Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю) Программно-аппаратные средства защиты информации

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем

Специализация №4

Безопасность автоматизированных систем критически важных объектов

Присваиваемая квалификация (степень)

Специалист по защите информации

Форма обучения

Очная

Год набора 2025

Челябинск, 2025 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность: 10.05.03 Информационная безопасность автоматизированных систем
Специализация: Безопасность автоматизированных систем критически важных объектов
Дисциплина: Программно-аппаратные средства защиты информации
Семестр: 7
Форма промежуточной аттестации: экзамен
Система оценивания: оценивание результатов осуществляется в рамках 5-балльной системы.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Программно-аппаратные средства защиты информации» направлено на формирование следующих компетенций:

Коды компетенции (по ФГОС)	Содержание компетенций согласно ФГОС	Индикаторы достижения компетенций согласно ОПОП	Перечень планируемых результатов обучения по дисциплине
ОПК-2	Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1. Обладает знаниями о современных программных средствах системного и прикладного назначений, в том числе отечественного производства, в своей профессиональной области. ОПК-2.2. Демонстрирует умения применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.	Для достижения индикатора ОПК-2.1: Знать о современных программных средствах системного и прикладного назначений, в том числе отечественного производства, в своей профессиональной области (SecretNet, БлокХост, Аккорд, Соболь, HASP, Guardian, Kaspersky, Dr.Web, Norton, Avast, Eset NOD). Для достижения индикатора ОПК-2.2: Уметь применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности. Для достижения индикатора ОПК-2.2: Владеть навыками применения программных средств системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1 Виды оценочных средств

№ п/п	Контролируемые темы/ разделы	Код компетенции	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации
1	Теоретические аспекты применения программно-	ОПК-2	Собеседование и отчеты по	Вопросы к экзамену (№1-7)

	аппаратных средств обеспечения информационной безопасности.		лабораторным работам. Тест. Реферат	
2	Программно-аппаратные средства обеспечения информационной безопасности	ОПК-2	Собеседование и отчеты по лабораторным работам. Тест. Реферат	Вопросы к экзамену (№8-18)
3	Нормативные документы, регулирующие применение программно-аппаратных средств защиты информации	ОПК-2	Собеседование и отчеты по лабораторным работам. Тест. Реферат	Вопросы к экзамену (№19-23)

3.2 Содержание оценочных средств

Перечень тем лабораторных занятий:

1) Разработка архитектуры системы защиты информации автоматизированной системы с применением программно-аппаратных средств защиты информации.
2) Построение моделей защищенной автоматизированной системы.
3) Изучение методов идентификации и аутентификации с применением программно-аппаратных средств защиты информации.
4) Изучение современных программно-аппаратных средств обеспечения информационной безопасности.
5) Назначение, функции, область применения программно-аппаратных средств защиты информации.
6) Изучение и сравнение особенностей и аналогов программно-аппаратных средств обеспечения информационной безопасности различных категорий.
7) Освоение новых образцов программных средств.
8) Контрольные проверки работоспособности применяемых программно-аппаратных средств защиты информации.
9) Изучение нормативной документации, в том числе руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации.
10) Поиск программно-аппаратных средств защиты информации, соответствующих требованиям руководящих документов.

Критерии оценивания собеседования и отчета по лабораторным работам:

В процессе выполнения практической работы каждый студент составляет индивидуальный отчет, который включает расчетную часть, а также аналитическую часть и выводы. По подготовленному отчету проводится собеседование.

Практическая работа засчитывается студенту, если он представил правильно оформленный отчет, владеет методикой обработки экспериментальных данных; усвоил теоретический материал по данной теме (последовательно, грамотно и логически стройно его излагает, уверенно отвечает на вопросы). Допускаются несущественные неточности в оформлении и ответах на вопросы.

Практическая работа не засчитывается студенту в случаях: наличия ошибок в

расчетах, неправильного оформления отчета, искажающего смысл задания, существенных ошибок при ответах на вопросы.

Примерная тематика рефератов:

1) Дискреционная модель доступа к файлам;
2) Мандатное управление доступом;
3) Проверка целостности файлов;
4) Программа для аутентификации с помощью usb-устройства;
5) Аутентификация с использованием ключа eToken;
6) Разграничение доступа к принтерам;
7) Разграничение доступа к устройствам. Флеш-накопители;
8) Реализация асимметричного шифрования;
9) Реализация симметричного шифрования;
10) Расширение базовой системы аутентификации Windows;
11) Антифишинговый фильтр;
12) Программный межсетевой экран;
13) Разработка защиты от программ слежения за набором на клавиатуре

Реферат – творческая исследовательская работа, основанная, прежде всего, на изучении значительного количества научной и иной литературы по теме исследования. Цель написания реферата – привитие студенту навыков краткого и лаконичного представления собранных материалов и фактов в соответствии с требованиями, предъявляемыми к научным отчетам, обзорам и статьям. Реферат оценивается руководителем исходя из установленных показателей и критериев оценки реферата:

1) Новизна реферированного текста (Макс. - 5 баллов)
- актуальность проблемы и темы;
- новизна и самостоятельность в постановке проблемы, в формулировании нового аспекта выбранной для анализа проблемы;
- наличие авторской позиции, самостоятельность суждений.

2) Степень раскрытия сущности проблемы (Макс. - 5 баллов)
- соответствие плана теме реферата;
- соответствие содержания теме и плану реферата;
- полнота и глубина раскрытия основных понятий проблемы;
- обоснованность способов и методов работы с материалом;
- умение работать с литературой, систематизировать и структурировать материал;
- умение обобщать, сопоставлять различные точки зрения по рассматриваемому вопросу, аргументировать основные положения и выводы.

3) Обоснованность выбора источников (Макс. - 5 баллов)
- круг, полнота использования литературных источников по проблеме;
- привлечение новейших работ по проблеме (журнальные публикации, материалы сборников научных трудов и т.д.).

4) Соблюдение требований к оформлению (Макс. - 5 баллов)
- правильное оформление ссылок на используемую литературу;
- грамотность и культура изложения;
- владение терминологией и понятийным аппаратом проблемы;
- соблюдение требований к объему реферата;
- культура оформления: выделение абзацев.

5) Грамотность (Макс. - 5 баллов)

- отсутствие орфографических и синтаксических ошибок, сти-листических погрешностей;
- отсутствие опечаток, сокращений слов, кроме общепринятых;
- литературный стиль

Реферат оценивается по 25 балльной шкале, балы переводятся в оценки успеваемости следующим образом:
15 баллов и выше - "зачтено"
меньше 15 баллов - "не зачтено"

Рекомендации по написанию реферата:

1) Тема реферата выбирается в соответствии с интересами студента и не обязательно должна соответствовать приведенному примерному перечню. Важно, чтобы в реферате были освящены стороны проблемы, а также представлены теоретические положения и конкретные примеры.
2) Реферат должен основываться на проработке нескольких дополнительных к основной литературе источников. Как правило это научные монографии или статьи.
3) План реферата должен быть авторским. В нем проявляется подход автора, его мнение, анализ проблемы.
4) Все приводимые в реферате факты и заимствованные соображения должны сопровождаться ссылками на источник информации.
5) Недопустимо просто скомпоновать реферат из кусков заимствованного текста. Все цитаты должны быть представлены в кавычках с указанием в скобках источника и страницы.
6) Реферат оформляется в виде текста на листах формата А-4. Работа начинается с титульного листа, в котором указывается название университета, название кафедры, учебной дисциплины, тема реферата, ФИО студента, номер группы, год и географическое место местонахождения университета. Затем следует оглавление с указанием страниц разделов. Сам текст реферата желательно подразделить на разделы: главы, подглавы и озаглавить их. Приветствуется использование в реферате количественных данных и иллюстраций (графики, таблицы, диаграммы, рисунки).
7) Завершают реферат разделы «Заключение» и «Список использованной литературы». В заключении должны быть представлены основные выводы, ясно сформулированные в тезисной форме.
8) Источник литературы должен быть составлен в полном соответствии с действующим стандартом (правилами), включая особую расстановку знаков препинания.

Тест

Тест - система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Важнейшими достоинствами тестов являются:
1) экономия времени преподавателя
2) возможность поставить всех студентов в одинаковые условия
3) возможность разработки равноценных по трудности вариантов вопросов
4) возможность проверить обоснованность оценки
5) уменьшение субъективного подхода к оценке подготовки студента, обусловленного его индивидуальными особенностями
За тест ставится оценка "зачтено", если выполнено правильно более половины заданий.

Тест№1

1. Как называется исторически первый оценочный стандарт:
А) Критерии оценки безопасности информационных технологий
Б) Критерии оценки доверенных компьютерных систем
В) Оранжевая книга
Г) X.800
2. Критерии оценивания степени доверия информационной системе:
А) Конфиденциальность
Б) Политика безопасности
В) Целостность
Г) Уровень гарантированности
3. Какими качествами обладает монитор обращений:
А) Верифицируемость
Б) Полнота
В) Изолированность
Г) Целостность
4. Какие элементы включает в себя политика безопасности:
А) Метки безопасности
Б) Произвольное управление доступом
В) Принудительное управление доступом
Г) Безопасность повторного использования объектов
5. На какие категории делятся средства подчиненности:
А) Идентификация и аутентификация
Б) Аудит
Б) Администрирование
В) Предоставление доверенного пути
6. На какие виды делится гарантированность:
А) Технологическая
Б) Архитектурная
В) Операционная
Г) Канальная
7. Какими критериями должен обладать класс безопасности B2:
А) Пользователи должны идентифицировать себя в вычислительной базе
Б) Доверенная вычислительная база должна создавать, поддерживать и защищать журнал регистрационной информации
В) Снабжаться метками должны все ресурсы системы
Г) Процедура анализа должна быть выполнена для временных тайных каналов
8. Уровень безопасности B, согласно "Оранжевой книге", характеризуется:
А) Верифицируемой безопасностью
Б) Принудительным управлением доступом
В) Произвольным управлением доступом
Г) Признан неудовлетворительным
9. Для реализации сервисов безопасности используются механизмы:
А) Шифрование
Б) Неотказуемость
В) Управление маршрутизацией
Г) Нотаризация
10. По каким направлениям, согласно X.800, должны распространятся усилия

администратора:
А) Администрирование сервисов безопасности
Б) Администрирование механизмов безопасности
В) Администрирование сетей
Г) Администрирование информационной системы в целом

Тест №2

1. Какие защитные механизмы применяются для обеспечения непрерывности функционирования для сетевых конфигураций:
А) Сетевая доверенная вычислительная база
Б) Наличие средств нейтрализации отказов
В) Криптография
Г) Монитор обращений

2. Выберите правильные утверждения для стандарта ISO/IEC 15408:
А) Носит название «Общие критерии»
Б) Издан 1 декабря 1989
В) Можно считать набором библиотек
Г) Является международным стандартом

3. Какие виды требований безопасности содержит стандарт «Критерии оценки безопасности информационных технологий»:
А) Профили защиты
Б) Задания по безопасности
В) Функциональные
Г) Функциональный пакет

4. Что в иерархии класс-семейство-компонент-элемент определяется как минимальный набор требований, фигурирующий как целое:
А) Класс
Б) Семейство
В) Компонент
Г) элемент

5. Сколько функциональных семейств содержится в «Общих критериях»
А) 11
Б) 66
Б) 135
В) Не ограниченное количество

6. Выберите классы функциональных требований «Общих критериев»:
А) Приватность
Б) Анонимность
В) Псевдонимность
Г) Аудит безопасности

7. Что относится к семейству функционального класса «Использование ресурсов»:
А) Невозможность ассоциации
Б) Отказоустойчивость
В) Скрытность
Г) Обслуживание по приоритетам

8. Выделите недостатки функциональных требований «Общих критериев»:
А) Нет готовых классов защиты

Б) Отсутствие объектного подхода
В) Отсутствуют архитектурные требования
Г) Профили защиты носят субъективный характер

9. Назовите типы требования доверия безопасности:

А) Действия разработчиков
Б) Действия оценщиков
В) Управление безопасностью
Г) Представление и содержание свидетельств

10. Какой оценочный уровень доверия предполагает применение неформальной модели политики безопасности:

А) 2
Б) 3
В) 4
Г) 5

Тест №3

1. На какой главной основе строится политика безопасности:

А) Объектно-ориентированный подход
Б) Анализ рисков
В) Тестирование информационной системы
Г) Позиция организации по данному аспекту

2. Для политики безопасности верхнего уровня цели организации информационной безопасности формулируются в терминах:

А) Конфиденциальности
Б) Надежности
В) Целостности
Г) Доступности

3. Что характерно для политики безопасности верхнего уровня:

А) Решает проблемы весьма общего характера
Б) Исходит от руководства организации
В) Решает вопросы конкретных информационных сервисов
Г) Является основой подотчетности персонала

4. С какими аспектами законопослушности и исполнительской дисциплины имеет дело верхний уровень политики безопасности:

А) Система поощрений и наказаний для персонала
Б) Контроль лиц, ответственных за выработку программы безопасности
В) Правила разграничения доступа к производственной информации
Г) Соответствие политики безопасности действующему законодательству

5. Как называется раздел британского стандарта BS 7799:1995, отвечающий за порядок реагирования на нарушения режима безопасности:

А) Управляющий
Б) Классификационный
В) Штатный
Г) Организационный

6. Какие аспекты освещает политика безопасности на среднем уровне:

А) Законопослушность
Б) По отношению к чему (кому) определяется данная политика безопасности

В) Как организован удаленный доступ к сервису
Г) Включает информацию о должностных лицах, ответственных за реализацию политики безопасности

7. Какие вопросы решаются на нижнем уровне политики безопасности:
А) Права доступа к объектам
Б) Как организован удаленный доступ к сервису
В) Роли и обязанности в информационной системе
Г) Чтение и модифицирование данных

8. Какие этапы в жизненном цикле информационного сервиса имеются:
А) Закупка
Б) Эксплуатация
В) Стратегическое планирование
Г) Инициация

9. На каком этапе жизненного цикла информационного сервиса решается вопрос квалификации персонала и уделяется вопросам совместимости нового сервиса с существующей конфигурацией:
А) Эксплуатация
Б) Закупка
В) Инициация
Г) Установка

Тест №4

1. Выберите правильные утверждения для понятия управления рисками:
А) Рассматривается на уровне штатных сотрудников предприятия
Б) Актуальна для всех организаций
В) Уровень риска является вероятностной функцией
Г) Оценка рисков необходима для учета изменений обстановки в области безопасности

2. Управления рисками включает в себя следующие виды деятельности:
А) Оценка рисков
Б) Переоценка рисков
В) Выбор эффективных и экономичных защитных средств
Г) Нейтрализация рисков

3. По отношению к выявленным рискам возможны следующие действия:
А) Уменьшение риска
Б) Переадресация риска
В) Идентификация риска
Г) Принятие риска

4. Какие этапы относятся к нейтрализации рисков:
А) Идентификация активов
Б) Выбор защитных мер
В) Анализ угроз и их последствий
Г) Оценка остаточного риска

5. На каком этапе жизненного цикла информационной системы риски помогают выбрать соответствующие архитектурные решения:
А) Инициация
Б) Закупка
В) Установка

Г) Эксплуатация

6. Недостатки метода CRAMM:

А) Высокая стоимость лицензии

Б) Требует специальной подготовки и высокой квалификации аудитора

В) Не может использоваться для управления рисками на базе периодических оценок на техническом уровне

Г) Не позволяет создавать собственные шаблоны отчетов или модифицировать имеющиеся

7. Если требуется выполнить только разовую оценку уровня рисков в компании, то целесообразно применить

А) CORAS

Б) CRAMM

В) OCTAVE

Г) COBIT

8. Какие типы активов существуют:

А) Информация

Б) Программно-аппаратные средства

В) Персонал организации

Г) Имидж организации

9. В общей формуле определения риска реализации хотя бы одной угрозы из всего перечня актуальных угроз $R = P_{угр} R_n C \frac{K_0 + K_t}{2} 100\%$ **K_t означает:**

А) Ценность актива

Б) Вероятность использования организационных уязвимостей

В) Вероятность реализации хотя бы одной угрозы из всего перечня актуальных угроз

Г) Вероятность использования технических уязвимостей

10. На каком этапе процесса управления рисками используется процедура экранирования для обеспечения безопасности сразу нескольких прикладных сервисов:

А) Оценка рисков

Б) Выбор защитных мер

В) Реализация и проверка выбранных мер

Г) Оценка остаточного риска

Тест №5

1. В каком классе мер процедурного уровня системные ошибки администратора и пользователей наиболее опасны:

А) Управление персоналом

Б) Физическая защита

В) Поддержание работоспособности

Г) Реагирование на нарушения режима безопасности

2. Какими принципами нужно руководствоваться в управлении персоналом:

А) Принцип доверительных отношений

Б) Принцип минимизации привилегий

В) Принцип регламентированных отношений

Г) Принцип разделения обязанностей

3. С какого момента начинается администрирование нового персонала:

А) С приема нового сотрудника
Б) С составления описания должности
В) С момента заведения системного счета
Г) По усмотрению администратора

4. Какие направления физической защиты существуют:
А) Противопожарные меры
Б) Защита мобильных систем
В) Конфигурационное управление
Г) Поддержка программного обеспечения

5. Для какого направления физической защиты характерны такие методы защиты как выбор оборудования с максимальным временем наработки на отказ и дублирование ответственных узлов:
А) Физическое управление доступом
Б) Противопожарные меры
В) Защита поддерживающей инфраструктуры
Г) Защита от перехвата данных

6. Какие направления повседневной деятельности существуют:
А) Проверка стратегии
Б) Обработка перечня возможных аварий
В) Идентификация ресурсов
Г) Документирование

7. Какие аспекты в поддержке программного обеспечения существуют:
А) Поддержка эталонных копий программных средств
Б) Необходимо следить, какое программное обеспечение на компьютерах установлено
В) Контроль за отсутствием неавторизованного изменения программ
Г) Контроль за отсутствием неавторизованного изменения прав к программам и файлам

8. Какие цели преследует реакция на нарушения режима безопасности:
А) Выявление нарушителя
Б) Предупреждение повторных нарушений
В) Локализация инцидента
Г) Уменьшение наносимого вреда

9. Каким категориям относятся критичные ресурсы
А) Персонал
Б) Программная инфраструктура
В) Физическая инфраструктура
Г) Информационная инфраструктура

10. Какие элементы включает в себя информационная инфраструктура:
А) Программы и данные
Б) Компьютеры
В) Документы
Г) Информационные сервисы внешних организаций

Тест №6

1. На что направлены программно-технические меры:
А) На контроль оборудования
Б) На контроль программ
В) На контроль данных
Г) На контроль компьютерных сущностей

2. Почему бурное развитие информационных технологий объективно затрудняет обеспечение надежной защиты:

А) Конкуренция среди производителей программного обеспечения приводит к повышению качества тестирования

Б) Развитие архитектур и микросхем позволяет преодолевать барьеры ранее казавшиеся недоступными

В) Появление новых информационных сервисов ведет к образованию новых уязвимых мест

Г) Развитие сетей сужает круг злоумышленников, имеющих техническую возможность организовать атаки

3. Что относится к вспомогательным сервисам безопасности:

А) Экранирование

Б) Сервисы безопасности

В) Шифрование

Г) Управление

4. Какие виды мер безопасности существуют:

А) Локализующие

Б) Превентивные

В) Восстановления режима безопасности

Г) Прогнозирующие

5. К каким мерам безопасности относится обеспечение отказоустойчивости:

А) Превентивные

Б) Обнаружения нарушений

В) Локализующие

Г) По выявлению нарушителя

6. Какие принципы вытекают из теоретической основы решения проблемы архитектурной безопасности:

А) Необходимость выработки единой политики безопасности

Б) Необходимость обеспечения целостности при сетевых взаимодействиях

В) Не должно быть информационных потоков, идущих к незащищенным сервисам

Г) Необходимость формирования составных сервисов по содержательному принципу

7. Что относится к принципам архитектурной безопасности:

А) Усиление самого слабого звена

Б) Невозможность миновать защитные средства

В) Разнообразие защитных средств

Г) Управляемость информационной системы

8. Иерархическая организация информационной системы необходима для:

А) Повышения надежности информационной системы

Б) Уменьшения ущерба от случайных действий пользователей

В) Обеспечения управляемости системой

Г) Технологических соображений

9. Какие принципы необходимо соблюдать для обеспечения непрерывности функционирования информационной системы:

А) Минимизация объема защитных средств

Б) Внесение в конфигурацию формы избыточности

В) Наличие единой точки отказа

Г) Выделение подсетей и изоляция групп пользователей друг от друга

10. Причины использования минимизации объема защитных средств:

А) Рассредоточенность сетевого управления
Б) Конфигурации клиентских систем трудно или невозможно контролировать
В) Для доступа в корпоративную сеть могут использоваться потребительские устройства с ограниченной функциональностью
Г) Наличие средств обнаружения нештатных ситуаций

Тест №7

1. Идентификация позволяет:
А) Сообщить свое имя
Б) Убедиться, что субъект действительно тот, за кого себя выдает
В) Организовать первую линию бороны
Г) Подтвердить подлинность субъекта
2. Аутентификация бывает
А) Взаимной
Б) Односторонней
В) Двусторонней
Г) Взаимоисключающей
3. По каким причинам затруднена надежность идентификации:
А) Высокая стоимость надежных средств защиты
Б) Необходимо обеспечить защиту от перехвата и изменения данных
В) Отсутствие противоречий между надежностью аутентификации и удобствами
Г) Все аутентификационные сущности можно узнать и украсть
4. Главные достоинства многоразовых паролей
А) Надежность
Б) Простота
В) Дешевизна
Г) Привычность использования
5. Система S/KEY является:
А) Разработкой компании Kerberos
Б) Internet-стандартом
В) Программным генератором одноразовых паролей
Г) Доверенной третьей стороной
6. Kerberos был разработан:
А) В середине 1990-х годов
Б) Компанией Bellcone
В) В Массачусетском технологическом институте
Г) Для генерации нового пароля через небольшой промежуток времени
7. Почему в серверной аутентификации Kerberos субъект C не может просто послать серверу S свой секретный ключ:
А) Сеть является открытой
Б) Сеть является незащищенной
В) Сервер S не знает секретный ключ субъекта C
Г) Сервер S не должен знать секретный ключ субъекта C
8. Какой ответ возвращает Kerberos после посылки ему запроса сведений о субъекте C и сервере S [C⇒{A,B}⇒ Kerberos]:
А) Билет зашифрованный ключом сервера S

Б) Билет зашифрованный ключом субъекта С
В) Дополнительную информацию, зашифрованную ключом сервера S
Г) Дополнительную информацию, зашифрованную ключом субъекта С

9. В биометрии идентификация/аутентификация применяется на основе:
А) Генетических характеристик
Б) Поведенческих характеристик
В) Псевдослучайных характеристик
Г) Физиологических характеристик

10. Почему к биометрии необходимо относиться с осторожностью:
А) Биометрические данные человека меняются
Б) Биометрический шаблон сравнивается с результатом первоначальной обработки характеристик пользователя
В) Отсутствие разницы между применением биометрии на контролируемой территории и без охраны
Г) Биометрические методы не более надежны, чем база данных шаблонов

Тест №8

1. В основе произвольного управления доступом лежит:
А) Идентификатор пользователя
Б) Метка безопасности
В) Сетевой адрес компьютера
Г) Группа пользователя

2. Под управлением доступом полагается:
А) Физическое управление
Б) Логическое управление
В) Ролевое управление
Г) Информационное управление

3. Какие недостатки имеет дискреционное управление доступом:
А) Число связей в них пропорционально произведению количества пользователей на количество объектов.
Б) Рассредоточенность управления доступом
В) Противоречат принципу инкапсуляции
Г) Права доступа существуют отдельно от данных

4. Выберите правильные положения для ролевого управления доступом:
А) У одной роли может быть только один предшественник и несколько наследников, которые называются преемниками
Б) Позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей
В) Для ролей не применим принцип минимизации привилегий
Г) Один пользователь может быть приписан нескольким ролям

5. В статическом разделении обязанностей используется:
А) Временное ограничение доверия
Б) Рассматриваются роли одновременно активные для данного пользователя
В) Налагает ограничения на приписывание пользователей ролям
Г) Задается ограничение «множество ролей-число» (множество состоит как минимум из 1 роли, а число должно быть больше 2)

6. Как называется категория функции, утвержденная стандартом ролевого

управления доступом, которая позволяет приписать пользователю право роли или ликвидировать существующую ассоциацию, создать (удалить) ограничения для статического (динамического) разделения обязанностей:
А) Административные функции
Б) Вспомогательные функции
В) Информационные функции
Г) Односторонние функции
7. Какой подход к управлению доступом используется для Java-среды:
А) Дискреционная
Б) Мандатная
В) Модель фильтрации
Г) Модель «песочница»
8. Как называется потенциально ненадежная программа, поступившая по сети, в модели безопасности JDK 1.0:
А) «Песочница»
Б) Апплет
В) Дескриптор
Г) Предикат
9. Какие понятие были введены в модели безопасности JDK 1.2:
А) Политика безопасности
Б) Право
В) Множество прав
Г) Источник программы
10. Какие перечисленные ограничения можно назвать добровольными:
А) Ограничения на вызываемый метод
Б) Ограничения на вызывающий метод
В) Предикат, описывающий семантику метода
Г) Предикат, описывающий особенности реализации метода

Тест №9

1. Событии при протоколировании делятся на:
А) Клиентские
Б) Объектные
В) Внешние
Г) Внутренние
2. Какие задачи решает протоколирование и аудит:
А) Обеспечение подотчетности пользователей и администраторов
Б) Обнаружение попыток нарушений информационной безопасности
В) Позволяют найти виновника вторжения
Г) Помогают улучшить такой параметр как доступность информации
3. Как сказывается слишком обширное или подробное протоколирование:
А) Снижает производительность сервисов
Б) Облегчает аудит
В) Увеличивает информационную безопасность
Г) Отрицательно сказывается на доступности информации
4. Какие события выделены в «Оранжевой книге» применительно к операционным системам:

А) Вход в систему
Б) Дата и время события
В) Операции с файлами
Г) Результат действия

5. Характерная особенность протоколирования и аудита:
А) Выборочное протоколирование
Б) Зависимость от других средств безопасности
В) Служат отправной точкой подотчетности пользователей
Г) Защищают конфиденциальность и целостность регистрационной информации

6. Обнаружение попыток нарушений информационной безопасности является:
А) Функцией выборочного протоколирования
Б) Функцией сенсора
В) Функцией «Решателя»
Г) Функцией активного аудита

7. Причины сложности организации согласованного протоколирования и аудита в распределенной разнородной системе:
А) Необходимость экранировать некоторые компоненты другими сервисами
Б) Необходимость увязывать между собой события в разных сервисах
В) Некоторые компоненты могут не обладать своими ресурсами протоколирования
Г) Необходимость фиксировать неудачные попытки входа в систему

8. Под подозрительной активностью понимается поведение пользователя или компоненты информационной системы, являющееся:
А) Злоумышленным
Б) Нетипичным согласно принятым критериям
В) Не соответствующим согласно определенной политике безопасности
Г) Неэтичным

9. Достоинства сигнатурного метода:
А) Малое число ошибок 1-го рода
Б) Малое число ошибок 2-го рода
В) Высокая производительность
Г) Умение обнаруживать неизвестные атаки и вариации известных атак

10. Как называются компоненты извлечения регистрационной информации:
А) «Решатели»
Б) Анализаторы
В) Сенсоры
Г) Мониторы

Тест №10

1. Сущность статического режима изучения логики работы программы заключается
А) в выполнение трассировки программы
Б) в изучении исходного текста программы
В) в использование самогенерирующих кодов

2. Динамический режим изучения алгоритма программы предполагает
А) использование самогенерирующих кодов
Б) изучении исходного текста программы
В) выполнение трассировки программы

3. Какой метод может противодействовать дизассемблированию

А) изучение
Б) хэширование
В) шифрование

4. Сущность метода, основанного на использовании самогенерируемых кодов, заключается в том что

А) исполняемые коды программы получаются самой программой в процессе ее выполнения
Б) исполняемые коды программы получаются самой программой после процесса ее выполнения
В) исполняемые коды программы получаются самой программой до процесса ее выполнения

5. Трассировка программ обычно осуществляется с помощью

А) шифрования
Б) программных продуктов, называемых отладчиками
В) самогенерируемых кодов

6. Под компьютерным вирусом понимается

А) программа не имеющая доступ к файлам системы, и не имеющая возможность работать с процессами системы
Б) программа имеющая доступ к файлам системы, и имеющая возможность работать с процессами системы
В) автономно функционирующая программа, обладающая способностью к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ

7. Резидентные вирусы - это

А) вирусы, которые выполняются только в момент запуска зараженной программы
Б) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам
В) вирусы, заражающие программы, хранящиеся в системных областях дисков

8. Транзитные вирусы – это

А) вирусы, которые выполняются только в момент запуска зараженной программы
Б) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам
В) вирусы, заражающие программы, хранящиеся в системных областях дисков

9. Вирусы-мутанты (MtE-вирусы) – это

А) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса
Б) вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных
В) вирусы, заражающие программы, хранящиеся в системных областях дисков

10. Stealth-вирусы – это

А) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам
Б) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса
В) вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных

11. Загрузочные (бутовые) вирусы – это

А) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам

Б) вирусы, заражающие программы, хранящиеся в системных областях дисков

В) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса

12. Троянские программы – это

А) программы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса

Б) программы которые содержат скрытые последовательности команд (модули), выполняющие действия, наносящие вред пользователям

В) программы которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам

13. Файловые вирусы – это

А) вирусы, заражающие файлы с программами

Б) вирусы, заражающие программы, хранящиеся в системных областях дисков

В) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам

Тест №11

1. На какие типы делятся файлы в системе NTFS:

А) Файлы метаданных

Б) Файлы данных

В) Обычные файлы

Г) Скрытые файлы

2. В каком файле метаданных содержится набор общих дескрипторов безопасности:

А) MFT

Б) $Secure

В) Зеркало MFT

Г) ACL (ACE)

3. Какой файл метаданных содержит индексы каталогов и хранит атрибуты файлов и папок:

А) SACLs

Б) DACLs

В) MFT

Г) $Secure

4. Какой тип ACE-записи перечисляет операции, которые должны проверяться для данного объекта:

А) System Audit ACE

Б) Allow ACE

В) Deny ACE

Г) SID ACE

5. Группа Power Users (Опытные пользователи) принадлежит:

А) Встроенной группе безопасности

Б) Назначенной группе безопасности

В) Неявной группе безопасности

Г) Особой группе безопасности

6. Какие из следующих утверждений верным образом описывают NTFS-разрешения для файлов и папок?

А) NTFS-защита эффективна только при получении пользователем доступа к файлам и папкам по сети

Б) NTFS-защита эффективна при получении пользователем доступа к файлам и папкам с локального компьютера (напрямую)

В) NTFS-разрешения используются для определения того, какие пользователи и группы могут получить доступ к файлам и папкам, и того, что они могут делать с их содержимым

Г) NTFS-разрешения могут быть использованы на всех файловых системах

7. Какие из следующих NTFS-разрешений для папки позволяют удалить ее?

А) Read

Б) Read&Execute

В) Modify

Г) Change

8. Кто из следующих пользователей может задавать разрешения учетным записям пользователей и группам?

А) Administrators (Администраторы)

Б) Power Users (Опытные пользователи)

В) Пользователи с разрешением Full Control (Полный доступ)

Г) Владельцы файлов и папок

9. Какие из следующих утверждений о копировании файла или папки верны?

А) При копировании файла из одной папки в другую, на том же томе, разрешения не меняются

Б) При копировании файла из папки на NTFS-томе в папку на FAT-томе, разрешения для файла не меняются

В) При копировании файла из папки на NTFS-томе в папку на другом NTFS-томе, разрешения для файла соответствуют разрешениям папки-адресата

Г) При копировании файла из папки на NTFS-томе в папку на FAT-томе, разрешения теряются

10. Какие из следующих утверждений о перемещении файла или папки верны?

А) При перемещении файла из одной папки в другую, на том же томе, разрешения не меняются

Б) При перемещении файла из папки на NTFS-томе в папку на FAT-томе, разрешения для файла не меняются

В) При перемещении файла из папки на NTFS-томе в папку на другом NTFS-томе, разрешения для файла соответствуют разрешениям папки-адресата

Г) При перемещении файла из папки на NTFS-томе в папку на том же NTFS-томе, разрешения для файла соответствуют разрешениям папки-адресата

Тест №12

1. Какие из следующих функций выполняет Cipher?

А) Находит фрагментированные файлы и папки и выстраивает их в непрерывном виде

Б) Ищет и пытается исправить ошибки файловой системы

В) Позволяет шифровать и расшифровать файлы и папки из командной строки

Г) Удаляет временные и кэшируемые файлы

2. Что из нижеперечисленного относится к разрешениям общей папки?

А) Read

Б) Write
В) Modify
Г) Full Control

3. Какая часть дискового пространства отводится по умолчанию под кэш для обеспечения автономного доступа к общим папкам?

А) 5%
Б) 10%
В) 15%
Г) 20%

4. Какие из следующих утверждений относительно сочетания разрешений общей папки и NTFS-разрешений являются верными?

А) Разрешения общих папок можно использовать во всех общих папках
Б) Разрешение общей папки Change является более строгим, чем NTFS-разрешение Read
В) NTFS-разрешения можно использовать во всех общих папках
Г) Разрешение общей папки Read является более строгим, чем NTFS-разрешение Change

5. Способы предоставления доступа к папкам:

А) Команды NET SHARE
Б) Посредством консоли «Управление компьютером»
В) Windows Explorer
Г) Диалоговое окно Caching Settings

6. Какие из следующих утверждений относительно разрешений общей папки и NTFS-разрешений являются верными?

А) NTFS-разрешения применяются только тогда, когда доступ предоставляется по сети
Б) NTFS-разрешения применяются независимо от того, как предоставляется доступ – локально или по сети
В) Разрешения общей папки применяются только тогда, когда доступ предоставляется по сети
Г) Разрешения общей папки применяются независимо от того, как предоставляется доступ – локально или по сети

7. При переименовании общей папки, исходная папка

А) Перестает быть общедоступной
Б) По-прежнему остается общей
В) Задается вручную пользователем

8. Вам необходимо обеспечить, чтобы любой файл мог быть восстановлен и срок его последней актуальной архивной копии составлял не более 24 часов. Кроме того, вы не хотите задействовать более одного носителя. Время, затрачиваемое на выполнение архивации, не имеет значения. Какая стратегия архивации наиболее полно подойдет в этом случае?

А) Еженедельная обычная и ежедневные разностные архивации
Б) Еженедельная обычная и ежедневные добавочные архивации
В) Ежедневные обычные архивации
Г) Еженедельная обычная и ежедневные разностные архивации, с проведением копирующей архивации в среду

9. Вы установили новый драйвер устройства для звуковой карты, и теперь система не будет загружаться. Какая технология восстановления позволит системе загрузиться с предыдущим набором драйверов?

А) Recovery Console

Б) Last Known Good Configuration
В) Automated System Recovery (ASR)
Г) Safe Mode

10. Какой из следующих шаблонов безопасности можно использовать для восстановления настроечных параметров системы безопасности в случае неполадок с настройками?

А) Compatws.inf
Б) Hisecwc.inf
В) Setup security.inf
Г) Rootsec.inf

Вопросы к экзамену:

1) Понятие политики безопасности. Описание типовых политик безопасности.
2) Угрозы безопасности компьютерных систем. Модель компьютерной системы.
3) Понятие монитора безопасности. Концепция диспетчера доступа.
4) Обеспечение гарантий выполнения политики безопасности.
5) Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности.
6) Модели безопасного взаимодействия в КС.
7) Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды.
8) Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности.
9) Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности.
11) Взаимодействие с общесистемными компонентами вычислительных систем.
12) Методы и средства ограничения доступа к компонентам вычислительных систем.
13) Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
14) Управление ключами криптографическими ключами. Методы и средства хранения ключевой информации.
15) Защита программ от изучения.
16) Способы встраивания средств защиты в программное обеспечение.
17) Защита от разрушающих программных воздействий и вредоносного программного обеспечения.
18) Защита программ от изменения и контроль целостности.
19) Роль стандартов информационной безопасности. Документы Государственной технической комиссии России.
20) Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
21) Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
22) Показатели защищенности средств вычислительной техники от несанкционированного доступа. Классы защищенности автоматизированных систем.
23) Требования к процессу сертификации продукта информационных технологий

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

Студент допускается к экзамену по дисциплине в случае выполнения им учебного плана по дисциплине: выполненных и защищенных работ. В случае наличия учебной задолженности студент отрабатывает пропущенные занятия в форме, предложенной преподавателем и представленной в настоящей программе.

Экзамен проводится по билетам в устной форме. При проведении экзамена экзаменуемый выбирает билет в случайном порядке. Экзаменатору предоставляется право по ходу экзамена задавать экзаменуемому уточняющие и дополнительные вопросы. Время подготовки студента для устного ответа на экзамене должно составлять не менее 40 минут, время ответа экзаменуемого – не более 20 минут. При подготовке и ответе на вопросы билета экзаменуемый должен вести необходимые записи в листе устного ответа, который по окончании экзамена подписывается студентом, сдаётся экзаменатору и сохраняется им до окончания экзаменационной сессии. Студент, испытавший затруднения при подготовке к ответу по выбранному билету, вправе выбрать второй билет с продлением времени на подготовку. При этом окончательная оценка студента снижается на один балл. Выбор студентом третьего билета не допускается.

Проявленные студентом в ходе экзамена знания оцениваются оценками «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств

Критерии оценивания ответа (устного опроса) на экзамене:

Оценка «отлично» выставляется:

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. Знания 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» выставляется:

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 некоторые неточности или незначительные ошибки, исправленные студентом с помощью преподавателя.

Оценка «удовлетворительно» выставляется:

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» выставляется:

1) 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. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента.

2) Ответ на вопрос полностью отсутствует.

3) Отказ от ответа.

Особенности проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обозначены в рабочей программе дисциплины (модуля).

4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

1. Высокий уровень сформированности компетенций соответствует оценке «отлично».
2. Средний уровень сформированности компетенций соответствует оценке «хорошо».
3. Базовый уровень сформированности компетенций соответствует оценке «удовлетворительно».
4. Низкий уровень сформированности компетенций соответствует оценке «неудовлетворительно».

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:
Проректор по учебной работе утверждено 24.02.25 А.А. Саламатов

Ученым советом физического факультета

Протокол заседания № 05 от 06.02.2025

Председатель Ученого совета
физического факультета согласовано М.А. Загребин

Заседанием кафедры радиофизики и электроники

Протокол заседания № 07 от 04.02.2025

Заведующий кафедрой согласовано А.В. Бутаков

Автор (составитель) А.В. Бутаков

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1