. уничтожить

4. опубликовать

5. блокировать

26. Принципы обработки персональных данных (*выберите все правильные ответы*):

1. объединение различных баз данных

2. определение целей обработки персональных данных

3. содержание и объем обрабатываемых персональных данных соответствуют целям обработки

4. персональные данные хранятся в течение года после достижения цели обработки

27. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (*выберите все правильные ответы*):

1. цели и применяемые оператором способы обработки персональных данных;

2. сведения о работниках оператора, которые имеют доступ к персональным данным

3. сроки обработки персональных данных

4. наименование и место нахождения оператора

28. Оператор вправе поручить обработку персональных данных другому лицу:

1. Да

2. Нет

29. Оператор обязан предоставить субъекту персональных данных следующую информацию (персональные данные получены не от субъекта персональных данных) (*выберите все правильные ответы*):

1. цель обработки персональных данных и ее правовое основание

2. сведения о работниках оператора, которые имеют доступ к персональным данным

3. сроки обработки персональных данных

4. источник получения персональных данных

5. информацию о предполагаемой трансграничной передаче данных

30. Типовая форма документов при обработке ПДн, осуществляемой без использования средств автоматизации, должна содержать сведения о (*выберите все правильные ответы*):

1. источнике получения ПДн

2. согласии субъекта ПДн

3. цели обработки ПДн

4. сведения о работниках оператора, которые имеют доступ к ПДн

31. Для ИСПДн актуальны угрозы, связанные с наличием недекларированных возможностей в прикладном программном обеспечении. Это угрозы:

1. 1-го типа
2. 2-го типа
3. 3-го типа

32. При обработке персональных данных, касающиеся политических взглядов, она относится к ИСПДн, обрабатывающей:

1. биометрические персональные данные
2. общедоступные персональные данные
3. специальные категории персональных данных
4. иные категории персональных данных

33. Для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает паспортные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора. Для нее устанавливается уровень защищенности:

1. 1
2. 2
3. 3
4. 4
5. 5

34. Для обеспечения какого уровня защищенности персональных данных при их обработке в ИСПДн необходимо, чтобы было назначено должностное лицо, ответственное за обеспечение безопасности персональных данных в ИСПДн? (*выберите все правильные ответы*):

1. 1
2. 2
3. 3
4. 4
5. 5

35. Контроль за выполнением требований к защите персональных данных в ИСПДн проводится:

1. не реже 1 раза в течение года

2. не реже 1 раза в 2 года

3. не реже 1 раза в 3 года

4. ничего из вышеперечисленного

36. После утверждения политики в отношении обработки персональных данных, документы ее определяющие, подлежат опубликованию на официальном сайте государственного или муниципального органа в течение:

1. 5 дней

2. 10 дней

3. 20 дней

4. месяца

37. Какой этап НЕ проводится при проведении классификации ИСПДн?

1. формирование и утверждение комиссии

2. сбор исходных данных по ИСПДн

3. анализ исходных данных по ИСПДн

4. присвоение ИСПДн соответствующего класса

5 документальное оформление результатов классификации

38. К какому классу защищенности относится локальная вычислительная сеть муниципального органа одного из районов Ростовской области для которого определены уровни ущерба: конфиденциальность – средний; целостность – средний; доступность – низкий:

1. К1

2. К2

3. К3

4. К4

39. При проведении классификации ИСПДн учитываются исходные данные (*выберите все правильные ответы*):

1. характеристики безопасности ПДн

2. режим обработки ПДн

3. тип угрозы ИСПДн

4. согласие субъекта ПДн

5. класс ИСПДн

40. Для определения актуальных угроз безопасности персональных данных в ИСПДн учитываются (*выберите все правильные ответы*):

1. вероятность реализации угрозы

2. вид технического канала утечки информации

3. уровень опасности угрозы

4. угрозы безопасности ПДн, передаваемых по сетям связи

5. негативные последствия для субъектов ПДн

41. К какой категории внутренних потенциальных нарушителей относится системный администратор ИСПДн?

1. 3

2. 4

3. 5

4. 6

5. 7

42. К типовым угрозам, реализуемым на сетевом и транспортном уровнях, относятся (*выберите все правильные ответы*):

1. угроза, направленная на подмену доверенного объекта

2. угроза, направленная на создание в сети ложного маршрута

3. угроза, направленная на изменение полномочий доверенного объекта

4. угрозы, направленные на создание ложного объекта с использованием недостатков алгоритмов удаленного поиска

43. К какому уровню защищенности необходимо отнести ИСПДн, для которой актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора:

1. 1

2. 2

3. 3

4. 4

5. 5

44. В каком документе приведен перечень мер, направленных на обеспечение выполнения обязанностей операторами, являющимися государственными или муниципальными органами, по защите персональных данных:

1. Федеральный закон от 27.07.2006 № 152-ФЗ.

2. Постановление Правительства РФ от 01.11.2012 №1119.

3. Постановление Правительства РФ от 21.03.2012 №211.

4. Постановление Правительства РФ от 15.09.2008 №687.

5. Приказ ФСТЭК от 18.02.2013 №21.

45. В каком документе приведен состав и содержание организационных и технических мер, направленных на обеспечение безопасности персональных данных при их обработке в ИСПДн:

1. Федеральный закон от 27.07.2006 № 152-ФЗ.
2. Постановление Правительства РФ от 01.11.2012 №1119.
3. Постановление Правительства РФ от 21.03.2012 №211.
4. Постановление Правительства РФ от 15.09.2008 №687.
5. Приказ ФСТЭК от 18.02.2013 №21.

46. К конфиденциальным документам можно отнести:

1.Учредительные документы, уставы

2. Документы, содержащие персональные данные

3.Документы, составляющие служебную тайну

47. Утрата конфиденциальной информации, обрабатываемой и хранимой в компьютере, чаще всего происходит по причине:

а) Отказов оборудования

б) Угроз от окружающей среды

в) Непреднамеренных ошибок лиц, обслуживающих систему обработки данных

г) Хакерских атак

д) Последствий ошибок проектирования и разработки системы обработки данных

СПИСОК ОСНОВНОЙ ЛИТЕРАТУРЫ

1. Мельников, В. П. Информационная безопасность / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Academia, 2018. - 336 с.

2. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие. - М.: Форум; Инфра-М, 2012.

3. Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации: Учебное пособие / В.С. Горбатов, СВ. Дворянкин, А.П. Дураковский, Р.С. Енгалычев [и др.], под общ. ред. Ю.Н. Лаврухина. - М: НИЯУ МИФИ, 2014.-560 с.

4. Гафнер, В. В. Информационная безопасность / В.В. Гафнер. - М.: Феникс, 2019. - 336 с.

5. Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям безопасности информации: Учебное пособие / А.А. Голяков, В.С. Горбатов, А.П. Дураковский, А.Е. Панин, М.С. Чистяков; под общ. ред. Ю.Н., Лаврухина. - М: НИЯУ МИФИ, 2014. - 208 с: ил.

6. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с.

7. Контроль защищенности речевой информации в помещениях. Аттестационные испытания выделенных помещений по требованиям безопасности информации: Учебное пособие / В.С. Горбатов, А.П. Дураковский, И.В. Куницын, А.Е. Панин, под общ. ред. Ю.Н. Лаврухина. - М: НИЯУ МИФИ, 2014. - 248 с: ил.

8. Партыка, Т.Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: ИНФРА-М, 2019. - 368 с.

9.Технические средства и методы защиты информации: Учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков; под ред. А.П. Зайцева и А.А. Шелупанова. - 7-е изд. испр. - М.: Горячая линия - Телеком, 2012.

10..Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / Ю.Ю. Коваленко. - М.: Горячая линия - Телеком, 2012.

11. Концептуальные основы создания и применения системы защиты объектов / В.А. Воронов, В.А. Тихонов. - М.: Горячая линия - Телеком, 2013.

12. Грибунин В.Г. Комплексная система защиты информации на предприятии: Учебное пособие. - М.: Академия, 2009.

13.Гришина Н.В. Комплексная система защиты информации на предприятии: Учебное пособие. - М: Форум, 2013.

14.Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г.
15.Безопасность глобальных сетевых технологий. - 2-е изд. / В.М. Зима, А.А. Молдовян, Н.А. Молдовян. - СПб.: БХВ-Петербург, 2014. - 368 с
16. Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. - М.: ИНФРА-М, 2019. - 304 с.
17. Крамаров, С.О. Криптографическая защита информации: Учебное пособие / С.О. Крамаров, Е.Н. Тищенко, С.В. Соколов и др. - М.: Риор, 2019. - 112 с.

СПИСОК ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

1. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации».
5. Указ Президента Российской Федерации от 17.03.2008 №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
6. Указ Президента Российской Федерации от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти. Утверждено постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233.
8. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации 05.12.2016 № 646.
9. Указ Президента Российской Федерации от 9.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».
10. Постановление Правительства Российской Федерации от 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности».
11. Постановление Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».
12. Постановление Правительства Российской Федерации от 26.06.1995 № 608 «О сертификации средств защиты информации».

13. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
14. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
15. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
16. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Госстандарт СССР, 1990.
17. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. Госстандарт СССР, 1990.
18. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. Ростехрегулирование, 2008.
19. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. Ростехрегулирование, 2008.
20. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт, 2012.
21. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. Росстандарт, 2013.
22. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. Росстандарт, 2013.
23. ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимости. Росстандарт, 2015.
24. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимости информационных систем. Росстандарт, 2015.
25. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Гостехкомиссии при Президенте Российской Федерации от 4 июня 1999 г.

№114.
26. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 2.03.2001 № 282.
27. Положение об аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25.11.1994.
28. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
29. 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 марта 2014 г. №31.
30. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
31. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
32. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15.02.2008.
33. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14.02.2008;

БАЗЫ ДАННЫХ, ИНФОРМАЦИОННО-СПРАВОЧНЫЕ И ПОИСКОВЫЕ СИСТЕМЫ

1. Информационно-правовая система «Законодательство России» // Официальный интернет-портал правовой информации – URL: http:// www.pravo.gov.ru;
2.Официальный сайт ФСТЭК России – URL: http:// www.fstec.ru; банк данных угроз безопасности информации – URL: http://bdu.fstec.ru;
3.Каталог стандартов // Официальный сайт Росстандарта – URL: http://www.gost.ru/wps/portal/pages.CatalogOfStandarts;
4.Правовые справочно-поисковые системы («Гарант», «Консультант Плюс»).