Приложение 4 Фонд оценочных средств учебных дисциплин
к ОПОП по специальности
10.02.05 Обеспечение информационной
безопасности автоматизированных систем.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

ПМ 03. Защита информации техническими средствами

программы подготовки специалистов среднего звена
по специальности СПО
10.02.05 Обеспечение информационной безопасности автоматизированных

Регистрационный №22ИБ/ 37ФОС

Санкт-Петербург
2022

Фонд оценочных средств по профессиональному модулю ПМ 03. Защита информации техническими средствами составлен на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного Приказом Министерства образования и науки от 09.12.2016 № 1553.

Организация-разработчик:

Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение «Академия промышленных технологий» (СПб ГБОУ «АПТ»)

Разработчик:

Еропкин И.В.- преподаватель учебной цикловой комиссии

Информационных технологий СПб ГБПОУ «АПТ»

Фонд оценочных средств рассмотрен на заседании учебной цикловой комиссии Информационных технологий
ФОС соответствует требованиям к содержанию, структуре, оформлению.

Протокол № 10 от 06.06. 2022

Председатель УЦК Еропкин И.В.

Фонд оценочных средств соответствует требованиям к содержанию, структуре, оформлению.

Фонд оценочных средств одобрен на заседании Педагогического совета и рекомендован к использованию в учебном процессе.
Протокол №1 от 30.08.2022

СОДЕРЖАНИЕ

1. Общие положения

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности Защита информации техническими средствами и составляющих его профессиональных компетенций, а также общие компетенции, формирующиеся в процессе освоения ОПОП в целом.

Формой аттестации по профессиональному модулю является экзамен

Формы контроля и оценивания элементов профессионального модуля

Элемент модуля	**Форма контроля и оценивания**	
	Промежуточная аттестация	**Текущий контроль**
МДК.03.01. Техническая защита информации	Экзамен	Тестирование на ПК Защита практических работ Устный опрос
МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации	Экзамен	Тестирование на ПК Защита практических работ Устный опрос
УП	Диф. зачет	Выполнение практических заданий
ПП	Диф.зачет	Наблюдение за выполнением задания по производственной практике на предприятии (организации); Анализ представленных студентом материалов по этапам программы практики
ПМ	Экзамен квалификационный	

2. Результаты освоения модуля, подлежащие проверке на экзамене по модулю

2.1. В результате аттестации по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций:

Профессиональные и общие компетенции, которые возможно сгруппировать для проверки	**Показатели оценки результата**
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации
ПК 3.3 Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и

Профессиональные и общие компетенции, которые возможно сгруппировать для проверки	Показатели оценки результата
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; знание и использование ресурсосберегающих технологий в
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической	- эффективность вьшолнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;
ОК 9. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.

3. Оценка освоения профессионального модуля

Типовые задания для оценки освоения МДК 03.01. Техническая защита информации

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
1. 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

Типовые практические задания:

1. Оценивается система видеонаблюдения помещения, где расположен сервер;
2. Проверяются помещения, предназначенные для переговоров, на предмет наличия различных подслушивающих устройств;
3. Производится установка специального оборудования, призванного распознавать подслушивающие устройства
4. Организационные меры защиты информации
5. Оценка вероятного противника
6. Оценка условий решения задачи защиты информации
7. Инженерно-технические меры защиты информации

8. Анализ объекта защиты
9. Разработка политики защиты контролируемой зоны
10. Обеспечение защиты помещения проведения совещаний
11. Обеспечение защиты помещения руководителя
12. Обеспечение защиты помещения серверной

Критерии оценивания выполнения практического задания

- рациональное распределение времени по этапам выполнения задания
- обращение в ходе задания к информационным источникам
- знание терминологии
- скорость выполнение
- количество предложенных вариантов решения поставленной задачи.

3.2. Типовые задания для оценки освоения МДК 03.02. Инженерно-технические средства физической защиты объектов информатизации

Список экзаменационных вопросов:

1. Понятие информации. Проблема обеспечения безопасности в информационных системах, политика информационной безопасности.
2. Устройства защиты от утечки информации по радиоканалам, основные методы обнаружения радиозакладок.
3. Физические средства
4. Аппаратные средства
5. Программные средства
6. Криптографические средства
7. Индикаторы поля, акустическая развязка, дифференциальный индикатор поля.
8. Генераторы шума.
9. Особенности работы и основные характеристики сканирующих радиоприемников.
10. Блок-схема типового сканирующего радиоприемника.
11. Автоматизированные комплексы обнаружения радиозакладок. Методы обнаружения локализации в пространстве закладных устройств.
12. Виды модуляции и кодирования передаваемой информации.
13. Амплитудная модуляция. Амплитудная модуляция с подавлением верхней или нижней боковой частоты. Частотная модуляция. Фазовая модуляция.
14. Кодово-импульсная модуляция. Специальные виды модуляции. Основные требования к специальным системам связи.
15. Использование ШПС и ППРЧ сигналов. Основные характеристики.
16. Обнаружители и подавители диктофонов. Назначение. Принципы работы. Основные характеристики.
17. Принципы работы локаторов нелинейностей. Основные методы обнаружения ложных и истинных соединений.
18. Концепции инженерно-технической защиты информации.
19. Системный подход к защите информации.
20. Основные проблемы инженерно-технической защиты информации.
21. Основные концептуальные положения инженерно-технической защиты информации.
22. Направления инженерно-технической защиты информации.
23. Показатели эффективности инженерно-технической защиты информации.
24. Теоретические основы инженерно-технической защиты информации.
2. 5. Источники опасных сигналов.
26. Виды побочных опасных электромагнитных излучений.
27. Характеристика технической разведки.
28. Технические каналы утечки информации.
29. Методы инженерно-технической защиты информации.
30. Методы инженерной защиты и технической охраны объекта.

31. Методы скрытия информации и ее носителей.
32. Физические основы защиты информации.
33. Физические основы побочных электромагнитных излучений и наводок.
34. Распространение сигналов в технических каналах утечки информации.
35. Физические процессы подавления опасных сигналов.
36. Технические средства добывания и инженерно-технической защиты.
37. Средства технической разведки.
38. Средства инженерной защиты и технической охраны.
39. Средства предотвращения утечки информации по техническим каналам.
40. Организационные основы инженерно-технической защиты информации.
41. Государственная система защиты информации.
42. Контроль эффективности инженерно-технической защиты информации.
43. Методическое обеспечение инженерно-технической защиты автоматизированных систем от вредоносных программных воздействий.
44. Моделирование инженерно-технической защиты информации.
45. Методические рекомендации по оценке эффективности защиты информации.

Типовое практическое задание для оценки освоения МДК 03.02 Применение инженерно-технических средств физической защиты объектов информатизации

Инструкция для выполнения задания

Внимательно прочитайте задание.

Время выполнения задания - 45 минут.

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 и 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 и финансовым вопросам.

1. Определите объекты и субъекты системы безопасности предприятия.

2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему видеонаблюдения административной зоны.

Критерии оценки

Выполнение задания

- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.

Подготовленный продукт

- разработанная система видеонаблюдения административной зоны. *Устное обоснование*
- определение объектов и субъектов системы безопасности предприятия;
- определение видов охраны предприятия.

3.3 Комплект материалов для оценки сформированности знаний, умений, практического опыта ПМ.ОЗ Защита информации техническими средствами

Квалификационный экзамен предназначен для контроля и оценки результатов освоения профессионального модуля ПМ.ОЗ Защита информации техническими средствами по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Экзаменационные задания включают выполнение практических заданий, ориентированные на проверку освоения вида деятельности в целом и проверяющие освоение группы компетенций, соответствующих разделам модуля.

Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/не освоен».

Для вынесения положительного заключения об освоении ВПД, необходимо подтверждение сформированности всех компетенций, перечисленных в программе ПМ. При отрицательном заключении хотя бы по одной из профессиональных компетенций принимается решение «вид профессиональной деятельности не освоен».

Теоретические вопросы к экзамену по ПМ. 03 Защита информации техническими средствами:

1. Инженерно-техническая защита информации. Задачи государственной системы защиты информации защиты
2. Структура государственной системы защиты информации. Направления работ по защите информации.
3. Органы государственной системы защиты информации
4. Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты.
5. Понятие о демаскирующих признаках объектов защиты.

6. Характеристики и особенности семантической (смысловой) информации и информации о демаскирующих признаках объекта

7. Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности объектов.

8. Видовые, сигнальные и вещественные демаскирующие признаки.

9. Основные видовые демаскирующие признаки объектов наблюдения. Особенности видовых признаков в оптическом и радиодиапазона.

10. Определение основных характеристик аналоговых и дискретных (импульсных) электрических сигналов, средств связи, радиолокационных станций, лазерных и других излучений.

11. Изучение основных признаков, характеризующие физические и химические
свойства материальных тел. Понятие о демаскирующих объектах, сигналах и веществах.

12. Технические каналы утечки информации.

13. Понятие об опасных сигналах и их источниках.

14. Диагностика основных и вспомогательных технических средств и систем

15. Побочные электромагнитные излучения и наводки.

16. Акустоэлектрические преобразователи, их виды и принципы работы.

17. Принципы высокочастотного навязывания. Высокочастотные и низкочастотные побочные излучения технических средств и систем (ТСС).

18. Паразитная генерация усилителей. Виды паразитных связей между цепями ТСС.

19. Исследование паразитных наводок в цепях электропитания, заземления, в токопроводящих конструкциях помещений и зданий

20. Характеристики каналов утечки информации.

21. Структура технических каналов утечки информации.

22. Виды технических каналов утечки информации.

23. Основные характеристики технических каналов утечки информации.

24. Способы комплексного использования злоумышленниками технических каналов утечки информации

25. Оптические каналы утечки информации. Структура оптического канала утечки информации.

26. Характеристики среды распространения оптических лучей. Основные показатели оптоэлектронных линий связи и способы снятия с них информации.

27. Радиоэлектронные каналы утечки информации. Особенности радиоэлектронных каналов утечки информации. Виды и структура радиоэлектронных каналов утечки информации.

28. Особенности распространения радиоволн различных диапазонов частот. Способы повыппения дальности передачи информации в ультракоротком диапазоне радиоволн.

29. Классификация и характеристики помех в радиоэлектронных каналах утечки информации

30. Диагностика акустических каналов утечки информации.

31. Структура акустического канала утечки информации.

32. Отражение и поглощение акустических волн в среде распространения.

33. Понятие о реверберации и влияние времени реверберации на разборчивость речи.

34. Материально-вещественные каналы утечки информации.

35. Анализ способов утечки демаскирующих веществ в твердом, жидком и газообразном виде.

36. Виды потенциальных угроз безопасности информации. Преднамеренные и случайные воздействия на источники информации

37. Технические каналы утечки речевой информации. Технические каналы утечки информации при передачи ее по каналам связи

38. Электрические каналы утечки информации. Электромагнитные каналы утечки информации

39. Средства нейтрализации угроз и управления физической защитой

40. Средства инженерной защиты. Инженерные конструкции

41. Ограждения территорий, зданий, помещений. Двери, окна, ворота. Металлические сейфы, хранилища. Запирающие устройства

42. Устройства ввода идентификационных признаков. Магнитные карты доступа. Проксимити-карты

43. Биометрические характеристики человека.

44. Устройства управления и исполнения. Турникеты, шлагбаумы, шлюзовые кабины, блокираторы

45. Направленные микрофоны, виды, сравнение характеристик. Диктофоны и стетоскопы.

46. Сканирующие приемники. Нелинейные локаторы. Подавители сигналов

47. Приемно-контрольные приборы. Ретрансляторы.

48. Пульты централизованной охраны.

49. Радиоканальные системы охраны и оповещения. GSM, Internet оповещение

50. Принципы функционирования средств видеонаблюдения. Определение характеристик используемых камер и объективов.

51. Средства отображения видеоинформации. Средства регистрации, хранения и
архивации данных. Освещение

52. Системы охранно-тревожной сигнализации. Система пожарной сигнализации

53. Звукоизоляция и звукопоглощение.

54. Диагностика побочных преобразований акустической волны в электрический сигнал.

55. Средства обнаружения, локализации и подавления радиоизлучающих устройств.

56. Средства контроля проводных систем передачи информации.

Билет №1

Практическое задание

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 больший востребованностью создаваемых программных продуктов, а также с появлением новых конкурирующих фирм, предоставляющих аналогичные услуги, охране и защите коммерческих секретов уделено усиленное внимание.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а п- 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).
4. Создайте модель защиты в Corel DRAW.

Билет №2

Практическое задание

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.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.

3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а п-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).
4. Создайте модель защиты в Corel DRAW.

Билет №3

Практическое задание

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.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а п-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).
4. Создайте модель защиты в Corel DRAW.

Билет №4

Практическое задание

Торгово-посредническая фирма «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.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а п-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).
4. Создайте модель защиты в Corel DRAW.

Билет №5

Практическое задание

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.

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.

3. Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а п-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).
4. Создайте модель защиты в Corel DRAW.

4.Требования к минимальному материально-техническому обеспечению Лаборатории технических средств защиты информации

Оборудование учебного кабинета: доска, 15 автоматизированных рабочих мест для студентов: столы-15 шт., стулья -15 шт., ПК-15 шт., автоматизированное рабочее место для преподавателя - 1 шт., сканер-1 шт., принтер-1 шт., проектор - 1шт., экран - 1 шт.; программное обеспечение общего и профессионального назначения, лабораторные учебные макеты.

Основное оборудование: учебно-методическая документация; аппаратные средства аутентификации пользователя.

4.1. Информационное обеспечение

4.1.1. Основные печатные источники:

1. Гребенюк Е. И., Гребенюк Н. А. Технические средства информатизации. Учебник для СПО М.: ИЦ Академия,2020 - 352 с.
2. Техническая защита информации в объектах информационной инфраструктуры (1-е изд.) учебник Бубнов А.А.,М.: ИЦ Академия, 2019 - 272 с.

4.1.2. Дополнительные печатные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.
2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2 Организационное обеспечение информационной безопасности: учеб, пособие. - М.: МИЭТ, 2013- 172 с.
4. Организационно-правовое обеспечение Информационной безопасности: учеб, пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. - М.: Издательский центр «Академия», 2017-336с
5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
8. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
9. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
10. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

11. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
12. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
13. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
14. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
15. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
16. 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.
17. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
18. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
19. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
20. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России
21. от 30 августа 2002 г. № 282.
22. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
23. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России
24. от 31 августа 2010 г. № 416/489.
25. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

26. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
27. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода- вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
28. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
29. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
30. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
31. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
32. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
3. 6. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
37. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
38. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
39. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
40. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
41. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
42. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
43. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

44. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
45. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
47. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
48. Номенклатура показателей качества. Ростехрегулирование, 2005.
49. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
50. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
51. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
52. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
53. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
54. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
55. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
56. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
57. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
58. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

59. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
60. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
61. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

3.2.3 Электронные ресурсы

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.
https://urait.ru/bcode/456793
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с.
https://urait.ru/bcode/449548
3. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с.
https://urait.ru/bcode/451933
4. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
5. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
6. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
7. Справочно-правовая система «Консультант Плюс» www.consultant.ru
8. Справочно-правовая система «Гарант» » www.garant.ru
9. Федеральный портал «Российское образование www.edu.ru
10. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
11. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения СПб ГБПОУ «АПТ» https://c2298.c.3072.ru/