государственное бюджетное профессионального образовательное учреждение
«Пермский политехнический колледж имени Н.Г. Славянова»

УТВЕРЖДАЮ
Заместитель директора
_____ /С.Н. Нагиева/
09.11.2023

КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ МЕЖДИСЦИПЛИНАРНОГО КУРСА МДК.03.02 БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

для реализации Программы подготовки специалистов среднего звена
по специальности
09.02.06 Сетевое и системное администрирование
(технологический профиль профессионального образования)

2023

Рассмотрено и одобрено на заседании
Предметной цикловой комиссией
«Выпускающая студентов на государственную итоговую аттестацию»
Протокол №2
от 21 октября 2023г.
Председатель ПЦК
_____ С.В. Вепрева

Разработчик:
ГБПОУ «Пермский политехнический колледж имени Н.Г. Славянова»
Быстров Никита Олегович, преподаватель

Пояснительная записка

Промежуточная аттестация студентов проводится после завершения освоения программы междисциплинарного курса МДК.03.02 Безопасность компьютерных сетей

КОС промежуточной аттестации студентов МДК.03.02 Безопасность компьютерных сетей составлены в соответствии с требованиями ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование, утверждённого Приказом Минпросвещения России от 10.07.2023 N 519 (Зарегистрировано в Минюсте России 15.08.2023 N 74796) и учебным планом специальности 09.02.06, утвержденным директором 12.10.2023

КОС промежуточной аттестации имеют своей целью определение полноты и прочности теоретических знаний и практических навыков по МДК.02.02 Программное обеспечение компьютерных сетей сформированности общих и профессиональных компетенций:

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках

ПК 3.1. Осуществлять проектирование сетевой инфраструктуры.

ПК 3.2. Обслуживать сетевые конфигурации программно-аппаратных средств

ПК 3.3. Осуществлять защиту информации в сети с использованием программно-аппаратных средств.

ПК 3.4. Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры

ПК 3.5. Модернизировать сетевые устройства информационно-коммуникационных систем

ПК 3.6. Проводить мониторинг системы в облачных сервисах

Формы контроля промежуточной аттестации: дифференцированный зачет

Комплект заданий промежуточной аттестации

Билет 1
1. Стеганография и шифрование как способы защиты информации. Криптография и криптоанализ как разделы криптологии. Шифры. Примеры исторических шифров.
2. Процессы информационного взаимодействия (нормальное протекание и отклонения). Угрозы со стороны: злоумышленника, отправителя сообщения, получателя сообщения. Взаимодействие сторон в условии взаимного доверия.

Билет 2
1. Ответственность за преступления в сфере компьютерной информации.
2. Симметричные криптосистемы. Подстановки, перестановки, гаммирование, блочные шифры. Система шифрования Вижинера.

Билет 3
1. Асимметричные криптосистемы. Сравнение систем с открытым и закрытым ключами.
2. Криптоалгоритм RSA.

Билет 4
1. Криптоалгоритм Вернама.
2. Электронная подпись. Задачи, решаемые с помощью электронной подписи. Пример использования алгоритма RSA для электронной подписи. Хэш-функции.

Билет 5
1. Криптографические протоколы. Обмен ключами и вскрытие «человек в середине».
2. Сертификация открытых ключей при помощи цифровой подписи. Алгоритм разделения секрета.

Билет 6
1. Криптоанализ. Виды криптоанализа. Метод вскрытия встреча посередине. Вскрытие со словарем.
2. Атака на криптоалгоритм RSA по выбранному шифротексту. Вскрытие хэш-функций с использованием парадокса дня рождения.

Билет 7
1. Системы защиты программного обеспечения. Классификация систем защиты ПО по методу установки и механизму защиты. Типовые методы защиты ПО.
2. Классификация систем защиты по методу функционирования: упаковщики / шифраторы, СЗ от несанкционированного копирования, СЗ от несанкционированного доступа.

Билет 8
1. Программно-аппаратные средства защиты ПО с электронными ключами. Типы электронных ключей.
2. Условно бесплатные программы. Схемы распространения условно-бесплатных программ. Особенности систем защиты условно-бесплатных программ.

Билет 9
1. Типовые методы защиты условно-бесплатных программ. Статические пароли и генераторы ключей. Многоэшелонные системы защиты. Системы электронной регистрации условно-бесплатных программ.

2. Компьютерные вирусы. Классификация компьютерных вирусов по среде обитания.

Билет 10

1. Резидентные и нерезидентные компьютерные вирусы. Полиморфные вирусы. Стеллс вирусы.
2. Файловые вирусы. Внедрение вируса в программы формата COM. Вирусы спутники.

Билет 11

1. Файловые вирусы. Внедрение в файлы формата EXE. Запись в конец, способ сдвига, способ переноса.
2. Макровирусы. Принципы функционирования полиморфных вирусов.

Билет 12

1. Антивирусные программы. Классификация антивирусных программ. Требования к антивирусным программам.
2. Цели злоумышленников при реализации сетевых атак. Атаки на удаленные сервера и рабочие станции. Атаки на DNS сервера.

Билет 13

1. Атаки на среду передачи информации и узлы коммутации сетей.
2. DoS атаки. Ошибки, приводящие к возможности атак на информацию.

Билет 14

1. Межсетевые экраны (firewalls). Фильтрация пакетов.
2. Межсетевые экраны (firewalls). Фильтры пакетов с контекстной проверкой. Контроль на уровне соединения и на уровне приложений.

Билет 15

1. Международные стандарты информационного обмена.
2. Понятие угрозы.

Билет 16

1. Информационная безопасность в условиях функционирования в России глобальных сетей.
2. Виды противников или «нарушителей».

Билет 17

1. Понятия о видах вирусов.
2. Три вида возможных нарушений информационной системы. Защита.

Билет 18

1. Основные нормативные руководящие документы. Стандарт шифрования данных ГОСТ 28147-89
2. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Билет 19

1. Основные положения теории информационной безопасности информационных систем.
2. Модели безопасности и их применение.

Билет 20
1. Анализ способов нарушений информационной безопасности.
2. Криптографические методы

Билет 21
1. Использование защищенных компьютерных систем.
2. Методы криптографии.

Билет 22
1. Основные технологии построения защищенных ЭИС.
2. Концепция информационной безопасности

Билет 23
1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.

Билет 24
1. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
2. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.

Билет 25
1. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
2. Понятие политики безопасности информационных систем. Назначение политики безопасности.

Билет 26
1. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
2. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.

Билет 27
1. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
2. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.

Билет 28
1. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
2. Основные положения руководящих документов Гостехкомиссии России. Классификация автоматизированных систем по классам защищенности. Показатели защищенности средств вычислительной техники от несанкционированного доступа.

Билет 29
1. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.

2. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).

Билет 30

1. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
2. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.

Билет 31

1. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
2. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).

Билет 32

1. Биометрические средства идентификации и аутентификации пользователей.
2. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.

Билет 33

1. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
2. Законодательный уровень применения цифровой подписи.

Билет 34

1. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
2. Причины нарушения безопасности информации при ее обработке криптографическими средствами.

Билет 35

1. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
2. Распределенные информационные системы. Удаленные атаки на информационную систему.

Билет 36

1. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
2. Физические средства обеспечения информационной безопасности.

Билет 37

1. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
2. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.

Билет 38

1. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
2. Виртуальные частные сети, их функции и назначение.

Критерии оценки:

Оценка «отлично» Дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание по предмету демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком с использованием современной терминологии. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа.

Оценка «хорошо» Дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен литературным языком с использованием современной терминологии. Могут быть допущены 2-3 неточности или незначительные ошибки, исправленные студентом с помощью преподавателя.

Оценка «удовлетворительно» Дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. В ответе отсутствуют выводы. Умение раскрыть значение обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.

Оценка «неудовлетворительно» Ответ представляет собой разрозненные знания с существенными ошибками по вопросу. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь обсуждаемого вопроса по билету с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная, терминология не используется. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента.