Автономная некоммерческая организация
профессионального образования
«Колледж информационных технологий «КАСПИЙ»
367013, г. Махачкала, пр-кт. Гамидова, зд.18м
ОГРН: 1220500003580, ИНН: 0572030404

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем
квалификация - Техник по защите информации

Махачкала, 2025 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу профессионального модуля ПМ.03 Защита информации техническими средствами. КОС включает контрольные материалы для промежуточной аттестации. освоение содержания профессионального модуля ПМ.03 Защита информации техническими средствами обеспечивает достижение студентами следующих результатов:

- Иметь практический опыт
- умений
- знаний

Формы промежуточной аттестации по профессиональному модулю в ходе освоения ОПОП ППССЗ

Наименование профессионального модуля	**Форма промежуточной аттестации (дифференцированный зачет, экзамен)**
МДК 03.01 Техническая защита информации	Экзамен Контрольная работа
МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации	Экзамен Контрольная работа

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

В результате аттестации по профессинальному модулю осуществляется комплексная проверка компетенций (ОК, ПК).

Результаты обучения компетенции	**Показатели оценки результата**	**Форма контроля и оценивания**
Иметь практический опыт	• установки, монтажа и настройки технических средств защиты информации; • технического обслуживания технических средств защиты информации; • выявления технических каналов утечки информации; • участия в мониторинге эффективности технических средств защиты информации; • диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; • проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой	Задание 1. Дифференцированный зачет по МДК 03.01 Задание 2. Комплексный экзамен по МДК 03.01, МДК 03.02

	установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; • проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; • установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.	
Знать	• порядок технического обслуживания технических средств защиты информации; • номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; • физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; • порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; • методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; • номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; • основные принципы действия и характеристики технических средств	Задание 1. Дифференцированный зачет по МДК 03.01 Задание 2. Комплексный экзамен по МДК 03.01, МДК 03.02
Уметь	• применять технические средства для криптографической защиты информации конфиденциального	1.Контрольные задания для экзамена по междисциплинарному

	характера; • применять технические средства для уничтожения информации и носителей информации; • применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; • применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; • применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; • применять инженерно-технические средства физической защиты объектов информатизации	курсу МДК 02.01 Задание № 1. Контрольные задания для дифференцированного зачета по междисциплинарному курсу МДК 02.01 Задание № 2. 2. Контрольные задания для экзамена по междисциплинарному курсу МДК 02.02 Задание № 2. Контрольные задания для дифференцированного зачета по междисциплинарному курсу МДК 02.01 Задание № 2.

Профессиональные и общие компетенции, которые возможно сгруппировать для проверки	**Показатели оценки результата**
ПК 3.1. Применять инженерно-технические средства обеспечения информационной безопасности.	-обосновать выбора инженерных, технических и организационных решений; -точность и грамотность оформления организационной и технической
ПК3.2 Участвовать в эксплуатации инженерно-технических средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности.	-точность и скорость диагностики нарушений эксплуатационных характеристик систем; -качество анализа эксплуатационных свойств системы, исходя из ее служебного назначения; -качества рекомендаций по повышению эксплуатационных свойств системы; -умение проводить техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность
ПК 3.3 Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности	-обоснованность подбора средств и методов мониторинга эффективности инженерно-технических средств обеспечения информационной безопасности в автоматизированных системах
ПК 3.4. Решать частные технические задачи, возникающие при проведении всех	-умение решать частные технические задачи, возникающие при проведении

видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, технических средств.	всех видов плановых и внеплановых контрольных проверок, при аттестации объектов, помещений, программ, алгоритмов. -умение осуществлять мероприятия по выявлению о оценке свойств каналов утечки информации
ПК 3.5Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами	-точность и грамотность применения нормативных правовых актов, нормативно-методических документов по обеспечению информационной безопасности инженерно-техническими средствами
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес	демонстрация интереса к будущей профессии. Эта ОК проверяется с помощью портфолио
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество	- деятельность по выполнению проектного задания организована правильно в соответствии с планом - методы и способы решения проектного задания выбраны верно в соответствии с задачами проекта. - самооценка эффективности и качества выполненного задания проведена верно в соответствии с требованиями к качеству и качества выполнения профессиональных задач.
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	решение стандартных и нестандартных профессиональных задач в области разработки программного обеспечения
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	- эффективный поиск необходимой информации; - использование различных источников, включая электронные.
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности	работа на ПЭВМ.
ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями	ОК проверяется с помощью портфолио
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий	самоанализ и коррекция результатов собственной работы.
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	ОК проверяется с помощью портфолио
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной	анализ инноваций в области разработки программного обеспечения.

деятельности	
ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей)	готовность исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний.
ОК 11 Формулировать задачи логического характера и применять средства математической логики для их решения	-демонстрация способности формулировать задачи логического характера и применять для их решения средства математической логики
ОК 12 Владеть основными методами и средствами разработки программного обеспечения	демонстрация умения применять основные методы и средства разработки программного обеспечения
ОК 13 Производить инсталляцию и настройку автоматизированных информационных систем, выполнять в автоматизированных информационных системах регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах	демонстрация умения производить инсталляцию и настройку автоматизированных информационных систем, выполнять регламентные работы по обновлению, техническому сопровождению и восстановлению при отказах автоматизированных систем

ТЕСТ

1. Под информационной безопасностью понимается…

А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации, и поддерживающей инфраструктуре.

Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

В) нет правильного ответа

2. Защита информации – это_____

А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) от компьютеров

Б) от поддерживающей инфраструктуры

В) от информации

4. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

5. Доступность – это_____

А) возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость

В) нет правильного ответа

6. Целостность – это_____

А) целостность информации

Б) непротиворечивость информации

В) защищенность от разрушения

7. Конфиденциальность – это_____

А) защита от несанкционированного доступа к информации

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

8. Для чего создаются информационные системы?

А) получения определенных информационных услуг

Б) обработки информации

В) все ответы правильные

9. Целостность можно подразделить:

А) статическую

Б) динамичную

В) структурную

10. Где применяются средства контроля динамической целостности?

А) анализе потока финансовых сообщений

Б) обработке данных

В) при выявлении кражи, дублирования отдельных сообщений

11. Какие трудности возникают в информационных системах при конфиденциальности?

А) сведения о технических каналах утечки информации являются закрытыми

Б) на пути пользовательской криптографии стоят многочисленные технические проблемы

В) все ответы правильные

12. Угроза – это…

А) потенциальная возможность определенным образом нарушить информационную безопасность

Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

13. Атака – это…

А) попытка реализации угрозы

Б) потенциальная возможность определенным образом нарушить информационную безопасность

В) программы, предназначенные для поиска необходимых программ.

14. Источник угрозы – это..

А) потенциальный злоумышленник

Б) злоумышленник

В) нет правильного ответа

15. Окно опасности – это…

А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.

Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области

В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

16. Какие события должны произойти за время существования окна опасности?

А) должно стать известно о средствах использования пробелов в защите.

Б) должны быть выпущены соответствующие заплаты.

В) заплаты должны быть установлены в защищаемой И.С.

17. Угрозы можно классифицировать по нескольким критериям:

А) по спектру И.Б.

Б) по способу осуществления

В) по компонентам И.С.

18. По каким компонентам классифицируется угрозы доступности:

А) отказ пользователей

Б) отказ поддерживающей инфраструктуры

В) ошибка в программе

19. Основными источниками внутренних отказов являются:

А) отступление от установленных правил эксплуатации

Б) разрушение данных

В) все ответы правильные

20. Основными источниками внутренних отказов являются:

А) ошибки при конфигурировании системы

Б) отказы программного или аппаратного обеспечения

В) выход системы из штатного режима эксплуатации

21. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности

Б) обрабатывать большой объем программной информации

В) нет правильного ответа

22. Какие существуют грани вредоносного П.О.?

А) вредоносная функция

Б) внешнее представление

В) способ распространения

23. По механизму распространения П.О. различают:

А) вирусы

Б) черви

В) все ответы правильные

24. Вирус – это…

А) код обладающий способностью к распространению путем внедрения в другие программы

Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи

25. Черви – это…

А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения
Б) код обладающий способностью к распространению путем внедрения в другие программы

В) программа действий над объектом или его свойствами

26. Конфиденциальную информацию можно разделить:

А) предметную
Б) служебную
В) глобальную

27. Природа происхождения угроз:

А) случайные
Б) преднамеренные
В) природные

28. Предпосылки появления угроз:

А) объективные
Б) субъективные
В) преднамеренные

29. К какому виду угроз относится присвоение чужого права?

А) нарушение права собственности
Б) нарушение содержания
В) внешняя среда

30. Отказ, ошибки, сбой – это:

А) случайные угрозы
Б) преднамеренные угрозы
В) природные угрозы

31. Отказ - это…

А) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

Б) некоторая последовательность действий, необходимых для выполнения конкретного задания

В) структура, определяющая последовательность выполнения и взаимосвязи процессов

32. Ошибка – это…

А) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния

Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

В) негативное воздействие на программу

33. Сбой – это…

А) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент

Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния

В) объект-метод

34. Побочное влияние – это…

А) негативное воздействие на систему в целом или отдельные элементы

Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент

В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

35. СЗИ (система защиты информации) делится:

А) ресурсы автоматизированных систем

Б) организационно-правовое обеспечение

В) человеческий компонент

36. Что относится к человеческому компоненту СЗИ?

А) системные порты

Б) администрация

В) программное обеспечение

37. Что относится к ресурсам А.С. СЗИ?

А) лингвистическое обеспечение

Б) техническое обеспечение

В) все ответы правильные

38. По уровню обеспеченной защиты все системы делят:

А) сильной защиты

Б) особой защиты

В) слабой защиты

39. По активности реагирования СЗИ системы делят:

А) пассивные

Б) активные

В) полупассивные

40. Правовое обеспечение безопасности информации – это…

А) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации

Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

В) нет правильного ответа

41. Правовое обеспечение безопасности информации делится:

А) международно-правовые нормы

Б) национально-правовые нормы

В) все ответы правильные

42. Информацию с ограниченным доступом делят:

А) государственную тайну

Б) конфиденциальную информацию

В) достоверную информацию

43. Что относится к государственной тайне?

А) сведения, защищаемые государством в области военной, экономической … деятельности

Б) документированная информация

В) нет правильного ответа

44. Вредоносная программа - это…

А) программа, специально разработанная для нарушения нормального функционирования систем

Б) упорядочение абстракций, расположение их по уровням

В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение

45. Основополагающие документы для обеспечения безопасности внутри организации:

А) трудовой договор сотрудников

Б) должностные обязанности руководителей

В) коллективный договор

46. К организационно - административному обеспечению информации относится:

А) взаимоотношения исполнителей

Б) подбор персонала

В) регламентация производственной деятельности

47. Что относится к организационным мероприятиям:

А) хранение документов

Б) проведение тестирования средств защиты информации

В) пропускной режим

48. Какие средства используется на инженерных и технических мероприятиях в защите информации:

А) аппаратные

Б) криптографические

В) физические

49. Программные средства – это…

А) специальные программы и системы защиты информации в информационных системах различного назначения

Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла

В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

50. Криптографические средства – это…

А) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования

Б) специальные программы и системы защиты информации в информационных системах различного назначения

В) механизм, позволяющий получить новый класс на основе существующего

Задание 1. Какие виды электрических полей существуют в природе? Каким образом электрические заряды взаимодействуют друг с другом? Назовите источники электрических полей и способы его обнаружения.

Задание 2. В чем отличие электростатического поля от вихревого электрического поля?

Какому закону подчиняется взаимодействие неподвижных электрических зарядов?

Задание 3. Что является источником магнитных полей? Приведите примеры магнитных полей в природе. Перечислите свойства линий магнитной индукции. В каких случаях магнитное поле называется однородным?

Задание 4. Какими существенными свойствами отличается магнитное поле от электрического?

Задание 5. Назовите характеристики электрического поля и их единицы измерения.

Задание 6. Назовите характеристики магнитного поля и их единицы измерения.

Задание 7. От чего зависит характер электромагнитного поля в той или иной точке пространства? В чем сущность явления электромагнитной индукции? На какие зоны и по какому принципу подразделяется пространство вокруг источника электромагнитного поля?

Задание 8. Как изменяются векторы напряженности электрического и магнитного поля в ближней зоне? Как изменяются векторы напряженности электрического и магнитного поля в дальней зоне?

Задание 9. Что такое акустическое поле? На какие виды оно подразделяется?

Задание 10. Расскажите об экранировании электрических полей (типы полей, диапазон частот). Какие известны способы уменьшения паразитной емкости при экранировании низкочастотных электрических полей?

Задание 11. Когда применяется экранирование от магнитных полей?

Задание 12. Какие физические принципы лежат в основе экранирования постоянных магнитных полей? На чем основано «шунтирование» магнитного поля?

ВОПРОСЫ К ЭКЗАМЕНАМ

1. Особенности информации как предмета защиты. Свойства информации.
2. Виды, источники и носители защищаемой информации.
3. Демаскирующие признаки объектов наблюдения, сигналов и веществ.
4. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства, и системы.
5. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке
6. Классификация технических средств разведки.
7. Методы и средства технической разведки.
8. Средства несанкционированного доступа к информации.
9. Средства и возможности оптической разведки.
10. Средства дистанционного съема информации
11. Физические основы побочных электромагнитных излучений и наводок.
12. Акустоэлектрические преобразования.
13. Паразитная генерация радиоэлектронных средств.
14. Виды паразитных связей и наводок.
15. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.
16. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей.
17. Скрытие речевой информации в каналах связи.
18. Подавление опасных сигналов акустоэлектрических преобразований.
19. Экранирование.
20. Зашумление.
21. Технические средства акустической разведки.
22. Непосредственное подслушивание звуковой информации.
23. Прослушивание информации направленными микрофонами.
24. Система защиты от утечки по акустическому каналу.
25. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.
26. Принцип работы микрофона и телефона.
27. Использование коммуникаций в качестве соединительных проводов.
28. Негласная запись информации на диктофоны.
29. Системы защиты от диктофонов.
30. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.
31. Прослушивание информации от радиотелефонов.
32. Прослушивание информации от работающей аппаратуры.
33. Прослушивание информации от радиозакладок.
34. Приемники информации с радиозакладок.
35. Прослушивание информации о пассивных закладках.
36. Системы защиты от утечки по электромагнитному каналу.
37. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.
38. Прослушивание информации от радиотелефонов.
39. Прослушивание информации от работающей аппаратуры.
40. Прослушивание информации от радиозакладок.
41. Приемники информации с радиозакладок.
42. Прослушивание информации о пассивных закладках.
43. Системы защиты от утечки по электромагнитному каналу.
44. Номенклатура применяемых средств защиты информации от

несанкционированной утечки 1. Задание для устного опроса по темам

45. Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.

46. Использование микрофона телефонного аппарата при положенной телефонной трубке.

47. Низкочастотное устройство съема информации.

48. Высокочастотное устройство съема информации.

49. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.

50. Утечка информации по сотовым цепям связи.

51. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.

52. Телевизионные системы наблюдения.

53. Приборы ночного видения.

54. Системы защиты информации по оптическому каналу.

55. Технические средства для уничтожения информации и носителей информации, порядок применения.

56. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.

57. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.

58. Этапы эксплуатации технических средств защиты информации.

59. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.

60. Установка и настройка технических средств защиты информации.

61. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации

62. Характеристики потенциально опасных объектов.

63. Содержание и задачи физической защиты объектов информатизации.

64. Основные понятия инженерно-технических средств физической защиты.

65. Категорирование объектов информатизации.

66. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.

67. Особенности задач охраны различных типов объектов.

68. Общие принципы обеспечения безопасности объектов.

69. Жизненный цикл системы физической защиты.

70. Принципы построения интегрированных систем охраны.

71. Классификация и состав интегрированных систем охраны.

72. Требования к инженерным средствам физической защиты.

73. Информационные основы построения системы охранной сигнализации.

74. Назначение, классификация технических средств обнаружения.

75. Построение систем обеспечения безопасности объекта.

76. Периметровые средства обнаружения: назначение, устройство, принцип действия.

77. Объектовые средства обнаружения: назначение, устройство, принцип действия.

78. Аналоговые и цифровые системы видеонаблюдения.

79. Назначение системы телевизионного наблюдения.

80. Состав системы телевизионного наблюдения.

81. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.

82. Периметровые и объектовые средства обнаружения, порядок применения.

83. Работа с периферийным оборудованием системы контроля и управления

доступом.

84. Особенности организации пропускного режима на КПП.

85. Управление системой телевизионного наблюдения с автоматизированного рабочего места.

86. Порядок применения устройств отображения и документирования информации.

87. Управление системой воздействия.

88. Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.

89. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.

90. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.

91. Организация ремонта технических средств физической защиты.

92. Предмет и задачи технической защиты информации.

93. Характеристика инженерно-технической защиты информации как области информационной безопасности.

94. Системный подход при решении задач инженерно-технической защиты информации.

95. Основные параметры системы защиты информации.

96. Задачи и требования к способам и средствам защиты информации техническими средствами.

97. Принципы системного анализа проблем инженерно-технической защиты информации.

98. Классификация способов и средств защиты информации.

99. Демаскирующие признаки объектов наблюдения, сигналов и веществ.

100. Понятие об опасном сигнале. Источники опасных сигналов.

101. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.

102. Понятие и особенности утечки информации.

103. Структура канала утечки информации.

104. Классификация существующих физических полей и технических каналов утечки информации.

105. Характеристика каналов утечки информации.

106. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.

107. Классификация технических средств разведки.

108. Методы и средства технической разведки.

109. Средства несанкционированного доступа к информации.

110. Средства и возможности оптической разведки.

111. Средства дистанционного съема информации.

112. Физические основы побочных электромагнитных излучений и наводок.

113. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок.

114. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.

115. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей.

116. Скрытие речевой информации в каналах связи.

117. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.

118. Технические средства акустической разведки.

119. Непосредственное подслушивание звуковой информации. Прослушивание

информации направленными микрофонами.

120. Система защиты от утечки по акустическому каналу.

121. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.

122. Негласная запись информации на диктофоны. Системы защиты от диктофонов.

123. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.

124. Системы защиты информации от утечки по вибрационному каналу.

125. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.

126. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок.

Системы защиты от утечки по электромагнитному каналу.

127.Характеристика инженерно-технической защиты информации как области информационной безопасности.

128. Системный подход при решении задач инженерно-технической защиты информации.

129. Основные параметры системы защиты информации.

130. Задачи и требования к способам и средствам защиты информации техническими средствами.

131. Принципы системного анализа проблем инженерно-технической защиты информации.

132. Классификация способов и средств защиты информации.

133. Демаскирующие признаки объектов наблюдения, сигналов и веществ.

134. Понятие об опасном сигнале. Источники опасных сигналов.

135. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.

136. Понятие и особенности утечки информации.

137. Структура канала утечки информации.

138. Классификация существующих физических полей и технических каналов утечки информации.

Характеристика каналов утечки информации.

138. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.

139. Классификация технических средств разведки.

Характеристики потенциально опасных объектов.

140. Содержание и задачи физической защиты объектов информатизации.

141. Основные понятия инженерно-технических средств физической защиты.

142. Категорирование объектов информатизации.

143. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.

144. Особенности задач охраны различных типов объектов.

145. Общие принципы обеспечения безопасности объектов.

146. Жизненный цикл системы физической защиты.

147. Принципы построения интегрированных систем охраны.

148. Классификация и состав интегрированных систем охраны.

149. Требования к инженерным средствам физической защиты.

150. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.

Критерии оценки

Отметкой «отлично» оцениваются ответы, которые показывают прочные знания основных понятий и задач изучаемой дисциплины, отличаются глубиной и полнотой раскрытия вопросов; владение терминологическим аппаратом; умение давать определения, описывать последовательность технологий материалов, их особенности, делать выводы и обобщения, давать аргументированные ответы, приводить примеры.

Отметкой «хорошо» оцениваются ответы, обнаруживающие прочные знания основных понятий и задач изучаемой дисциплины, отличаются глубиной и полнотой раскрытия вопросов; владение терминологическим аппаратом; умение давать определения, описывать последовательность технологий материалов, их особенности, делать выводы и обобщения, приводить примеры. Однако допускаются две-три неточности в ответах.

Отметкой «удовлетворительно» оцениваются ответы, свидетельствующие в основном о знании материалов, их свойств, технологий, но отличающиеся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа тем изучаемой дисциплины, недостаточным умением давать аргументированные ответы и приводить примеры. Допускается несколько ошибок в содержании ответа.

Отметкой «неудовлетворительно» оцениваются ответы, обнаруживающие незнание материалов, их свойств, технологий изучаемой предметной области, отличающиеся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа тем изучаемой дисциплины; неумением давать аргументированные ответы. Допускаются серьезные ошибки в содержании ответов.

ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Задание 1.

Опишите способы непосредственного воздействия на носители защищаемой информации. Приведите способы вывода из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи. Опишите виды дестабилизирующего воздействия на защищаемую информацию со стороны источника воздействия — технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи.

Задание № 2

Составьте документацию на заданное контролируемое помещение, определите возможные разведопасные направления и возможные виды разведки. Составьте план проведения визуального осмотра помещения и выявите объекты, требующие при обследовании использования имеющихся средств видеонаблюдения.

Задание № 3

Какие виды электрических полей существуют в природе? Каким образом электрические заряды взаимодействуют друг с другом? Назовите источники электрических полей и способы его обнаружения. От чего зависит характер электромагнитного поля в той или иной точке пространства? В чем сущность явления электромагнитной индукции? На какие зоны и по какому принципу подразделяется пространство вокруг источника электромагнитного поля?

Задание № 5

Перечислите типы устройств, используемых для перехвата информации с различных типов кабелей. Приведите основные причины утечки информации в волоконно-оптических линиях. Опишите основные причины излучения световой энергии в окружающее пространство в местах соединения оптических волокон. Приведите примеры технических средств защиты от утечки информации по проводному каналу

Задание № 5

Перечислите типы устройств, используемых для перехвата информации с различных типов кабелей. Приведите основные причины утечки информации в волоконно-оптических линиях. Опишите основные причины излучения световой энергии в окружающее пространство в местах соединения оптических волокон. Приведите примеры технических средств защиты от утечки информации по проводному каналу.

Задание № 6

Что является основой анализа разборчивости речевой информации? Каков диапазон уровней человеческой речи? Какие звуки являются наиболее информативными с точки зрения разборчивости речевой информации? На каком расстоянии от источника производится измерение уровней речи? Что используют для количественной оценки качества перехваченной речевой информации? Приведите примеры технических средств защиты от утечки по виброакустическому каналу.

Задание № 7

Опишите способы перехвата побочных электромагнитных излучений технических средств передачи, обработки, информации ограниченного доступа (ТСПИ). Приведите методы защиты информации от ПЭМИН. Опишите технологию исследования ПЭМИН-монитора.

Задание № 8

Опишите варианты утечки информации по цепям заземления и электропитания. Приведите меры по предотвращению утечки защищаемой информации по цепям заземления и электропитания. Опишите принцип действия прибора РНИ-1.1

Задание № 9

Назовите и охарактеризуйте пассивные технические средства защиты телефонной линии. Как осуществляется контроль состояния телефонной линии и обнаружение атак? Приведите методы активной защиты информации в телефонных линиях. Опишите

технологию защита речевой информации в IP-телефонии.

Задание № 10

Опишите оптические каналы утечки информации, способы получения информации в оптическом канале. Опишите технологию работы телевизионных систем наблюдения.

Задание 11.

Определите, к какому типу относится заданный объект, виды и масштабы возможного ущерба в результате нарушения безопасности, категорию заданного объекта по уровню важности в соответствии с ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) «Системы тревожной сигнализации», содержание и местонахождение защищаемых ресурсов на заданном объекте. Постройте план объекта, выделите защищаемые зоны на плане.

Задание 12.

Постройте пространственную модель заданного объекта защиты. Проанализируйте характеристики технической укрепленности объекта защиты. Проанализируйте защищаемую информацию и проведите её структурирование. Определите пожаро - и взрывоопасность данного объекта, что осуществляется в соответствии с Федеральным законом № 117-ФЗ от 10 июля 2012 г.

«Технический регламент о требованиях пожарной безопасности».

Задание 13.

Сформируйте перечень требований к системе физической защиты заданного объекта. Составьте таблицы требований к физическим средствам защиты заданного объекта информатизации в соответствии с РД 78.36.003-2002 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств». Определите количество рубежей защиты для заданного объекта.

Задание 14.

Сформируйте перечень требований к системе физической защиты заданного объекта. Составьте таблицы требований к физическим средствам защиты заданного объекта информатизации в соответствии с РД 78.36.003-2002 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств». Определите количество рубежей защиты для заданного объекта.

Задание 15.

Проведите выбор и обоснование охранных извещателей для заданного объекта. Какие факторы влияют на выбор средств обнаружения? Приведите их характеристики. Разработайте схему размещения средств подсистемы обнаружения на объекте.

Задание 16.

Проведите выбор и обоснование пожарных извещателей для заданного объекта. Какие факторы влияют на выбор пожарной сигнализации? Приведите их характеристики. Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы пожарной сигнализации.

Задание 17.

Проведите выбор и обоснование средств оповещения для заданного объекта. Какие факторы влияют на выбор средств оповещения? Приведите их характеристики. Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы охранной сигнализации.

Задание 18.

Приведите примеры программно-аппаратных систем аутентификации. Опишите назначение и возможности персонального средства аутентификации и хранения данных в Token. Приведите характеристики USB-ключей. Опишите функции комбинированных устройств аутентификации.

Задание 19.

Опишите основные компоненты системы контроля и управления доступом. Приведите характеристики карт пользователей. Опишите назначение и технологию

управления шлюзами. Опишите технологию идентификации и регистрации транспортных средств антенным считывателем SmartPass. Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы контроля и управления доступом.

Задание 20.

Опишите устройство и принципы работы IP-камеры. Каково назначение и основные характеристики видеорегистраторов? Приведите характеристики сетевого видеорегистратора DVR. Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы видеонаблюдения.

Задание 21.

Опишите состав современных систем сбора и обработки информации. Приведите схему. Приведите алгоритмы расчета показателей надежности систем сбора и обработки информации. Опишите возможности системы сбора и обработки информации ОРИОН.

Задание № 22

Опишите способы непосредственного воздействия на носители защищаемой информации. Приведите способы вывода из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи. Опишите виды дестабилизирующего воздействия на защищаемую информацию со стороны источника воздействия — технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи.

Задание № 23

Составьте документацию на заданное контролируемое помещение, определите возможные разведопасные направления и возможные виды разведки. Составьте план проведения визуального осмотра помещения и выявите объекты, требующие при обследовании использования имеющихся средств видеонаблюдения.

Задание № 24

Какие виды электрических полей существуют в природе? Каким образом электрические заряды взаимодействуют друг с другом? Назовите источники электрических полей и способы его обнаружения. От чего зависит характер электромагнитного поля в той или иной точке пространства? В чем сущность явления электромагнитной индукции? На какие зоны и по какому принципу подразделяется пространство вокруг источника электромагнитного поля? Каково назначение экранирования в системах обработки и передачи информации? Расскажите об экранировании электрических полей (типы полей, диапазон частот). Какие способы уменьшения паразитной емкости при экранировании низкочастотных электрических полей Вам известны? Как взаимосвязаны толщина и магнитная проницаемость экрана? Из каких материалов изготавливают экраны против высокочастотных магнитных полей? На каком принципе осуществляется экранирование высокочастотных магнитных полей?

Задание № 25

Перечислите типы устройств, используемых для перехвата информации с различных типов кабелей. Приведите основные причины утечки информации в волоконно-оптических линиях. Опишите основные причины излучения световой энергии в окружающее пространство в местах соединения оптических волокон. Приведите примеры технических средств защиты от утечки информации по проводному каналу.

Задание № 26

Что является основой анализа разборчивости речевой информации? Каков диапазон уровней человеческой речи? Какие звуки являются наиболее информативными с точки зрения разборчивости речевой информации? На каком расстоянии от источника производится измерение уровней речи? Что используют для количественной оценки качества перехваченной речевой информации? Приведите примеры технических средств защиты от утечки по виброакустическому каналу.

Задание № 27

Опишите способы перехвата побочных электромагнитных излучений технических

средств передачи, обработки, информации ограниченного доступа (ТСПИ). Приведите методы защиты информации от ПЭМИН. Опишите технологию исследования ПЭМИН-монитора.

Задание № 28

Опишите варианты утечки информации по цепям заземления и электропитания. Приведите меры по предотвращению утечки защищаемой информации по цепям заземления и электропитания. Опишите принцип действия прибора РНИ-1.1

Задание № 29

Назовите и охарактеризуйте пассивные технические средства защиты телефонной линии. Как осуществляется контроль состояния телефонной линии и обнаружение атак? Приведите методы активной защиты информации в телефонных линиях. Опишите технологию защита речевой информации в IP-телефонии.

Опишите оптические каналы утечки информации, способы получения информации в оптическом канале. Опишите технологию работы телевизионных систем наблюдения.

Задание 30.

Определите, к какому типу относится заданный объект, виды и масштабы возможного ущерба в результате нарушения безопасности, категорию заданного объекта по уровню важности в соответствии с ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) «Системы тревожной сигнализации», содержание и местонахождение защищаемых ресурсов на заданном объекте. Постройте план объекта, выделите защищаемые зоны на плане.

Задание 31.

Постройте пространственную модель заданного объекта защиты. Проанализируйте характеристики технической укрепленности объекта защиты. Проанализируйте защищаемую информацию и проведите её структурирование. Определите пожаро- и взрывоопасность данного объекта, что осуществляется в соответствии с Федеральным законом № 117-ФЗ от 10 июля 2012 г.

«Технический регламент о требованиях пожарной безопасности».

Задание 32.

Сформируйте перечень требований к системе физической защиты заданного объекта. Составьте таблицы требований к физическим средствам защиты заданного объекта информатизации в соответствии с РД 78.36.003-2002 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств». Определите количество рубежей защиты для заданного объекта.

Задание 33.

Проведите выбор и обоснование охранных извещателей для заданного объекта. Какие факторы влияют на выбор средств обнаружения? Приведите их характеристики. Разработайте схему размещения средств подсистемы обнаружения на объекте.

Задание 34.

Проведите выбор и обоснование пожарных извещателей для заданного объекта. Какие факторы влияют на выбор пожарной сигнализации? Приведите их характеристики. Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы пожарной сигнализации.

Задание 35.

Проведите выбор и обоснование средств оповещения для заданного объекта. Какие факторы влияют на выбор средств оповещения? Приведите их характеристики. Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы охранной сигнализации.

Задание 36.

Приведите примеры программно-аппаратных систем аутентификации. Опишите назначение и возможности персонального средства аутентификации и хранения данных eToken. Приведите характеристики USB-ключей. Опишите функции комбинированных устройств аутентификации.

Задание 37.

Опишите основные компоненты системы контроля и управления доступом. Приведите характеристики карт пользователей. Опишите назначение и технологию управления шлюзами. Опишите технологию идентификации и регистрации транспортных средств антенным считывателем SmartPass. Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы контроля и управления доступом.

Задание 38. Опишите устройство и принципы работы IP-камеры. Каково назначение и основные характеристики видеорегистраторов? Приведите характеристики сетевого видеорегистратора DVR. Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы видеонаблюдения.

Задание 39.

Опишите состав современных систем сбора и обработки информации. Приведите схему. Приведите алгоритмы расчета показателей надежности систем сбора и обработки информации. Опишите возможности системы сбора и обработки информации ОРИОН.

ЗАДАНИЯ К КВАЛИФИКАЦИОННОМУ ЭКЗАМЕНУ

ЗАДАНИЕ 1.

Инструкция

Внимательно прочитайте задание.

Текст задания:

ООО «Киновидеопрокат», является почти полным монополистом относительно посреднических услуг в сфере кинобизнеса. Отдел маркетинга, изучив ситуацию на рынке кинофильмов, принимает решение о покупке

тех или иных кинолент. Отдел закупок претворяет эти решения в жизнь,

причем лента может быть куплена как у производителя, так и у посредника. Отдел аренды «Киновидеопроката» сдает закупленные фильмы кинотеатрам города в аренду. В связи с возникающей больший конкуренцией охране и защите коммерческих секретов уделено усиленное внимание.

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии, который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформируйте таблицу №1 Данных о защищаемой информации.

Используя Corel DRAW произведите моделирование объектов защиты.

ЗАДАНИЕ 2.

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

Торгово-посреднической фирмы «Столица». Бизнес этого предприятия предельно прост: «покупай дешевле – продавай дороже», или состыкуй продавца и покупателя и получи «комиссионные». Основной упор фирма делает на закупки продуктов питания в других регионах страны и за рубежом – там, где они производятся и стоят дешевле, чем в нашем регионе. Часть продукции может быть закуплена и у местных продавцов. В этом случае фирма получает прибыль за счет того, что крупные партии товара стоят дешевле, чем мелкие. Так как в данной сфере количество фирм на сегодняшний день увеличивается, то маркетинговой политики предприятия охраняется как службой безопасности, так и лично руководством.

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии, который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 Данных о защищаемой информации.

Используя Corel DRAW произведите моделирование объектов защиты.

ЗАДАНИЕ 3.

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

Рассмотреть работу отдела кадров университета, в которой находятся данные всех сотрудников: от преподавателя до ректора, и их трудовой деятельности. Также в отделе кадров хранится информация о трудовой деятельности сотрудника: о предыдущих местах работы, сроке работы

и предприятии. Отдел кадров занимается подготовкой трудовых договоров

с преподавателями после избрания их по конкурсу на очередной срок.

Также в его ведении находятся сведения о наложении взысканий на сотрудников и их поощрениях, часть данных не имеет общего права доступа. Взыскания в трудовую книжку не заносятся, а хранятся в электронном виде.

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии, который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 Данных о защищаемой информации.

Используя Corel DRAW произведите моделирование объектов защиты.

ЗАДАНИЕ 4.

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

Фармацевтическая компания занимается производством и оптовой продажей лекарств больницам и аптекам города. В ее ассортименте – тысячи наименований лекарств, а также различных аптечных принадлежностей (градусники, шприцы, бинты и т. д.) Возможна продажа лишь тех лекарств, которые одобрены Минздравом РФ, т. е. имеют регистрационный номер Минздрава РФ. Поступающие лекарства сопровождаются документами – приходными накладными ведомостями. Имеются наркосодержащие лекарства, доступ к работе с ними имеют возможности, только работники, имеющие допуск. Допуск к данным о сроках покупок и доставок такой продукции строго ограничен, склады с такими лекарствами охраняются службой безопасности, также усилено охраняется рецептура производимых лекарств.

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии, который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 Данных о защищаемой информации.

Используя Corel DRAW произведите моделирование объектов защиты.

ЗАДАНИЕ 5.

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

Туристическая компания «Вояж» формирует туристические группы для заграничных поездок и обеспечивает им полную поддержку на маршруте. Количество туристов в группе заранее известно и ограничено.

Маршрут группы может пролегать через несколько городов страны назначения. Вместе с группой следует представитель компании, который несет полную ответственность за качество услуг, предоставляемых компанией. Так как в данной сфере количество фирм на сегодняшний день увеличивается, то сохранностью и невозможностью легкого доступа к сведениям относительно туристов, а также сведения договоров охраняется как службой безопасности, так и лично руководством.

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии, который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 Данных о защищаемой информации.

Используя Corel DRAW произведите моделирование объектов защиты.

ЗАДАНИЕ 6.

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

В собственности рекламного агентства «Rapid» находится примерно около сотни рекламных щитов, расположенных по всему городу. Установка их согласована с администрацией города, и все необходимые формальности выполнены. На этих щитах может быть размещена реклама по заказу любой организации города. Срок размещения, стоимость аренды щита и стоимость изготовления самой рекламы – договорные, условия договора строго конфиденциальны и индивидуальны для каждого партнера.

Договор размещения рекламы может быть продлен по взаимной договоренности сторон.

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии, который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 Данных о защищаемой информации.

Используя Corel DRAW произведите моделирование объектов защиты.

ЗАДАНИЕ 7.

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

ООО «Центр оценки и продажи недвижимости» занимается организацией покупки и продажа квартир. Центр оценки имеет большой штат специалистов, позволяющий этой организации проводить сделки купли-продажи на высоком профессиональном уровне. Владелец квартиры, желающий ее продать, заключает договор с Центром, в котором указывается сумма, срок продажи и процент отчислений в пользу Центра оценки и продажи недвижимости в случае успешного проведения сделки. Все сделка проходят строго конфиденциально, все условия договора индивидуальны для каждого клиента.

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии, который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 Данных о защищаемой информации.

Используя Corel DRAW произведите моделирование объектов защиты.

ЗАДАНИЕ 8.

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

Отдел вневедомственной охраны квартир обеспечивает электронную охрану квартир граждан в одном районе города. Для установки охранной сигнализации требуется наличие квартирного телефона. Условия установки системы охраны, ее свойства и методы оговариваются в договоре, условия договора строго конфиденциальны и индивидуальны для каждого партнера

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии, который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 Данных о защищаемой информации.

Используя Corel DRAW произведите моделирование объектов защиты.

ЗАДАНИЕ 9.

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

Промышленное предприятие (условно ОАО «Маяк»), специализирующееся на производстве пластмассовых труб, которые по своим качествам пользуются большим спросом. Охрана и защита коммерческих секретов, связанных с технологией производства труб, находятся в центре внимания руководства и службы безопасности предприятия. Предприятие имеет административную зону, где расположены управленческие структуры, производственную н складскую зоны. Все эти зоны разделены заборами. Предприятие имеет широкий круг партнеров, клиентов (в том числе и за рубежом). В сфере деятельности предприятия часто возникают конфликтные ситуации с конкурентами и спорные вопросы с органами местной власти по земельным н финансовым вопросам.

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Разработайте и обоснуйте систему видеонаблюдения административной зоны.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии, который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 Данных о защищаемой информации.

Используя Corel DRAW произведите моделирование объектов защиты.

ЗАДАНИЕ 10.

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

Детективное агентство предлагает частным лицам и организациям услуги специалистов сыскного дела. Опытные детективы с юридическим образованием окажут помощь в получении любых нужных вам сведений с неопровержимыми доказательствами их правдивости. На абсолютно законных основаниях. Полная конфиденциальность сведений, полученных от клиента в ходе расследования дела. Неразглашение имени заказчика кому бы то ни было. Сохранение тайны обращения в детективное агентство.

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии, который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 Данных о защищаемой информации.

Используя Corel DRAW произведите моделирование объектов защиты.

ЗАДАНИЕ 11.

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

Научно-внедренческого предприятия «Звезда» занимается прокладкой компьютерных сетей и разработкой программных комплексов для организаций нашего города. Численность работников в «Звезде» – примерно 80 человек. Одновременно находится в разработке до 30 проектов. Один разработчик может участвовать в нескольких проектах одновременно, степень секретности для каждого проекта индивидуальна. Одна организация может заказать в «Звезде» несколько разработок. В связи с большей востребованностью создаваемых программных продуктов, а также с появлением новых конкурирующих фирм, предоставляющих аналогичные услуги, охране и защите коммерческих секретов уделено усиленное внимание.

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии, который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 Данных о защищаемой информации.

Используя Corel DRAW произведите моделирование объектов защиты.

ЗАДАНИЕ 12.

Инструкция

1. Внимательно прочитайте задание.

Текст задания:

Судоходной компании «Балтика» занимается перевозками грузов между континентами. В ее собственности несколько десятков судов различного класса и грузоподъемности. К услугам этой компании обращаются тысячи клиентов из различных стран мира. Судно следует по маршруту. Маршрут разрабатывается главным менеджером

компании и проходит через несколько портов. В очередном порту назначения производится лишь частичная погрузка и выгрузка грузов, и судно следует дальше. Компания имеет в своей собственности складские зоны. Все эти зоны разделены между собой. В связи с большим количеством конкурирующих фирм, охране и защите коммерческих секретов, связанных со статусом груза и маршрутом следования, уделено усиленное внимание.

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии, который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 Данных о защищаемой информации.

Используя Corel DRAW произведите моделирование объектов защиты.

Техническая защита информации

Задание №1

Физические средства защиты информации

Выберите один из 4 вариантов ответа:

1) средства, которые реализуются в виде автономных устройств и систем

2) устройства, встраиваемые непосредственно в аппаратуру, АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу

3) это программы, предназначенные для выполнения функций, связанных с защитой информации

4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

Задание №2

Технические средства защиты информации

Выберите один из 4 вариантов ответа:

1) средства, которые реализуются в виде автономных устройств и систем

2) устройства, встраиваемые непосредственно в аппаратуру, АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу

3) это программы, предназначенные для выполнения функций, связанных с защитой информации

4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

Задание №3

Утечка информации

Выберите один из 3 вариантов ответа:

1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу

2) ознакомление постороннего лица с содержанием секретной информации

3) потеря, хищение, разрушение или неполучение переданных данных

Задание №4

Под изоляцией и разделением (требование к обеспечению ИБ) понимают

Выберите один из 2 вариантов ответа:

1) разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов)

2) разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп

Задание №5

Виды технической разведки (по месту размещения аппаратуры)

Выберите несколько из 7 вариантов ответа:

1) космическая
2) оптическая
3) наземная
4) фотографическая
5) морская
6) воздушная
7) магнитометрическая

Задание № 6

Основные группы технических средств ведения разведки

Выберите несколько из 5 вариантов ответа:

1) радиомикрофоны
2) фотоаппараты
3) электронные "уши"
4) дистанционное прослушивание разговоров
5) системы определения местоположения контролируемого объекта

Задание №7

Инженерно-техническая защита –это

Запишите ответ_____

Задание № 8

Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется

Выберите один из 4 вариантов ответа:

1) угрозой;
2) опасностью;
3) намерением;
4) предостережением.

Задание №9

Какая угроза возникает в результате технологической неисправности за пределами информационной системы?

Запишите ответ:

_____

Задание № 10

Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

Выберите один из 4 вариантов ответа:

1) операционной системы, сетевого программного обеспечения
2) операционной системы, сетевого программного обеспечения и системы управления базами данных;
3) операционной системы, системы управления базами данных;
4) сетевого программного обеспечения и системы управления базами данных.

Задание №11

Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется

Выберите один из 4 вариантов ответа:

1) системой угроз;
2) системой защиты;
3) системой безопасности;
4) системой уничтожения.

Задание №12

К угрозам какого характера относятся действия, направленные на сотрудников компании или осуществляемые сотрудниками компании с целью получения конфиденциальной информации или нарушения функции бизнес-процессов?

Запишите ответ:

_____

Задание №13

Выделите группы, на которые делятся средства защиты информации:

Выберите один из 3 вариантов ответа:

1) физические, аппаратные, программные, криптографические, комбинированные;
2) химические, аппаратные, программные, криптографические, комбинированные;
3) физические, аппаратные, программные, этнографические, комбинированные;

Задание №14

По функциональному назначению средства инженерно-технической защиты делятся на следующие группы:

Продолжите ответ_____

Задание №15

Надежным средством отвода наведенных сигналов на землю служит Запишите ответ:

_____

Задание № 16

Установите соответствие

Укажите соответствие для всех 2 вариантов ответа:

1) наука о скрытой передаче информации путем сохранения в тайне самого факта передачи

2) наука, скрывающая содержимое секретного сообщения

__ стеганография

__ криптография

Задание №17

Контроль доступа к информации обеспечивается последовательным использованием таких методов защиты информации…

Продолжите _____

Задание №18

Технический канал утечки информации…

Продолжите_____

Задание №19

Укажите соответствие для всех 4 вариантов ответа:

1) это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок

2) это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов

3) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей

4) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии

__ защита информации от утечки по акустическому каналу
__ Защита информации от утечки по визуально-оптическому каналу
__ Защита информации от утечки по электромагнитным каналам
__ Защита информации от утечки по материально-вещественному каналу

Задание №20

Разновидности угроз безопасности

Выберите несколько из 6 вариантов ответа:

1) техническая разведка
2) программные
3) программно-математические
4) организационные
5) технические
6) физические

Итоговый тест МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации

Задание №1

Создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи относится к:

1. правовым методам защиты информации
2. организационно-техническим методам защиты информации
3. организационно-распорядительным методам защиты информации
4. экономическим методам защиты информации

Задание №2

Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией, называется:

1. собственник информации
2. владелец информации
3. пользователь

Задание №3

Форма допуска, требуемая для работы со сведениями особой важности, является:

1. первой формой допуска
2. второй формой допуска
3. третьей формой допуска

Задание №4

Форма допуска, требуемая для работы с совершенно секретными сведениями, является:

1. первой формой допуска
2. второй формой допуска
3. третьей формой допуска

Задание №5

Форма допуска, требуемая для работы с секретными сведениями, является:

1. первой формой допуска
2. второй формой допуска
3. третьей формой допуска

Задание №6

В сфере государственной тайны действует функционально-зональный принцип. Это значит, что:

1. каждый пользователь допускается должностными лицами только к такой информации, которая требуется ему для исполнения должностных обязанностей
2. каждый пользователь допускается должностными лицами только к информации, касающейся зоны его проживания
3. каждый пользователь допускается должностными лицами ко всей информации, к которой у него есть форма допуска

Задание №7

Противоправные процессы утечки, утраты, распространения, разглашения, копирования, тиражирования, фальсификации, хранения с целью передачи, удаления информации называется процессом:

1. незаконного оборота информации
2. взлома информации
3. несанкционированного использования информации

Задание №8

Форма преднамеренного распространения или мнимого разглашения (утечки) неких планов и намерений, которые не отвечают реальным действиям называется:

1. дезинформация
2. легендирование
3. шпионаж

Задание № 9

Какое направление защиты в основном применяется для охраны материальных ценностей?

1. инженерно-техническая
2. организационно-техническая
3. организационно-распорядительная
4. нормативно-правовая
5. экономическая

Задание №10

Что из нижеперечисленного оборудования может выступать в качестве технического канала связи?

1. контроллер жесткого диска, передающий электрические импульсы, считанные магниторезистивной головкой с поверхности магнитного носителя, по шлейфу в системную магистраль для копирования в оперативную память
2. инфракрасный светодиод лазерного принтера, посылающий кратковременные
3. вспышки на электризованную поверхность фоточувствительного барабана
4. модулированный по силе тока поток электронов, засвечивающий в определенном
5. порядке пикселы люминофора электронно-лучевой трубки
6. экран компьютерного монитора и глаза пользователя
7. оптический канал связи
8. все варианты могут быть отнесены к техническим каналам связи

Задание №11

Какой канал утечки информации основан на использовании электромагнитной энергии видимого и инфракрасного диапазона?

1. визуально-оптический канал
2. электромагнитный канал
3. виброакустический канал
4. материально-вещественный канал

Задание № 12

Процесс перехвата и фиксации процесса клавиатурного ввода идентифицирующей информации является примером утечки информации:

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

Задание №13

Какой канал утечки информации включает в себя весь радиодиапазон от сверхнизких до сверхвысокочастотных волн?

1. визуально-оптический канал
2. электромагнитный канал
3. виброакустический канал
4. материально-вещественный канал

Задание №14

Электрические сигналы (напряжения, токи), модулированные по закону передаваемого сообщения, протекающие по проводникам и элементам радиоцепей (линиям связи, антеннам, конденсаторам) и возбуждающие в окружающем пространстве электромагнитную энергию является примером утечки информации:

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

Задание №16

Какой канал утечки информации представляет собой фактический побочный прием модулированной акустической энергии, распространяющейся в газообразной, жидкой или твердой средах

1. визуально-оптический канал
2. электромагнитный канал
3. виброакустический канал
4. материально-вещественный канал

Задание №17

Примером какого канала утечки информации служит звук голоса человека?

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

Задание №18

По какому признаку делят на классы средства технической разведки (СТР)?

1. по дальности канала
2. по форме допуска
3. по мощности
4. по степени финансирования

Задание №19

Портативные устройства для запечатления информации, скрытно проносимые на территорию объекта нарушителем на своем теле, относят к …

1. первому классу СРТ
2. второму классу СРТ
3. третьему классу СРТ

Задание № 20

Для наблюдения за объектами информатизации из-за пределов их охраняемой или контролируемой территории используются СРТ…

1. первого класса
2. второго класса
3. третьего класса

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1.Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2020. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711-1. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456793

2.Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456792

3.2.3. Периодические издания:

1.Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

2.Защита информации. Инсайд: Информационно-методический журнал

3.Информационная безопасность регионов: Научно-практический журнал

4.Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/

5.Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/