Государственное автономное профессиональное
образовательное учреждение
«Мамадышский политехнический колледж»

УТВЕРЖДАЮ
Зам. директора по ТО
_____ Файзреева В.В.
«01» сентября 2023 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля и промежуточной аттестации
по учебной дисциплине
ОП.10 Основы информационной безопасности
по специальности 09.02.01 Компьютерные системы и комплексы

2023 г.

Фонд оценочных средств разработан на основе рабочей программы учебной дисциплины ОП.10 Основы информационной безопасности и в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.01 Компьютерные системы и комплексы, приказ Министерства образования и науки от 25 мая 2022 г. № 362 (Зарегистрировано в Минюсте России 28.06.2022 г. №69046).

Обсуждена и одобрена на заседании предметно-цикловой комиссии общепрофессиональных дисциплин

Разработала преподаватель:

_____ Р.З. Искандарова

Протокол № 1

«28» августа 2023 г.

Председатель ПЦК _____ В.В. Мирзаянова

СОДЕРЖАНИЕ

1. ПАСПОРТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

1.1 Область применения

Контрольно-оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, осваивающих программу учебной дисциплины ***Программное обеспечение компьютерных систем.***

Контрольно-оценочные средства включают контрольные материалы для проведения текущего контроля и промежуточной аттестации в форме дифференцированного зачета.

КОС разработаны в соответствии с рабочей программой учебной дисциплины.

2. ПОКАЗАТЕЛИ ОЦЕНКИ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ФОРМЫ И МЕТОДЫ КОНТРОЛЯ И ОЦЕНКИ

Результаты обучения	***Критерии оценки***	***Формы и методы оценки***
Перечень знаний, осваиваемых в рамках дисциплины:	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполненияоценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера,	Оценка в рамках текущего контроля результатов выполнения индивидуальных контрольных заданий, результатов выполнения практических работ, устный индивидуальный опрос. Письменный опрос в форме тестирования.
Содержание актуальной нормативно-правовой документации; Современная научная и профессиональная терминология; Значимость профессиональной деятельности специальности.		
Перечень умений, осваиваемых в рамках дисциплины:		

Распознавать задачу и/или проблему в профессиональном и/или социальном контексте; Реализовать задачу и/или проблему и выделять её составные части; Определять этапы решениязадачи; Определять актуальность нормативно-правовой документации в профессиональной деятельности; Применять современную научную профессиональную терминологию; Выбирать сетевые топологии; Использовать программно- аппаратные средства технического контроля; Использовать программно- аппаратные средства технического контроля;	необходимые умения работы с освоенным материалом в основномсформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Экспертное наблюдение и оценивание выполнения практических работ. Текущий контроль в форме защиты практических работ.

3. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

ПЕРЕЧЕНЬ ТЕСТОВ

Тема 1. Понятие национальной безопасности. Понятие информационной безопасности.

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных

- Разработка и установка во всех компьютерных правовых сетях журналов учета действий

+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство

+ Перехват данных, хищение данных, изменение архитектуры системы

- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

+ Персональная, корпоративная, государственная

- Клиентская, серверная, сетевая

- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети

- инсайдерства в организации

- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных

- Информационные системы, психологическое состояние пользователей

- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации

- Техническое вмешательство, выведение из строя оборудования сети

+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

+ Экономической эффективности системы безопасности

- Многоплатформенной реализации системы

- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний

+ органы права, государства, бизнеса

- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

+ Установление регламента, аудит системы, выявление рисков

- Установка новых офисных приложений, смена хостинг-компании

- Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:

+ Неоправданных ограничений при работе в сети (системе)

- Рисков безопасности сети, системы

- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

+ Невозможности миновать защитные средства сети (системы)

- Усиления основного звена сети, системы

- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

+ Усиления защищенности самого незащищенного звена сети (системы)

- Перехода в безопасное состояние работы сети, системы

- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

- Одноуровневой защиты сети, системы

- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой

+ Логические закладки («мины»)

- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить

- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения

- Секретность информации определена скоростью передачи данных

+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь

+ Электронно-цифровая подпись

- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО

+ Ошибки эксплуатации и неумышленного изменения режима работы системы

- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования

- Моральный износ сети, инсайдерство

+ Сбой (отказ) оборудования, нелегальное копирование данных

тест_20) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет

+ Вирусы в сети, логические мины (закладки), информационный перехват

- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

+ Потерей данных в системе

- Изменением формы информации

- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

+ Целостность

- Доступность

- Актуальностьl

23) Угроза информационной системе (компьютерной сети) – это:

+ Вероятное событие

- Детерминированное (всегда определенное) событие

- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной

- Правовой

+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

+ Программные, технические, организационные, технологические

- Серверные, клиентские, спутниковые, наземные

- Личные, корпоративные, социальные, национальные

Тема 2. Угрозы информационной безопасности.

1. Основная масса угроз информационной безопасности приходится на:
а) Троянские программы +
б) Шпионские программы
в) Черви

2. Какой вид идентификации и аутентификации получил наибольшее распространение:
а) системы PKI
б) постоянные пароли +
в) одноразовые пароли

3. Под какие системы распространение вирусов происходит наиболее динамично:
а) Windows
б) Mac OS
в) Android +

4. Заключительным этапом построения системы защиты является:
а) сопровождение +
б) планирование
в) анализ уязвимых мест

5. Какие угрозы безопасности информации являются преднамеренными:
а) ошибки персонала
б) открытие электронного письма, содержащего вирус
в) не авторизованный доступ +

6. Какой подход к обеспечению безопасности имеет место:
а) теоретический
б) комплексный +
в) логический

7. Системой криптографической защиты информации является:
а) BFox Pro
б) CAudit Pro
в) Крипто Про +

8. Какие вирусы активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы +
б) троянцы
в) черви

9. Stuxnet — это:
а) троянская программа
б) макровирус
в) промышленный вирус +

10. Таргетированная атака — это:
а) атака на сетевое оборудование
б) атака на компьютерную систему крупного предприятия +
в) атака на конкретный компьютер пользователя

11. 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 верного ответа

12. Защита информации:
а) небольшая программа для выполнения определенной задачи
б) комплекс мероприятий, направленных на обеспечение информационной безопасности +
в) процесс разработки структуры базы данных в соответствии с требованиями пользователей

13. Информационная безопасность зависит от:
а) компьютеров, поддерживающей инфраструктуры +
б) пользователей
в) информации

14. Конфиденциальностью называется:
а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
б) описание процедур
в) защита от несанкционированного доступа к информации +

15. Для чего создаются информационные системы:
а) получения определенных информационных услуг +
б) обработки информации
в) оба варианта верны

16. Кто является основным ответственным за определение уровня классификации информации:

а) руководитель среднего звена
б) владелец +
в) высшее руководство

17. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
а) хакеры
б) контрагенты
в) сотрудники +

18. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству:
а) снизить уровень классификации этой информации
б) улучшить контроль за безопасностью этой информации +
в) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

19. Что самое главное должно продумать руководство при классификации данных:
а) управление доступом, которое должно защищать данные
б) оценить уровень риска и отменить контрмеры
в) необходимый уровень доступности, целостности и конфиденциальности +

20. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:
а) владельцы данных
б) руководство +
в) администраторы

Тема 3. Методы и средства обеспечения информационной безопасности компьютерных систем.

1. Как называется умышленно искаженная информация?
+ Дезинформация
- Информативный поток
- Достоверная информация
- Перестает быть информацией

2. Как называется информация, к которой ограничен доступ?
+ Конфиденциальная
- Противозаконная
- Открытая
- Недоступная

3. Какими путями может быть получена информация?
+ проведением, покупкой и противоправным добыванием информации научных исследований
- захватом и взломом ПК информации научных исследований
- добыванием информации из внешних источников и скремблированием информации научных исследовании
- захватом и взломом защитной системы для информации научных исследований

4. Как называются компьютерные системы, в которых обеспечивается безопасность информации?
+ защищенные КС
- небезопасные КС
- Само достаточные КС
- Саморегулирующиеся КС

5. Основной документ, на основе которого проводится политика информационной безопасности?
+ программа информационной безопасности
- регламент информационной безопасности
- политическая информационная безопасность
- Протекторат

6. Что называют защитой информации?
+ Все ответы верны
- Называют деятельность по предотвращению утечки защищаемой информации
- Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
- Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию

7. Шифрование информации это
+ Процесс ее преобразования, при котором содержание информации становится непонятным для не обладающих соответствующими полномочиями субъектов
- Процесс преобразования, при котором информация удаляется
- Процесс ее преобразования, при котором содержание информации изменяется на ложную
- Процесс преобразования информации в машинный код

8. Основные предметные направления Защиты Информации?
+ охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности

- Охрана золотого фонда страны
- Определение ценности информации
- Усовершенствование скорости передачи информации

9. Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право
- управление доступом
+ конфиденциальность
- аутентичность
- целостность
- доступность

10. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем
- защита от сбоев в электропитании
+ защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

11. Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных
- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
+ защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

12. Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.
- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
+ защита от утечек информации электромагнитных излучений

13. Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе
+ Информационная безопасность
- Защитные технологии
- Заземление
- Конфиденциальность

14. Можно выделить следующие направления мер информационной безопасности

- Правовые
- Организационные
+ Все ответы верны
- Технические

15. Что можно отнести к правовым мерам ИБ?

+ Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
- охрану вычислительного центра, установку сигнализации и многое другое

16. Что можно отнести к организационным мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.
+ Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.
- Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.
- Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

17. Что можно отнести к техническим мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- Охрану вычислительного центра, тщательный подбор персонала,

исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
+ Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое
- Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов
- В административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

18. Потенциальные угрозы, против которых направлены технические меры защиты информации
+ Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей
- Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения
- Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками.
- Потери информации из-за не достаточной установки сигнализации в помещении.
- Процессы преобразования, при котором информация удаляется

19. Средства защиты данных, функционирующие в составе программного обеспечения.
+ Программные средства защиты информации
- Технические средства защиты информации
- Источники бесперебойного питания (UPS)
- Смешанные средства защиты информации

20. Программные средства защиты информации.
+ средства архивации данных, антивирусные программы
- Технические средства защиты информации
- Источники бесперебойного питания (UPS)
- Смешанные средства защиты информации

21. Программное средство защиты информации.
+ криптография
- источник бесперебойного питания
- резервное копирование
- дублирование данных

22. Обеспечение достоверности и полноты информации и методов ее обработки.

- Конфиденциальность
+ Целостность
- Доступность
- Целесообразность

23. Обеспечение доступа к информации только авторизованным пользователям?

+ Конфиденциальность
- Целостность
- Доступность
- Целесообразность

24. Защита через права доступа заключается.

+присвоении каждому пользователю определенного набора прав
-запереть серверы в специальном помещении с ограниченным доступом
-присвоить пароль каждому общедоступному ресурсу
- в наличии преобразователя микрофона

25. Дифференцированное резервное копирование это

-Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании
-Копирование всех выбранных файлов без отметки о резервном копировании
-Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования
+Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании

26. Полное копирование данных это

+Копирование и маркировка выбранных файлов, вне зависимости от того, изменялись ли они со времени последнего резервного копирования
-Копирование всех выбранных файлов без отметки о резервном копировании
-Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании
-Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования

27. Наиболее распространенный криптографический код

+Код Хэмминга
-код Рида-Соломона
-код Морзе
-итеративный код

28. Ежедневное копирование данных это

+Копирование только тех файлов, которые были изменены в течение дня, без

отметки о резервном копировании
-Копирование всех выбранных файлов без отметки о резервном копировании
-Копирование и маркировка выбранных файлов, вне зависимости от того, изменялись ли они со времени последнего резервного копирования
-Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании

29. Что такое Информационная безопасность?
+ меры по защите информации от неавторизованного доступа
-меры по защите ПК
-безопасность личной информации
-все перечисленное

30. Целью информационной безопасности является?
+ все перечисленное
- обезопасить ценности системы
- защитить и гарантировать точность и целостность информации
- минимизировать разрушения

31. Укажите направления мер информационной безопасности.
+правовые, организационные, технические
-правовые, аппаратные, программные
-личные, организационные
-технические

32. Технические меры защиты можно разделить на:
+ средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания, и тд
-правовые, организационные, технические
-правовые, аппаратные, программные
-личные, организационные

33. Программные средства защиты можно разделить на:
+криптография, антивирусные программы, системы разграничения полномочий, средства контроля доступа и тд
- административные меры защиты, включающие подготовку и обучение персонала, организацию тестирования и приема в эксплуатацию программ, контроль доступа в помещения и тд
-правовые, организационные, технические
-правовые, аппаратные, программные

34. К наиболее важному элементу аппаратной защиты можно отнести?
+ защита от сбоев серверов, рабочих станций и локальных компьютеров
-защиту от вирусов

-защиту от хакеров
-все перечисленное

35. Как связаны ключи шифрования между собой?
+математической функцией
-связкой
-шифром
-специальным паролем

35. Что относится к возможным сигнатурам?
+ длина незаписанных участков магнитной ленты и неиспользованные дорожки на дискете
- дорожки дискеты и линии связи
- источник бесперебойного питания (UPS)
- источник питания и использованные дорожки на дискете

Оценка результатов тестирования. За каждый правильный ответ начисляется 1 балл. Для перевода баллов в оценку применяется универсальная шкала оценки образовательных достижений. Если обучающийся набирает

– от 90 до 100% от максимально возможной суммы баллов – выставляется оценка «отлично»;

– от 80 до 89% - оценка «хорошо»,

– от 51 до 79% - оценка «удовлетворительно»,

– менее 51% - оценка «неудовлетворительно».

4. КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Аттестация по результатам изучения учебной дисциплины – дифференцированный зачет*

ВОПРОСЫ К ДИФФЕРЕНЦИРОВАННОМУ ЗАЧЕТУ

1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.

2. Основные понятия информационной безопасности.

3. Структура понятия информационная безопасность.

4. Система защиты информации и ее структура.

5. Экономическая информация как товар и объект безопасности.

6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.

7. Персональные данные и их защита.

8. Информационные угрозы, их виды и причины возникновения.

9. Информационные угрозы для государства.

10. Информационные угрозы для компании.

11. Информационные угрозы для личности (физического лица).

12. Действия и события, нарушающие информационную безопасность.

13. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.

14. Способы воздействия информационных угроз на объекты.

15. Внешние и внутренние субъекты информационных угроз.

16. Компьютерные преступления и их классификация.

17. Исторические аспекты компьютерных преступлений и современность.

18. Субъекты и причины совершения компьютерных преступлений.

19. Вредоносные программы, их виды.

20. История компьютерных вирусов и современность.

21. Государственное регулирование информационной безопасности.

22. Деятельность международных организаций в сфере информационной безопасности.

23. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.

24. Доктрина информационной безопасности России.

25. Уголовно-правовой контроль над компьютерной преступностью в России.

26. Федеральные законы по ИБ в РФ.

27. Политика безопасности и ее принципы.

28. Фрагментарный и системный подход к защите информации.

39.Методы и средства защиты информации.

30. Организационное обеспечение ИБ.

31. Комплекс организационно-технических мероприятий по обеспечению защиты информации.

32. Инженерно-техническое обеспечение компьютерной безопасности.

33. Организационно-правовой статус службы безопасности.

34. Защита информации в Интернете.

35. Электронная почта и ее защита.

36. Защита от компьютерных вирусов.

Критерии и нормы оценки:

Оценка «отлично» ставится, если обучающийся показал полный объем, высокий уровень и качество знаний по данным вопросам, владеет культурой общения и навыками научного изложения материала, устанавливает связь между теоретическими знаниями и способами практической деятельности; ясно, точно и логично отвечает на заданные вопросы.

Оценка «хорошо» ставится, если обучающийся логично и научно изложил материал, но недостаточно полно определяет практическую значимость теоретических знаний; не высказывает своей точки зрения по данному вопросу, не смог дать достаточно полного ответа на поставленные

вопросы.

Оценка «удовлетворительно» ставится, если обучающийся при раскрытии вопроса допустил содержательные ошибки, не соотнес теоретические знания и собственную практическую деятельность, испытывает затруднения при ответе на большинство вопросов.

Оценка «неудовлетворительно» ставится, если обучающийся показал слабые теоретические и практические знания, допустил грубые ошибки при раскрытии вопроса, не смог ответить на заданные вопросы.