МИНИСТЕРСТВО ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»

Комплект контрольно-оценочных средств

по учебной дисциплине

ОП. 01 Основы информационной безопасности

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка – 2024

Комплект контрольно-оценочных средств разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 года № 1553, с учетом профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 536н, и с учетом профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 533н, и с учетом профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 года № 525н.

Составитель:
Ковалёв Н.А., преподаватель ОГАПОУ «Алексеевский колледж»

1. Паспорт комплекта оценочных средств

1.1 Область применения комплекта оценочных средств

Контрольно-оценочные средства (КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины ОП 01. Основы информационной безопасности.

КОС включают контрольные материалы для проведения промежуточной аттестации в форме дифференцированного зачета.

КОС разработан на основании рабочей программы учебной дисциплины ОП 01. Основы информационной безопасности

1.2 Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины:

В результате освоения учебной дисциплины обучающийся должен **уметь**:

У1 классифицировать защищаемую информацию по видам тайны и степеням секретности;

У2 классифицировать основные угрозы безопасности информации.

В результате освоения учебной дисциплины обучающийся должен **знать**:

З1 сущность и понятие информационной безопасности, характеристику ее составляющих;

З2 место информационной безопасности в системе национальной безопасности страны;

З3 виды, источники и носители защищаемой информации;

З4 источники угроз безопасности информации и меры по их предотвращению;

З5 факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;

З6 жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;

З7 современные средства и способы обеспечения информационной безопасности;

З8 основные методики анализа угроз и рисков информационной безопасности.

Профессиональные (ПК) и общие (ОК) **компетенции**, которые актуализируются при изучении учебной дисциплины:

ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие

ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей

ОК 09 Использовать информационные технологии в профессиональной деятельности

ОК 10 Пользоваться профессиональной документацией на государственном и иностранном языках

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

Перечень знаний и умений в соответствии с профессиональными стандартами «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н, «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н., «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н., «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н., которые актуализируются при изучении междисциплинарного курса:

1) способы защиты информации от утечки по техническим каналам;
2) основные методы управления защитой информации;
3) применять антивирусные средства защиты информации в операционных системах;
4) организационные меры по защите информации.

Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции чемпионатного движения по профессиональному мастерству «Профессионалы» и Чемпионата высоких технологий Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении профессионального модуля:

1) знать и понимать: скорость изменения ИТ-сферы и области информационной безопасности, а также важность соответствия современному уровню;
2) знать и понимать: подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия;
3) знать и понимать: особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, MWare Workstation;
4) знать и понимать: типы угроз информационной безопасности, типы инцидентов;
5) знать и понимать: Технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;
6) знать и понимать: структуру виртуальной защищенной сети. Назначение виртуальной защищенной сети. Особенности построения VPN-сетей. Основные типы классификаций VPN-сетей;

7) знать и понимать: подходы к проведению расследования инцидента информационной безопасности, методики оценки уровня угроз

1.3.Планируемые личностные результаты освоения рабочей программы

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа».

ЛР 7. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 10. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

ЛР 11. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

1.4 Результаты освоения учебной дисциплины, подлежащие проверке

Наименование тем	Коды умений (У), знаний (З), личностных результатов (ЛР), формированию которых способствует элемент программы	Средства контроля и оценки результатов обучения **в рамках текущей аттестации** (номер задания)	Средства контроля и оценки результатов обучения **в рамках промежуточной аттестации** (номер задания/контрольного вопроса/ экзаменационного билета)
Тема 1.1. Основные понятия и задачи информационной безопасности	У1-У2 З1-З8 ЛР 4 ЛР 7	ТЗ №1	КВ №1-5 ТЗ №1
Тема 1.2. Основы защиты информации	У1-У2 З1-З8 ЛР 4 ЛР 7 ЛР 10 ЛР 11	ПЗ №1-2	ТЗ №6-9 КВ №2-5
Тема 1.3. Угрозы безопасности защищаемой информации.	У1-У2 З1-З8 ЛР 4	ПЗ №3-4	ТЗ №10-14 КВ №6-8
Тема 2.1. Методологические подходы к защите информации	У1-У2 З1-З8 ЛР 4 ЛР 7 ЛР 10 ЛР 11	ПЗ №5	ТЗ №15-19 КВ №9-10
Тема 2.2. Нормативно правовое регулирование защиты информации	У1-У2 З1-З8 ЛР 4 ЛР 7 ЛР 10 ЛР 11	ПЗ №6-7	ТЗ №20-24 КВ №14
Тема 2.3. Защита информации в автоматизированных (информационных) системах	У1-У2 З1-З8 ЛР 4 ЛР 7 ЛР 10 ЛР 11	ПЗ №8-9	ТЗ №25-31 КВ №15-16

2. Комплект оценочных средств

2.1. Практические задания (ПЗ)

ПЗ №1 ОПРЕДЕЛЕНИЕ ОБЪЕКТОВ ЗАЩИТЫ НА ТИПОВОМ ОБЪЕКТЕ ИНФОРМАТИЗАЦИИ.

Задания для выполнения практической работы:

Задание 1. Построение структуры подразделений объекта защиты, характеристика назначения объекта и решаемых задач. Определение функционально-отраслевой принадлежности объекта.

Задание 2. Определение содержании и местонахождения защищаемых ресурсов на объекте.

Задание 3. Построение плана объекта. Определение защищаемых зон на плане. Построить план объекта, с помощью принятых стандартом условных обозначений показать все объекты защиты. Определить категории защищаемых зон. Определить структуру контролируемых зон.

Задание 4. Характеристика технической укрепленности объекта.Построение пространственной модели объекта защиты.Проанализировать характеристики технической укрепленности объектазащиты

ПЗ №2 КЛАССИФИКАЦИЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ ПО ВИДАМ ТАЙНЫ И СТЕПЕНЯМ КОНФИДЕНЦИАЛЬНОСТИ.

Задания для выполнения практической работы:

Исходя из 1 практической работы «Определение объектов защиты на типовом объекте информатизации» необходимо определить, какой вид и степень конфиденциальности используется в данной организации. Какие данные обрабатываются в организации. Необходимо подробное описание, почему выбраны вид и степень конфиденциальности для данной организации.

Таблица 1 - Варианты объектов защиты.

№ варианта	Объект информатизации
1	Здание администрации завода железобетонных изделий
2	Здание торгового центра
3	Здание поликлиники
4	Корпус университета
5	Здание научно-производственного объединения
6	Здание фармацевтической фирмы
7	Здание районного отдела полиции
8	Здание банка
9	Здание патентного бюро
10	Здание редакции научного издания
11	Здание научно-исследовательского института
12	Здание склада текстильной продукции
13	Здание рекламного агентства
14	Здание производственных цехов бурового оборудования
15	Здание птицефабрики
16	Здание республиканской библиотеки
17	Здание музея изобразительных искусств
18	Здание школы
19	Здание больницы
20	Здание районного суда

ПЗ №3-4 ОПРЕДЕЛЕНИЕ УГРОЗ ОБЪЕКТА ИНФОРМАТИЗАЦИИ И ИХ КЛАССИФИКАЦИЯ

Задания для выполнения практической работы:

Необходимо провести анализ защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия
7. Определить класс защищенности автоматизированной системы

ПЗ №5 ДИАГНОСТИКА И КОРРЕКЦИЯ ОШИБОК ОПЕРАЦИОННОЙ СИСТЕМЫ, КОНТРОЛЬ ДОСТУПА К ОПЕРАЦИОННОЙ СИСТЕМЕ.

Задания для выполнения практической работы:

1. Запустить командную строку: клавиша Пуск, Программы, Стандартные, Командная строка – ПКМ – «***Запустить от имени администратора***»
2. В открывшемся окне вводится команда: «chkdsk C: /F».
3. После ввода команды следует нажать кнопку Enter. При следующей перезагрузке система проведет проверку и исправление на ошибки.
4. По результатам проверки сделайте отчет.
5. Проверка командой sfc scannow Утилита также запускается из командной строки. Для запуска проверки понадобятся права Администратора.
6. В командной строке нужно ввести «sfc /scannow». Система автоматически проверит файлы, в том числе, закрытые, исправит ошибки, восстановит поврежденные из кэшированной копии.
7. По результатам проверки сделайте отчет.

ПЗ №6-7 РАБОТА В СПРАВОЧНО-ПРАВОВОЙ СИСТЕМЕ С НОРМАТИВНЫМИ И ПРАВОВЫМИ ДОКУМЕНТАМИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Задания для выполнения практической работы:

1. Найдите федеральный закон об электронной подписи, принятый в 2011 году.

2. Работа со словарем терминов. Найдите определения следующих понятий: «информация», «документированная информация», «документ», «обязательный экземпляр документа», «архивный документ», «безопасность», «технологическая карта», «кондитерское изделие», «мучное кондитерское изделие», «пекарни и цеха малой мощности».

ПЗ №8-9 ВЫБОР МЕР ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА

Задания для выполнения практической работы:

1. Выделить угрозы и уязвимости, которые можно устранить физическими и инженерно-техническими средствами.
2. Построить схему объекта. Выделить источники защищаемой информации. Определить зоны, классифицировать их (независимые, пересекающиеся, вложенные).
3. Построить движение злоумышленника до источника. Описать возможные меры физической защиты для увеличения времени проникновения.

4. Определить угрозы утечек по техническим, аудио- и видео- каналам. Описать возможные меры инженерно-технической защиты для нейтрализации.
5. Оценить вероятность каждой меры предотвратить уязвимость.

2.2. Тестовые задания (ТЗ)

ТЗ№1 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

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.

3. Комплект оценочных средств для промежуточной аттестации

3.1. Контрольные вопросы (КВ)

КВ№1 Понятие информации и информационной безопасности.
КВ№2 Информация, сообщения, информационные процессы как объекты информационной безопасности.
КВ№3 Обзор защищаемых объектов и систем.
КВ№4 Понятие «угроза информации».
КВ№5 Понятие «риска информационной безопасности».
КВ№6 Примеры преступлений в сфере информации и информационных технологий.
КВ№7 Сущность функционирования системы защиты информации.
КВ№8 Защита человека от опасной информации и от неинформированности в области информационной безопасности
КВ№9 Целостность, доступность и конфиденциальность информации.
КВ№10 Классификация информации по видам тайны и степеням конфиденциальности.
КВ№11 Понятия государственной тайны и конфиденциальной информации.
КВ№12 Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
КВ№13 Цели и задачи защиты информации.
КВ№14 Основные понятия в области защиты информации.
КВ№15 Элементы процесса менеджмента ИБ.
КВ№16 Модель интеграции информационной безопасности в основную деятельность организации.
КВ№17 Понятие Политики безопасности.
КВ№18 Определение объектов защиты на типовом объекте информатизации.
КВ№19 Классификация защищаемой информации по видам тайны и степеням конфиденциальности
КВ№20 Понятие угрозы безопасности информации.
КВ№21 Системная классификация угроз безопасности информации.
КВ№22 Каналы и методы несанкционированного доступа к информации
КВ№23 Применение потоков. Классификация потоков.
КВ№24 Реализация потоков. Уязвимости.
КВ№25 Методы оценки уязвимости информации
КВ№26 Определение угроз объекта информатизации и их классификация
КВ№27 Организационная структура системы защиты информации.
КВ№28 Законодательные акты в области защиты информации.
КВ№29 Российские и международные стандарты, определяющие требования к защите информации.
КВ№30 Система сертификации РФ в области защиты информации.
КВ№31 Основные правила и документы системы сертификации РФ в области защиты информации

3.2. Тестовые задания (ТЗ)

ТЗ №1

Задание 1 Какие законы существуют в России в области компьютерного права?

Выберите несколько из 6 вариантов ответа:

1) О государственной тайне
2) об авторском праве и смежных правах
3) о гражданском долге
4) о правовой охране программ для ЭВМ и БД
5) о правовой ответственности
6) об информации, информатизации, защищенности информации

Задание 2 Какие существуют основные уровни обеспечения защиты информации?

Выберите несколько из 7 вариантов ответа:

1) законодательный
2) административный
3) программно-технический
4) физический
5) вероятностный
6) процедурный
7) распределительный

Задание 3 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 4 В чем заключается основная причина потерь информации, связанной с ПК?

Выберите один из 3 вариантов ответа:

1) с глобальным хищением информации
2) с появлением интернета
3) с недостаточной образованностью в области безопасности

Задание 5 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 6 К аспектам ИБ относятся

Выберите несколько из 5 вариантов ответа:

1) Дискретность
2) целостность
3) конфиденциальность
4) актуальность
5) доступность

Задание 7 Что такое криптология?

Выберите один из 3 вариантов ответа

1) защищенная информация

2) область доступной информации

3) тайная область связи

Задание 8 Что такое несанкционированный доступ (нсд)?

Выберите один из 5 вариантов ответа:

1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа

2) Создание резервных копий в организации

3) Правила и положения, выработанные в организации для обхода парольной защиты

4) Вход в систему без согласования с руководителем организации

5) Удаление не нужной информации

Задание 9 Что является основой для формирования государственной политики в сфере информации? (Ответьте 1 словом

Запишите ответ:

Задание 10 Что такое целостность информации?

Выберите один из 4 вариантов ответа

1) Свойство информации, заключающееся в возможности ее изменения любым субъектом

2) Свойство информации, заключающееся в возможности изменения только единственным пользователем

3) Свойство информации, заключающееся в ее существовании в виде единого набора файлов

4) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)

Задание 11Кто является знаковой фигурой в сфере информационной безопасности

Выберите один из 4 вариантов ответа:

1) Митник

2) Шеннон

3) Паскаль

4) Беббидж

Задание 12В чем состоит задача криптографа?

Выберите один из 2 вариантов ответа:

1) взломать систему защиты

2) обеспечить конфиденциальность и аутентификацию передаваемых сообщений

Задание 13Под ИБ понимают

Выберите один из 3 вариантов ответа:

1) защиту от несанкционированного доступа

2) защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера

3) защиту информации от компьютерных вирусов

Задание 14Что такое аутентификация?

Выберите один из 5 вариантов ответа:

1) Проверка количества переданной и принятой информации

2) Нахождение файлов, которые изменены в информационной системе несанкционированно

3) Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).

4) Определение файлов, из которых удалена служебная информация

5) Определение файлов, из которых удалена служебная информация

Задание 15"Маскарад"- это

Выберите один из 2 вариантов ответа:

1) осуществление специально разработанными программами перехвата имени и пароля

2) выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями

Задание 16Верификация–

Выберите один из 3 вариантов ответа:

1) это проверка принадлежности субъекту доступа предъявленного им идентификатора.

2) проверка целостности и подлинности инф, программы, документа

3) это присвоение имени субъекту или объекту

Задание 17Кодирование информации –

Выберите один из 2 вариантов ответа

1) представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.

2) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом

Задание 18Утечка 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 19Под 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 20К аспектам ИБ относятся

Выберите несколько из 5 вариантов ответа:

1) дискретность

2) целостность

3) конфиденциальность

4) актуальность

5) доступность

Задание 21Линейное шифрование –

Выберите один из 3 вариантов ответа:

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

2) криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому

3) криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами

Задание 22Прочность защиты в АС

Выберите один из 3 вариантов ответа:

1) вероятность не преодоления защиты нарушителем за установленный промежуток времени

2) способность системы защиты информации обеспечить достаточный уровень своей

безопасности

3) группа показателей защиты, соответствующая определенному классу защиты

Задание 23Уровень секретности – это

Выберите один из 2 вариантов ответа:

1) ответственность за модификацию и НСД информации

2) административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов

Задание 24Угроза– это

Выберите один из 2 вариантов ответа:

1) возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов

2) событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов

Задание 25Под ИБ понимают

Выберите один из 3 вариантов ответа:

1) защиту от несанкционированного доступа

2) защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера

3) защиту информации от компьютерных вирусов

Ответы:

1) Верные ответы: 1; 2; 4; 6;
2) Верные ответы: 1; 2; 3; 6;
3) Верные ответы: 1;
4) Верные ответы: 3;
5) Верные ответы: 4;
6) Верные ответы: 2; 3; 5;
7) Верные ответы: 3;
8) Верные ответы: 1;
9) Верный ответ: "доктрина".
10) Верные ответы: 4;
11) Верные ответы: 1;
12) Верные ответы: 2
13) Верные ответы: 2;
14) Верные ответы: 3;
15) Верные ответы: 2;
16) Верные ответы: 2;
17) Верные ответы: 1;
18) Верные ответы: 2;
19) Верные ответы: 2;
20) Верные ответы: 2; 3; 5;
21) Верные ответы: 2;
22) Верные ответы: 1;
23) Верные ответы: 2;
24) Верные ответы: 1;
25) Верные ответы: 2;

4. Критерии оценивания

«5» «отлично» или «зачтено» – студент показывает глубокое и полное овладение содержанием программного материала по УД, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в форме грамотного, логического ответа (устного или письменного), а также высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;

«4» «хорошо» или «зачтено» – студент в полном объеме освоил программный материал по УД, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«3» «удовлетворительно» или «зачтено» – студент обнаруживает знание и понимание основных положений программного материала по УД, но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и профессиональных задач, не умеет доказательно обосновать свои суждения, но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«2» «неудовлетворительно» или «не зачтено» – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по УД, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

5. Информационное обеспечение

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с.
2. 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
3. Основы информационной безопасности. Учебник/ Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. – М.: Академия. 2019-256 с.
4. 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.

Дополнительные источники:

5. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. – М.: Издательство КДУ.
6. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: Инфа-М. 2016.
7. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD) : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — 2-е изд., стер. – М. : КНОРУС, 2016.
8. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. Учебное пособие. – М.: МГТУ им. Баумана. 2016.
9. Нестеров С.А. Основы информационной безопасности. Учебное пособие. – С-Пб.: Лань. 2016.
10. Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности. –М.: Академия. 2015.
11. Проскурин В.Г. Защита программ и данных: Учебное пособие для ВУЗов. - –М.: Академия. 2012.
12. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – С-Пб.: Изд. Питер. 2017.

Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях. ДМК Пресс, 2012.

Электронные издания (электронные ресурсы)

13. 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
14. 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. —https://urait.ru/bcode/456792
15. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

Цифровая образовательная среда СПО PROFобразование:

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/97562 (дата обращения: 18.11.2020). — Режим доступа: для авторизир. пользователей
2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/91640 (дата обращения: 18.11.2020). — Режим доступа: для авторизир. пользователей
3. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 с. — ISBN 978-5-4497-0338-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/89453 (дата обращения: 18.11.2020). — Режим доступа: для авторизир. пользователей

Электронно-библиотечная система:

IPR BOOKS
https://www.iprbookshop.ru/10746.html
https://www.iprbookshop.ru/43960.html

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/