Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

Иванцов А.М.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «ПРОФЕССИОНАЛЬНЫЙ ЭЛЕКТИВ. КОНТРОЛЬ СОСТОЯНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ»

Для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения

Ульяновск, 2022

Методические указания для самостоятельной работы студентов по дисциплине «Профессиональный электив. Контроль состояния технической защиты конфиденциальной информации» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2022. Настоящие методические указания предназначены для студентов специалитета по специальностям 10.05.01 и 10.05.03 очной формы обучения. В работе приведены литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля и тесты для самостоятельной работы. Студентам очной формы обучения они будут полезны при подготовке к лекциям, семинарам, курсовым работам и к зачёту по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол №3/22 от 19.04.2022 г.).

Содержание

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1. Основы информационной безопасности. Курс лекций. Часть 2 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2020 – 103 с.

2. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

3. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

4. Шелухин О.И., Обнаружение вторжений в компьютерные сети (сетевые аномалии): Учебное пособие для вузов / Под ред. профессора О.И. Шелухина. - М.: Горячая линия - Телеком, 2013. - 220 с. - ISBN 978-5-9912-0323-4 - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: http://www.studentlibrary.ru/book/ISBN9785991203234.html

5. Бузов Г.А., Защита информации ограниченного доступа от утечки по техническим каналам [Электронный ресурс] / Г.А. Бузов - М.: Горячая линия - Телеком, 2015. – 586 с. - ISBN 978-5-9912-0424-8 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204248.html

6. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России от 11 февраля 2014 г.

7. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

8. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

9. Инженерно-техническая защита информации: учебное пособие для студентов, обучающихся по специальностям в области информационной безопасности / А.А. Торокин. М.: Гелиос АРВ, 2005, 960 с.

10. Игнатенков В.Г., Сахнин А.А. Защищённое информационное пространство. Комплексный технический контроль радиоэлектронных средств / Под ред. А.А. Сахнина. – М.: Горячая линия – Телеком, 2018. – 336 с. ил.

11. Милославская, Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : учебное пособие для вузов / Милославская Н. Г. , Сенаторов М. Ю. , Толстой А. И. - Вып. 3. - Москва : Горячая линия - Телеком, 2013. - 170 с. (Серия "Вопросы управления информационной безопасностью") - ISBN 978-5-9912-0273-2. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785991202732.html

12. Разработка типовых документов в области информационной безопасности: методические указания [Электронный ресурс]: электронный учебный курс / Иванцов Андрей Михайлович; УлГУ. - Ульяновск : УлГУ, 2016. - 1 электрон. опт. диск (CD-ROM). **URL:** http://edu.ulsu.ru/cources/750/interface/.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. ОСНОВЫ ОРГАНИЗАЦИИ КОНТРОЛЯ СОСТОЯНИЯ ТЗКИ

ТЕМА 1. ОСНОВНЫЕ ЗАДАЧИ КОНТРОЛЯ СОСТОЯНИЯ ТЗКИ

Основные вопросы:

1. Сущность и задачи контроля состояния ТКЗИ
2. Система документов по контролю состояния ТЗКИ
3. Вопросы, подлежащие проверке при контроле состояния ТКЗИ в организации

Рекомендации по изучению темы:

Вопрос 1 изложен в [3].

Для самостоятельного изучения вопроса 1 следует обратиться к [6,8].

Вопрос 2 изложен в учебном пособии [7].

Для самостоятельного изучения вопроса 2 следует обратиться к [8, 10].

Вопрос 3 изложен в [8].

Для самостоятельного изучения вопроса 3 следует обратиться к учебному пособию [1] на стр. 77-82.

Контрольные вопросы по теме 1:

1. Перечислить основные документы по контролю состояния ТЗКИ
2. Сущность контроля состояния
3. Основные задачи контроля состояния ТКЗИ
4. Основные вопросы, подлежащие проверке при контроле состояния ТКЗИ в организации
5. Что предусматривает периодический контроль эффективности защиты информации?

Тесты для самостоятельной работы:

1. Методическое руководство и контроль за эффективностью предусмотренных мер защиты информации возлагается на:

а) руководителя организации

б) руководителей подразделений по защите информации организации

в) ответственных, назначенных приказом руководителя

2. С какой периодичностью должен проводиться контроль состояния защиты информации в организации:

а) не реже 2 раз в год

б) ежемесячно

в) не реже 1 раза в год

2.2. РАЗДЕЛ 1. ОСНОВЫ ОРГАНИЗАЦИИ КОНТРОЛЯ СОСТОЯНИЯ ТЗКИ

ТЕМА 2. ОРГАНИЗАЦИОННЫЙ И ТЕХНИЧЕСКИЙ КОНТРОЛЬ СОСТОЯНИЯ ТЗКИ

Основные вопросы:

1. Классификация видов контроля состояния ТКЗИ. Организационный и технический контроль состояния ТЗКИ
2. Система документации по контролю состояния ТЗКИ

Рекомендации по изучению темы:

Вопрос 1 изложен в [8].

Вопрос 2 изложен в учебном пособии [8].

Для самостоятельного изучения вопроса 2 следует обратиться к [6, 7].

Контрольные вопросы по теме 2

1. Что включает в себя контроль состояния ТЗИ
2. Пояснить сущность организационного контроля состояния ТЗКИ
3. Пояснить сущность технического контроля состояния ТЗКИ
4. Дать определение средства контроля эффективности защиты информации
5. Перечислить основные документы по контролю состояния ТЗКИ

Тесты для самостоятельной работы:

1. Чем характеризуется организационный контроль эффективности защиты информации?

а) контролем эффективности защиты информации, проводимой с использованием средств контроля

б) укомплектованностью подразделений по защите информации

в) проверкой полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации

2. **Технический контроль состояния защиты конфиденциальной информации осуществляется в соответствии с:**

а) программами и методикам, согласованными с ФСТЭК России

б) программами и методикам ФСБ России

в) программами и методикам, разработанными лицензиатами ФСТЭК России

2.3. РАЗДЕЛ 2. МЕТОДЫ И СРЕДСТВА КОНТРОЛЯ ЗАЩИЩЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

ТЕМА 3. МЕТОДЫ И СРЕДСТВА КОНТРОЛЯ ЗАЩИЩЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ, ОТ УТЕЧКИ ЗА СЧЕТ ПЭМИН

Основные вопросы:

1. Основные методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН
2. Методика оценки защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [5] стр. 278-308.

Для самостоятельного изучения вопроса 1 следует обратиться к [2, 3]

Вопрос 2 изложен в учебном пособии [5] стр. 308-314.

Контрольные вопросы по теме 3:

1. Назвать основные методы контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН
2. Назвать основные методы контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН
3. Обосновать понятие ПЭМИН
4. Что включает в себя методология оценки защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН
5. Охарактеризовать технический канал утечки информации за счет ПЭМИН

Тесты для самостоятельной работы:

1. Какой из режимов обработки информации средствами вычислительной техники является наиболее опасным с точки зрения утечки информации за счет побочных электромагнитных излучений:

а) Чтение информации с накопителей

б) Передача данных в каналы связи

в) Вывод информации на экран монитора

г) Ввод данных с клавиатуры

2. На что направлены активные методы защиты:
а) На ослабление наводок побочных электромагнитных излучений
б) На создание маскирующих электромагнитных помех
в) На исключение (ослабление) просачивания информативных сигналов в цепи электропитания

3. **Предъявляемые требования к аппаратуре измерения побочных электромагнитных излучений**
а) Диапазон частот
б) Чувствительность
в) Погрешность
г) Класс точности

4. **На что направлены пассивные методы защиты:**
а) На создание маскирующих электромагнитных помех
б) На создание маскирующих электрических помех в посторонних проводниках и соединительных линиях
в) На ослабление побочных электромагнитных излучений и наводок

5. **Предъявляемые требования к аппаратуре измерения наводок побочных электромагнитных излучений:**
а) Диапазон частот
б) Чувствительность
в) Погрешность
г) Класс точности

6. Предъявляемые требования к средствам пассивной защиты:
а) Диапазон частот
б) Чувствительность
в) Неравномерность амплитудно-частотной характеристики
г) Коэффициент затухания

2.4. РАЗДЕЛ 2. МЕТОДЫ И СРЕДСТВА КОНТРОЛЯ ЗАЩИЩЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

ТЕМА 4. МЕТОДЫ И СРЕДСТВА КОНТРОЛЯ ЗАЩИЩЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ АКУСТИЧЕСКОЙ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Основные вопросы:

1. Обобщённая структура технического канала утечки
2. Основные методы и средства контроля защищенности конфиденциальной акустической речевой информации от утечки

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [9] на с. 171-190.

Для самостоятельного изучения вопроса 1 следует обратиться к [5] на с. 9-17.

Вопрос 2 изложен в учебном пособии [9] на с. 352-360.

Для самостоятельного изучения вопроса 2 следует обратиться к [5] на с. 26-27.

Контрольные вопросы по теме 4:

1. Пояснить структуру образования канала утечки
2. В чём заключается отличие ОТСС от ВТСС? Привести 4-5 примеров
3. Раскрыть типовой канал утечки информации за счет возникновения паразитной генерации и самовозбуждения
4. Раскрыть типовой канал утечки информации вследствие акустозвуковых преобразований.
5. Что такое преобразователи акустических и вибрационных колебаний? Привести 5-6 примеров.
6. Что такое автономные закладные устройства? Привести 3-4 примера.
7. Пояснить физическую природу виброакустического канала утечки.
8. Назвать пассивные и активные способы защиты речи от несанкционированного прослушивания.
9. Основные правила выбора ограждающих конструкций выделенных помещений в процессе проектирования.
10. Типовая аппаратура активной защиты помещений от утечки речевой информации.
11. Назвать характерные особенности постановки акустических помех.
12. Основные рекомендации по выбору средств контроля систем виброакустической защиты.

Тесты для самостоятельной работы:

1. Что относится к активным способам защиты выделенных помещений:

а) Использование виброгенераторов на стеклах
б) Использование акустических излучателей
в) Двойные двери
г) Звукоизоляция стен

2. Предъявляемые требования к аппаратуре измерения акустических и вибрационных сигналов:

а) Чувствительность
б) Неравномерность амплитудно-частотной характеристики
в) Погрешность
г) Точность

3. **Что относится к пассивным способам защиты выделенных помещений:**

а) Использование виброгенераторов на стеклах
б) Двойные двери
в) Использование акустических излучателей
г) Звукоизоляция стен

4. **К каналам утечки акустической речевой информации относится:**

а) Магнитные и электрические излучения
б) Акустические колебания
в) Лазерные излучения
г) Вибрационные колебания

5. К параметрическим каналам утечки акустической речевой информации относится:

а) Высокочастотное навязывание
б) Электрические сигналы
в) Электромагнитные излучения
г) Высокочастотное облучение

2.5. РАЗДЕЛ 2. МЕТОДЫ И СРЕДСТВА КОНТРОЛЯ ЗАЩИЩЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

ТЕМА 5. МЕТОДЫ И СРЕДСТВА КОНТРОЛЯ ЗАЩИЩЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОТ НСД

Основные вопросы:

1. Межсетевые экраны, требования к ним и способы применения.
2. Системы обнаружения вторжений, требования к ним и способы применения.
3. Криптографические средства защиты информации.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 70-87.
Вопрос 2 изложен в учебном пособии [4] главы 2-3.
Вопрос 3 изложен в учебном пособии [1] на с. 30-57.

Контрольные вопросы по теме 5:

1. Что понимается под технологией межсетевого экранирования?
2. Классификация межсетевых экранов.
3. Основные функции межсетевых экранов.
4. Охарактеризовать элементы, входящие в обобщённую систему обнаружения вторжений (СОВ).
5. Каким образом оценивается эффективность СОВ.
6. Какие отличия интеллектуальной СОВ от поведенческой.
7. Пояснить классификацию СОВ.
8. Обобщенная схема асимметричной криптосистемы шифрования.
9. Процесс передачи зашифрованной информации в асимметричной криптосистеме.
10. Назвать характерные особенности асимметричных криптосистем.
11. Требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы.
12. Привести пример однонаправленной функции.
13. Преимущества и недостатки асимметричных криптосистем.
14. Функция хэширования и её свойства.
15. Что такое дайджест сообщения?
16. Электронная подпись.
17. От каких видов злоумышленных действий позволяет защитить использование ЭП?

18. Процедуры формирования и проверки ЭП.

Тесты для самостоятельной работы:

1. Сколько существует классов защищенности ИС от НСД к информации?

а) 10
б) 9
в) 12
г) 5

2. Что, из перечисленного, включает в себя ИС первой группы обработки информации?

а) ИС, в которых работает один пользователь
б) ИС, в которых пользователи имеют одинаковые права доступа
в) Многопользовательские ИС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности

3. К основным способам НСД не относится:

а) Непосредственное обращение к объектам доступа
б) Резервирование технических средств, дублирование массивов и носителей информации
в) Создание программных и технических средств
г) Модификация средств защиты

4. К принципам защиты от НСД не относится:

а) Защита СВТ обеспечивается комплексом программно-технических средств
б) Защита СВТ и АС основывается на положениях и требованиях соответствующих законов, стандартов и нормативно-методических документов по защите от НСД к информации
в) Защита АС обеспечивается отдельными сотрудниками, ответственными за защиту информации
г) Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер

2.6. РАЗДЕЛ 3. МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СРЕДСТВ И СИСТЕМ ИНФОРМАТИЗАЦИИ

ТЕМА 6. ЦЕЛИ, ЗАДАЧИ И ФУНКЦИИ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СРЕДСТВ И СИСТЕМ ИНФОРМАТИЗАЦИИ

Основные вопросы:

1. Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации
2. Состав и структура системы мониторинга информационной безопасности средств и систем информатизации
3. Порядок и методы мониторинга информационной безопасности средств и систем информатизации

Рекомендации по изучению темы:

Вопрос 1 изложен в [10] на стр. 90-105.
Вопрос 2 изложен в [10] на стр. 105-121.
Вопрос 3 изложен в [10] на стр. 122-134.

Контрольные вопросы по теме 6:

1. Цели, задачи и функции мониторинга информационной безопасности средств и систем информатизации
2. Состав типовой структура системы мониторинга информационной безопасности средств и систем информатизации
3. Характеристика основных элементов системы мониторинга информационной безопасности средств и систем информатизации
4. Порядок проведения мониторинга информационной безопасности средств и систем информатизации
5. Основные методы мониторинга информационной безопасности средств и систем информатизации

Тесты для самостоятельной работы:

1. Какой из нижеперечисленных факторов влияет на эффективность защиты информации от утечки?

а) Отношение сигнал/шум на входе приемника сигналов
б) Время и затраты на поиск канала утечки
в) Демаскирующие признаки носителя информации

2. Каким показателем характеризуется источник сигнала?

а) Мощность помех

б) Чувствительность
в) Диаграмма направленности излучения
г) Скорость распространения сигнала в среде

3. Каким из параметров обладает приемник сигналов?
а) Динамический диапазон сигнала
б) Параметр спектра сигнала
в) Пространственная селективность приемной антенны
г) Амплитудно-частотная характеристика

4. Основной метод при проведении специальных исследований:
а) радиомониторинг
б) нелинейная локация
в) инструментальный
г) Высокочастотное облучение и высокочастотное навязывание

2.7. РАЗДЕЛ 3. МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СРЕДСТВ И СИСТЕМ ИНФОРМАТИЗАЦИИ

ТЕМА 7. ОБНАРУЖЕНИЕ И ИДЕНТИФИКАЦИЯ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Основные вопросы:
1. Понятие события и инцидента ИБ
2. Система управления инцидентами ИБ
3. Этапы процесса управления инцидентами ИБ
4. Политика управления инцидентами ИБ

Рекомендации по изучению темы:
Вопрос 1 изложен в учебном пособии [11] на с. 20-26.
Для самостоятельного изучения вопроса 2 следует обратиться к соответствующим стандартам.
Вопрос 2 изложен в учебном пособии [11] на с. 31-39.
Вопрос 3 изложен в учебном пособии [11] на с. 39-45.
Вопрос 4 изложен в учебном пособии [11] на с. 71-72.
Для самостоятельного изучения вопроса 4 следует обратиться к соответствующим стандартам.

Контрольные вопросы по теме 7:
1. Нормативная база управления инцидентами ИБ
2. Суть жизненного цикла СУИБ
3. Понятие события и инцидента ИБ
4. Цели и задачи управления инцидентами ИБ
5. Цели организации по эффективному управлению инцидентами ИБ.

6. Процесс «Управление инцидентами ИБ»
7. Система управления инцидентами ИБ
8. Ключевые вопросы при создании результативно функционирующей СУИИБ
9. Этапы процесса управления инцидентами ИБ
10. Политика управления инцидентами ИБ
11. Обеспечение осведомленности и обучение в области инцидентов ИБ

Тесты для самостоятельной работы:

1. Какой пример, из перечисленных, может быть квалифицирован, как событие ИБ?

а) Отключение электропитания
б) Неверный ввод пароля 2 раз подряд
в) Отправка информации ограниченного доступа в сети Интернет без паролирования (шифрования)
г) Несанкционированное копирование информации ограниченного доступа на личный флэш-носитель

2. **Какой пример, из перечисленных, может быть квалифицирован, как инцидент ИБ?**

а) Отказ в обслуживании
б) Неудавшаяся попытка кражи носителя с информацией ограниченного доступа
в) Ввод неправильного пароля
г) Пароль, написанный на стикере, прикреплённый к монитору сотрудника

3. **Какой вариант цели организации не способствует эффективному управлению инцидентами ИБ**

а) Сохранить и восстановить данные
б) Наказать нарушителей Политики ИБ организации
в) Гарантировать целостность критически важных систем
г) Предотвратить развитие атак и будущие инциденты ИБ
д) Избежать нежелательной огласки информации об инциденте ИБ

4. **На каком этапе процесса управления инцидентами происходят реагирование на инцидент ИБ и определение необходимости проведения расследования инцидента ИБ?**

а) На этапе планирования и подготовки
б) На этапе совершенствования
в) На этапе использования
г) На этапе анализа

5. **Какие вопросы согласно требованиям стандартов отражаются в политике управления инцидентами ИБ?** Указать 4 варианта.

а) Обязательства высшего руководства относительно поддержки управления

инцидентами
б) Подробная программа обеспечения осведомлённости и обучения управлению инцидентами ИБ
в) Перечень ответственных лиц, необходимые для выполнения действия, уведомления об инцидентах ИБ
г) Извлечение уроков и улучшение процесса, следующего за инцидентами ИБ
д) Краткое изложение действий после подтверждения категории инцидента ИБ

2.8. РАЗДЕЛ 3. МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СРЕДСТВ И СИСТЕМ ИНФОРМАТИЗАЦИИ

ТЕМА 8. ПЛАНИРОВАНИЕ МЕР ПО УСТРАНЕНИЮ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Основные вопросы:

1. Общая характеристика планов управления инцидентами, обеспечения непрерывности бизнеса и восстановления бизнеса
2. Примерное содержание плана обеспечения непрерывности бизнеса

Рекомендации по изучению темы:

Вопрос 1 изложен в лекции.
Для самостоятельного изучения вопроса 1 следует обратиться к соответствующим стандартам.
Вопрос 2 изложен в учебном пособии [12] на с. 21-28.
Для самостоятельного изучения вопроса 2 следует обратиться к соответствующим стандартам.

Контрольные вопросы по теме 8:

1. Понятие управления непрерывности бизнеса
2. Обеспечение устойчивости бизнес-процессов к инцидентам
3. Восстановление бизнеса, включая бизнес-процессы, операции и ресурсы, организации после инцидентов
4. Система управления непрерывностью бизнеса
5. Типовые технические решения для обеспечения непрерывности бизнеса
6. Внедрение управления непрерывностью бизнеса в культуру организации
7. Общая характеристика планов управления инцидентами, обеспечения непрерывности бизнеса и восстановления бизнеса
8. Примерное содержание плана обеспечения непрерывности бизнеса
9. Основные требования к ресурсам
10. План восстановления бизнеса

Тесты для самостоятельной работы:

1. Какие условия требуют реализации стратегия немедленной защиты и восстановления? Отметить 4 условия.

а) Если ресурсы ИС недостаточно хорошо защищены от нарушителя
б) Если действия нарушителя могут привести к небольшому финансовому риску
в) Если преследование нарушителя невыгодно с финансовой точки зрения, либо отсутствует такая возможность или желание
г) Если возможно предъявление претензий со стороны клиентов Компании
д) Если существует значительный риск для пользователей ИС

2. Какие условия требуют реализации стратегия наблюдения за нарушителем и его преследования? Отметить 4 условия.
а) Ресурсы ИС адекватно защищены
б) Попытка НСД является продолжением предыдущих попыток, уже имевших место ранее
в) Доступ нарушителя к ресурсам ИС находится под контролем
г) Средства мониторинга не в состоянии осуществлять достаточно полное протоколирование действий нарушителя для того, чтобы собрать необходимые доказательства
д) Администраторы ИС достаточно хорошо подготовлены в плане знания ОС, системных утилит, СУБД и прикладных систем, чтобы осуществлять отслеживание действий нарушителя

3. **Какие технические решения могут входить в состав системы управления непрерывностью бизнеса?** Отметить 3 позиции.
а) Системы охранно-пожарной сигнализации
б) Системы резервного копирования
в) Системы криптографического преобразования информации
г) Системы резервного электропитания

4. **В каком из названных планов содержится набор документированных процедур и информации, которые разработаны, обобщены и актуализированы с целью их использования в случае возникновения инцидента?**
а) План защиты
б) План обеспечения непрерывности бизнеса
в) План восстановления

5. **В каком плане описывается, что должно испытываться при проверке реализуемости плана, кто должен проводить испытания, когда должны осуществляться испытания и каковы их результаты?**
а) План защиты
б) План обеспечения непрерывности бизнеса
в) План восстановления бизнеса

2.9. РАЗДЕЛ 3. МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СРЕДСТВ И СИСТЕМ ИНФОРМАТИЗАЦИИ

ТЕМА 9. ДОКУМЕНТИРОВАНИЕ ПРОЦЕДУР И РЕЗУЛЬТАТОВ КОНТРОЛЯ (МОНИТОРИНГА) ЗА ОБЕСПЕЧЕНИЕМ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

1. Содержание протоколов аттестационных испытаний и заключения по результатам аттестационных испытаний информационных (автоматизированных) систем
2. Содержание протоколов аттестационных испытаний и заключения по результатам аттестационных испытаний выделенных (защищаемых) помещений
3. Оформление аттестата соответствия на выделенное (защищаемое) помещение

Рекомендации по изучению темы:

Для изучения вопросов 1,2 следует обратиться к национальному стандарту ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний».

Для изучения вопроса 3 следует обратиться к Приложению 2 «Положения по аттестации объектов информатизации по требованиям безопасности информации» и к Приложению Б национального стандарта ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»

Контрольные вопросы по теме 9:

1. Перечислите основные разделы типовой программы и методики аттестационных испытаний
2. Перечислите основные этапы аттестации информационных (автоматизированных) систем.
3. Перечислите основные разделы протоколов аттестационных испытаний
4. Перечислите основные разделы заключения по результатам аттестационных испытаний
5. Перечислите основные разделы аттестата соответствия на информационную (автоматизированную) систему.
6. Перечислите основные разделы заключения по результатам аттестационных испытаний
7. Перечислите основные разделы аттестата соответствия на выделенное (защищаемое) помещение.

Тесты для самостоятельной работы:

1. Что не должно входить в состав отчетных документов о проведении обследования помещения?

а) Протоколы изъятия средств съема информации
б) Рекомендации по устранению и нейтрализации технических каналов утечки
в) Методические рекомендации о степени защищенности объекта

2. В течение какого времени действует аттестат соответствия на автоматизированную систему?

а) 5 лет
б) 3 года
в) бессрочно