МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Югорский государственный университет» (ЮГУ)
НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(НефтИн (филиал) ФГБОУ ВО «ЮГУ»)

РАССМОТРЕНО
На заседании ПЦК ЭТД
Протокол № 7 «31» августа_2022г.
Председатель ПЦК
_____ Тен М.Б.

УТВЕРЖДАЮ
Зам. директора по УВР
НефтИн (филиал) ФГБОУ ВО «ЮГУ»
«31» августа 2022 г.
_____Хайбулина Р.И

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

КОМПЛЕКТ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ
МАТЕРИАЛОВ ПО МЕЖДИСЦИПЛИНАРНОМУ КУРСУ

МДК 03.02. ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ

ИНФОРМАТИЗАЦИИ

(наименование МДК)

программы подготовки специалистов среднего звена (ППССЗ)

по специальности СПО

10.02.05 Обеспечение информационной безопасности автоматизированных систем

(код, наименование)

базовой подготовки

г. Нижневартовск

-2022-

Комплект контрольно-измерительных материалов по МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации программы подготовки специалистов среднего звена (ППССЗ) по специальности СПО 10.02.05Обеспечение информационной безопасности автоматизированных систембазового уровня разработан на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем, в соответствии с рабочей программой МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации

Разработчик(и):

НефтИн (филиал) ФГБОУ ВО «ЮГУ» преподаватель Г.З. Кульмасова
(место работы) (занимаемая должность) (инициалы, фамилия)

1. Паспорт комплекта контрольно-измерительных материалов

1.1. Область применения

Комплект контрольно-измерительных материалов предназначен для проверки результатов освоения междисциплинарного курса (далее - МДК) программы подготовки специалистов среднего звена (ППССЗ) по специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Комплект контрольно-измерительных материалов позволяет оценивать:

1.1.1. Освоение профессиональных компетенций (ПК) и общих компетенций (ОК)

Профессиональные и общие компетенции	Средства проверки (№ задания)
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Комплекс ПЗ №1 – №14 Комплекс тестовых заданий
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации	Комплекс ПЗ №1 – №14 Комплекс тестовых заданий
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным кон текстам	Комплекс ПЗ №1 – №14 Комплекс тестовых заданий
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	Комплекс ПЗ №1 – №14 Комплекс тестовых заданий
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	Комплекс ПЗ №1 – №14 Комплекс тестовых заданий
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	Комплекс ПЗ №1 – №14 Комплекс тестовых заданий
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Комплекс ПЗ №1 – №14 Комплекс тестовых заданий
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	Комплекс ПЗ №1 – №14 Комплекс тестовых заданий
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Комплекс ПЗ №1 – №14 Комплекс тестовых заданий
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания	Комплекс ПЗ №1 – №14 Комплекс тестовых заданий

необходимого уровня физической подготовленности.	
ОК 09. Использовать информационные технологии в профессиональной деятельности	Комплекс ПЗ №1 – №14 Комплекс тестовых заданий
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках	Комплекс ПЗ №1 – №14 Комплекс тестовых заданий

1.1.2. Освоение умений и усвоение знаний

Освоенные умения, усвоенные знания	№№ заданий для проверки
1	2
У 1. применять технические средства для криптографической защиты информации конфиденциального характера;	Комплекс тестовых заданий
У2. применять технические средства для уничтожения информации и носителей информации;	Комплекс ПЗ №12 – №15
У3. применять нормативные правовые акты, нормативны методическиедокументыпообеспечениюзащитыинформациитехническимисредствами;	Комплекс тестовых заданий Комплекс ПЗ №1 – №4
У4. применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;	Комплекс тестовых заданий Комплекс ПЗ №16
У5. применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;	Комплекс тестовых заданий
У6. применять инженерно-технические средства физической защиты объектов информатизации	Комплекс тестовых заданий
З1. порядок технического обслуживания технических средств защиты информации;	Комплекс тестовых заданий Комплекс ПЗ №1 – №6
З2. номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;	Комплекс тестовых заданий Комплекс ПЗ №1 – №6
З3. физические основы, структуру и условия формирования технических каналов утечкии нформации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;	Комплекс тестовых заданий Комплекс ПЗ №7 – №11

34. порядок устранения неисправностей технических средств защиты информациии организации ремонта технических средств защиты информации;	Комплекс тестовых заданий Комплекс ПЗ №5 – №6
35. методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;	Комплекс тестовых заданий Комплекс ПЗ №12-№15
36. номенклатуру их арактеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;	Комплекс тестовых заданий Комплекс ПЗ №5-№11
37. основные принципы действия и характеристики технических средств физической защиты;	Комплекс тестовых заданий Комплекс ПЗ №5-№11
38. основные способы физической защиты объектов информатизации;	Комплекс тестовых заданий Комплекс ПЗ №3-№4
39. номенклатуру применяемых средств физической защиты объектов информатизации.	Комплекс тестовых заданий Комплекс ПЗ №1-№4

1.2. Система контроля и оценки освоения программы учебной дисциплины

1.2.1. Формы рубежной аттестации по ППССЗ при освоении учебной дисциплины

Междисциплинарный курс	Формы промежуточной аттестации
1	2
МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации	Другие формы контроля-5семестр Экзамен -6 семестр Курсовой проект- 7 семестр

1.2.2. Организация контроля и оценки освоения программы учебной дисциплины

Текущий контроль по МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации осуществляется на учебных занятиях.

Рубежный контроль по МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации (5 семестр) осуществляется другими формами контроля. ДФК проводятся в виде компьютерного тестирования.

Рубежный контроль по МДК 03.02Инженерно-технические средства физической защиты объектов информатизации (6 семестр) осуществляется на экзамене. Экзамен проводится по экзаменационным билетам.

Выполнение курсового проекта предусмотрено в конце 7 семестра.

Условием допуска к экзамену является положительная оценка по всем практическим занятиям.

Условием положительной аттестации по МДК является положительная оценка освоения всех умений, знаний, а также формируемых профессиональных и общих компетенций по всем контролируемым показателям.

2 . Задания для оценки освоения умений и усвоения знаний

к комплекту КИМ по МДК

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

по МДК 03.02. Инженерно-технические средства физической защиты объектов информатизации

№ ПЗ	Темы практических занятий	Освоенные умения, усвоенные знания
1	Прогноз маршрута проникновения на объект информатизации	У 1. – У 6. З 1. – З 9
2	Контроль инженерно-технических средств по основным показателям защиты объекта	У 1. – У 6. З 1. – З 9
3	Специальная проверка технических средств на возможность противодействия проникновению на объект информатизации	У 1. – У 6. З 1. – З 9
4	Исследование технических средств на возможность утечки информации	У 1. – У 6. З 1. – З 9
5	Монтаж датчиков пожарной и охранной сигнализации	У 1. – У 6. З 1. – З 9
6	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	У 1. – У 6. З 1. – З 9
7	Рассмотрение принципов устройства, работы и применения средств контроля доступа	У 1. – У 6. З 1. – З 9
8	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения	У 1. – У 6. З 1. – З 9
9	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации	У 1. – У 6. З 1. – З 9
10	Применение метода высокочастотного воздействия на технические средства перехвата информации по радио	У 1. – У 6. З 1. – З 9

	каналу	
11	Испытание пожарного извещателя системы сигнализации по уровню инерции	У 1. – У 6. З 1. – З 9
12	Определение номинальных параметров датчика перемещения охранной сигнализации на объекте информатизации.	У 1. – У 6. З 1. – З 9
13	Оценка эффективности мер защиты информации по электромагнитному излучению.	У 1. – У 6. З 1. – З 9
14	Оценка эффективности мер защиты информации по электромагнитному излучению.	У 1. – У 6. З 1. – З 9
15	Испытание учебной аудитории на защищенность помещения от утечки акустической речевой информации.	У 1. – У 6. З 1. – З 9

к комплекту КИМ по МДК

КОМПЛЕКТ ТЕСТОВЫХ ЗАДАНИЙ, ВЫНОСИМЫХ НА ДРУГИЕ ФОРМЫ КОНТРОЛЯ

по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

1. К видам каналов утечки информации относятся …
   *субъективные
   *объективные
   *технические
   *материально-вещественные
2. Концепция системы защиты от информационного оружия должна включать …
   *средства нанесения контратаки с помощью информационного оружия
   *процедуры нанесения атак с помощью информационного оружия
   *механизмы защиты пользователей от различных типов и уровней угроз для национальной
   информационной инфраструктуры
   *признаки, сигнализирующие о возможном нападении
   *процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и
   отдельных пользователей
3. Формой защиты информации является …
   аналитическая
   организационно-техническая
   страховая
   правовая
4. Симптомами заражения является …
   изменение длины файлов и даты создания
   уменьшение объёма системной памяти и свободного места на диске без видимых причин
   периодическое мерцание экрана

замедление работы программ, зависание и перезагрузка

5. Инженерно-техническая защита решает задачи по предотвращению или уменьшению угроз, вызванных …

*стихийными носителями угроз

*попытками злоумышленников проникнуть к местам хранения источников информации

*организованной или случайной утечкой информации с использованием различных технических средств

6. Контролируемая зона – это …

*территория объекта

*территория объекта, на которой возможно пребывание посторонних лиц

*территория объекта, на которой исключено неконтролируемое пребывание лиц

7. Показателем безопасности информации является …

*время, необходимое на взлом защиты информации

*вероятность предотвращения угрозы

*время, в течение которого обеспечивается определённый уровень безопасности

*вероятность возникновения угрозы информационной безопасности

8. Базовая схема системы передачи информации представляет собой:

передатчик – эфир - приемник

источник информации – канал связи – получатель информации

человек – компьютер - человек

9. В необходимый минимум средств защиты от вирусов входит …

выходной контроль

профилактика

входной контроль

архивирование

10. Электромагнитный канал утечки информации возникает за счет …

*побочных электромагнитных излучений технических средств передачи информации

*побочных излучений технических средств передачи информации

*высокочастотного облучения технических средств передачи информации

11. К наиболее важным методам защиты информации от нелегального доступа относится …

архивирование (создание резервных копий)

использование специальных «электронных ключей»

установление паролей на доступ к информации

использование антивирусных программ

шифрование

12. К методам выявления технических каналов утечки информации относится …

инструментальный контроль

физический поиск

тестирование

13. Видовая информация – это …

*информация о внутреннем виде объекта разведки или документа, получаемая при помощи технических средств разведки в виде их изображений

*информация о внешнем виде объекта разведки или документа, получаемая при помощи технических средств разведки в виде их изображений

*информация о внешнем виде объекта разведки или документа, получаемая при помощи

программных средств разведки в виде их изображений

14. Техническая защита информации – это защита информации …

с помощью программно-аппаратных средств

некриптографическими методами

криптографическими методами

15. Наиболее важными методами защиты информации от ошибочных действий пользователя является …

*установление специальных атрибутов файлов

*автоматический запрос на подтверждение выполнения команды или операции

*шифрование файлов

*предоставление возможности отмены последнего действия

*дублирование носителей информации

16. Вспомогательные технические средства и системы, это средства …

*и системы непосредственно участвующие в обработке информации ограниченного доступа

*и системы непосредственно не участвующие в обработке информации ограниченного доступа

*телефонной связи, компьютеры

17. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну,

наносящий ее владельцу ущерб, - это ...

добросовестная конкуренция

конфиденциальная информация

политическая разведка

промышленный шпионаж

18. Организационно-технические мероприятия – это мероприятия, которые вводят ограничения на … функционирования объекта защиты

результаты

параметры

условия

19. К демаскирующим признакам по времени проявления признаков относятся …

*эпизодические

*периодические

*долгосрочные

*краткосрочные

*постоянные

20. Акустическая информация – это …

*распространение акустических волн различной формы и длительности, распространяющиеся от

источника в окружающее пространство

*звуковые волны

*возмущения упругой среды различной формы и длительности, распространяющиеся от

источника в окружающее пространство

21. Признаки вещества:

*цвет, ширина спектра

*мощность, частота, амплитуда

*физический и химический состав, структура и свойства

22. Средства инженерно-технической защиты подразделяются на:

*физические, аппаратные, программные, криптографические, комбинированные

*физические, программные, криптографические, комбинированные

*физические, аппаратные, программные, комбинированные

23. Технические средства передачи информации – это технические средства …
*непосредственно обрабатывающие информацию ограниченного доступа
*непосредственно обрабатывающие информацию
*не обрабатывающие информацию ограниченного доступа
24. Особенностью речевых сообщений является …
виртуальность
документальность
конфиденциальность
целостность
25. К демаскирующим признакам по информативности признаков относятся …
*прямые (дополнительные признаки объекта) [информативность в пределах от 0 до 1]
*именные (однозначно определяющие объект) [информативность =1]
*информационно-психологические
*косвенные (признаки, непосредственно не принадлежащие объекту)
*технические
*физические
26. Основные типы систем обнаружения атак …
*локальные
*сетевые
*программные
*аппаратные
27. К демаскирующим признакам по состоянию объекта относятся …
*опознавательные признаки
*признаки физические
*признаки программные
*признаки деятельности
28. Задачи, поставленные в рамках концепции национальной безопасности приоритетное развитие отечественных современных информационных и телекоммуникационных технологий и …
*ускорение развития новых информационных технологий и их широкое распространение
*установление необходимого баланса между потребностью в свободном обмене информацией и
допустимыми ограничениями её распространения
*совершенствование информационной структуры
29. Объектом защиты может являться …
информационные процессы
носители информации
субъект
30. Физические системы защиты подразделяются на:
*системы ограждения и физической изоляции, системы контроля доступа, запирающие устройства
и хранилища
*системы ограждения и физической изоляции, запирающие устройства и хранилища
*системы охлаждения, системы этз, запирающие устройства и хранилища
31. Источником информации при утечке по техническим каналам может являться …
*информация, обрабатываемая техническими средствами передачи информации
*видовая информация
*информация, передаваемая по каналам связи
*человек

32. Признаки сигналов описывают параметры полей и генерирующих сигналов:
*высоту, ширину, длину
*форму, размеры, детали, тон, цвет, структуру и фактуру
*мощность, частота, природа, вид (аналог, импульс), ширина спектра;
33. Видовые признаки включают:
*запах, палитру, оттенки
*высоту, ширину, длину
*форму, размеры, детали, тон, цвет, структуру и фактуру
*частоту, амплитуду, ширину спектра
34. Классифицировать компьютерные вирусы можно по …
*степени опасности
*способу заражения среды обитания
*степени полезности
*объёму программы
*среде обитания
35. FireWall – это …
*почтовая программа
*графический редактор
*тоже самое что и интернет браузер
*тоже самое что и брэндмауэр
36. Периодичность аттестационных проверок для помещений первой и второй группы:
*не реже 3 раз в год
*не реже 2 раз в год
*не реже 1 раза в год
37. К методам защиты по вибрационному каналу относится …
*обследование стетоскопами
*изучение архитектурно-строительной документации
*маскирование
38. Параметрический канал утечки информации возникает за счет …
*высокочастотного облучения информационных сигналов
*побочных электромагнитных излучений информационных сигналов
*низкочастотного облучения информационных сигналов
39. Аттестация выделенных помещений – это проверка выделенных помещений и находящихся в них …
*технических средств на соответствие требованиям защиты
*технических средств на не соответствие требованиям защиты
*программных средств на соответствие требованиям защиты
40. К демаскирующим признакам по характеристикам объекта относятся …
Искусственные
видовые (форма, размеры, детали, фактура)
признаки сигнала (мощность, частота, вид, спектр)
архитектурные (фасад, высота)
признаки вещества (физ/хим состав, структура, свойства)
41. Утечка информации по техническим каналам реализуется в результате …
подслушивания конфиденциальных разговоров и акустических сигналов
перехвата различного рода полей и сигналов
наблюдения за источниками информации
недостаточной организацией защиты информации
42. Информативность – мера … признака
объемности
открытости
индивидуальности

показательности

43. При экранировании помещения применяется …
    фтористая сетка
    алюминиевая фольга
    листовая сталь
    медная сетк

Критерии оценки:

- оценка «отлично» выставляется студенту, если ..…90 – 100 %;
- оценка «хорошо» …… ……80 – 89 %;
- оценка «удовлетворительно» ……70 – 79%;
- оценка «неудовлетворительно» ……..…<70 %.

к комплекту КИМ по МДК

ПЕРЕЧЕНЬ
ВОПРОСОВ И ПРАКТИЧЕСКИХ ЗАДАНИЙ, ВЫНОСИМЫХ НА ЭКЗАМЕН

по МДК.03.02 Инженерно-
техническиесредствафизическойзащитыобъектовинформатизации

1. Характеристики потенциально опасных объектов.
2. Содержание и задачи физической защиты объектов информатизации.
3. Основные понятия инженерно-технических средств физической защиты.
4. Категорирование объектов информатизации.
5. Модель нарушителя и возможные пути, и способы его проникновения на охраняемый объект.
6. Особенности задач охраны различных типов объектов.
7. Общие принципы обеспечения безопасности объектов.
8. Жизненный цикл системы физической защиты.
9. Принципы построения интегрированных систем охраны.
10. Классификация и состав интегрированных систем охраны.
11. Требования к инженерным средствам физической защиты.
12. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.
13. Информационные основы построения системы охранной сигнализации.
14. Назначение, классификация средств обнаружения.
15. Построение систем обеспечения безопасности объекта.
16. Периметровые средства обнаружения:назначение, устройство , принцип действия.
17. Объектовые средства обнаружения: назначение, устройство , принцип действия.
18. Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности.
19. Особенности построения и размещения СКУД.
20. Структура и состав СКУД.
21. Периферийное оборудование и носители информации в СКУД.
22. Основы построения и принципы функционирования СКУД.
23. Классификация средств управления доступом.
24. Средства идентификации и аутентификации.
25. Методы удостоверения личности, применяемые в СКУД.
26. Обнаружение металлических предметов и радиоактивных веществ

27. Аналоговые и цифровые системы видеонаблюдения.
28. Назначение системы телевизионного наблюдения.
29. Видеокамеры, объективы, термокожухи.
30. Поворотные системы.
31. Инфракрасные осветители.
32. Детекторы движения.
33. Классификация системы сбора и обработки информации.
34. Схема функционировании системы сбора и обработки информации
35. Варианты структур построения системы сбора и обработки информации.
36. Устройства отображения и документирования информации.
37. Назначение и классификация технических средств воздействия .
38. Основные показатели технических средств воздействия.
39. Периметровые и объектовые средства обнаружения, порядок применения.
40. Работа с периферийным оборудованием системы контроля и управления доступом.
41. Особенности организации пропускного режима на КПП.
42. Управление системой телевизионного наблюдения с автоматизированного рабочего места.
43. Порядок применения устройств отображения и документирования информации.
44. Управление системой воздействия.
45. Этапы эксплуатации инженерно-технических средств физической защиты.
46. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.
47. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.
48. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.
49. Организация ремонта технических средств физической защиты.

Задание1.Опишите устройство и принципы работы IP-камеры:

Задание2.
Приведите определения основных параметров видеокамеры:разрешение видеокамеры,светочувствительность,размер светочувствительной матрицы,отношение сигнал/шум,фокусное расстояние объектива,термический диапазон работы камеры
Задание3.Опишите назначение и основные характеристики видеорегистраторов.
Задание4.Приведите характеристики сетевого видеорегистратора DVR.
Задание5.Приведите основные параметры видеомониторов.

Задание 6.
Опишите порядок проведения технического обслуживания, установки, настройки, диагнос тики, организации ремонта периметровых технических средств обнаружения, системы контроля и управления доступом. системы видеонаблюдения.

Критерии оценки:

- оценка «отлично» выставляется студенту, если ..…90 – 100 %;
- оценка «хорошо» …… ……80 – 89 %;
- оценка «удовлетворительно» ……70 – 79%;
- оценка «неудовлетворительно» ……..…<70 %.

Составитель _____ / Кульмасова Г.З./
подпись Ф.И.О.