

Министерство просвещения РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Глазовский государственный инженерно-педагогический университет имени В.Г. Короленко»

*Рассмотрено и утверждено на заседании кафедры
математики и информатики
Протокол № 7 от 19.02.2025*

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации в форме дифференцированного зачета по
учебной дисциплине

ОП.10 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
название дисциплины

специальность: 09.02.01 Компьютерные системы и комплексы
квалификация выпускника: специалист по компьютерным системам

Глазов, 2025

Требования ФГОС к образовательным результатам:

В результате освоения дисциплины обучающийся должен уметь :	<ul style="list-style-type: none">- Получать информацию о параметрах компьютерной системы.- Подключать дополнительное оборудование и настраивать связь между элементами компьютерной системы.- Производить инсталляцию и настройку программного обеспечения компьютерных систем.
В результате освоения дисциплины обучающийся должен знать :	<ul style="list-style-type: none">- Базовые понятия и основные принципы построения архитектур вычислительных систем.- Типы вычислительных систем и их архитектурные особенности.- Организацию и принцип работы.- Основных логических блоков компьютерных систем.- Процессы обработки информации на всех уровнях компьютерных архитектур; основные компоненты программного обеспечения компьютерных систем.- Основные принципы управления ресурсами и организации доступа к этим ресурсам.

Уважаемый студент! Вам предлагается выполнить 30 заданий в тестовой форме для контроля усвоенных знаний и практическое задание для оценки усвоенных умений. Каждая часть дифзачета оценивается. Итоговая оценка складывается как среднее арифметическое двух заданий, с учетом текущей успеваемости по учебной дисциплине.

Задания для проверки усвоения знаний.

Критерии оценки тестовых заданий.

Правильный ответ на вопрос оценивается в 1 балл, неправильный ответ или его отсутствие – ноль баллов.

Оценка	Процент правильных ответов
5(отлично)	90% - 100%
4(хорошо)	70% - 89%
3(удовлетворительно)	55% - 69%
2(неудовлетворительно)	54% и менее

Время на выполнение заданий: 1 академический час.

2. Оценка освоения теоретического курса дисциплины

2.1. Контрольные вопросы для оценки усвоения знаний

1. Общие проблемы безопасности. Роль и место информационной безопасности.
2. Угрозы безопасности информации. Классификация угроз. Методы профилактики угроз.
3. Основные принципы защиты информации. Комплексный подход к построению системы безопасности и защите информации.
4. Политика государства в области информационной безопасности.
5. Административные методы защиты информации. Политика безопасности. Разграничение доступа к информации. Идентификация субъектов и контроль за их действиями.

6. Правовые методы защиты информации за рубежом. Политика безопасности организации.
7. Программно-математические средства защиты информации. Контроль доступа к информации, ее подлинности и целостности. Обнаружение вторжения и контроль активности.
8. Технические средства защиты информации. Технологии хранения, резервного копирования и разграничения доступа к информации.
9. Угрозы и нарушители безопасности информации.
10. Основные принципы построения систем видеонаблюдения.
11. Модель угроз безопасности информации.
12. Меры обеспечения защиты информации.
13. Методы контроля и разграничения доступа.
14. Исторический обзор криптографических методов защиты информации.
15. Криптография, криптология и криптоанализ. Классификация криптоалгоритмов. Процесс криптографического закрытия данных (программное и аппаратное). Требования к алгоритму шифрования.
16. Классификация компьютерных вирусов. Способы распространения и среда обитания вирусов. Методы защиты. Меры профилактики.
17. Основные виды антивирусных программ. Основные методы антивирусной защиты. Состав антивирусной программы.
18. Компьютерные преступления. Организационно-технические меры и программно-технические аспекты борьбы с компьютерной преступностью.
19. Способы защиты информации средствами ОС, идентификация пользователя в ОС, разграничения прав пользователей в клиентских ОС.
20. Компьютерное пиратство. Виды нелегального использования продуктов интеллектуальной деятельности. Способы защиты информационных продуктов от незаконного копирования и взлома. Права и обязанности субъектов в области защиты информации.

2.2. Типовые задания для оценки освоенных умений:

1. Для выбранного объекта защиты информации описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:
2. Провести анализ увеличения защищенности объекта защиты информации по следующим разделам:

Наименование объекта защиты информации:

1. Одиночно стоящий компьютер в бухгалтерии.
2. Сервер в бухгалтерии.
3. Почтовый сервер.
4. Веб-сервер.
5. Компьютерная сеть материальной группы.
6. Одноранговая локальная сеть с выходом в Интернет.
7. Сеть с выделенным сервером без выхода в Интернет.
8. Сеть с выделенным сервером с выходом в Интернет.
9. Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях.
10. Телефонная сеть.
11. Средства телекоммуникации (радиотелефоны, мобильные телефоны, пейджеры).
12. Банковские операции (внесение денег на счет и снятие).
13. Операции с банковскими пластиковыми карточками.
14. Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.
15. Компьютер, хранящий конфиденциальную информацию о разработках предприятия.

16. Материалы для служебного пользования на твердых носителях в производстве.
17. Материалы для служебного пользования на твердых носителях в архиве.
18. Комната для переговоров по сделкам на охраняемой территории.
19. Комната для переговоров по сделкам на неохраняемой территории.
20. Сведения для средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.).
21. Судебные материалы (твердая копия).
22. Материалы по владельцам автомобилей (твердая копия, фотографии, электронные носители и др.).
23. Материалы по недвижимости (твердая копия, фотографии, электронные носители и др.).
24. Сведения по тоталитарным сектам и другим общественно-вредным организациям.
25. Сведения по общественно-полезным организациям (красный крест и др.).

3. Структура контрольно-оценочных материалов (КОМ) для экзамена

I. ПАСПОРТ

Назначение:

КОМ предназначены для контроля и оценки результатов освоения дисциплины Элементы математической логики по специальности *09.02.07 Информационные системы и программирование*.

Освоенные умения:

1. Работать с современными case-средствами.
2. Устанавливать, настраивать и работать с системным программным обеспечением.
3. Создавать, устанавливать, настраивать и работать с антивирусным и криптографическим программным обеспечением.
4. Обеспечивать организацию доступа пользователей информационной системы к данным
5. Проектировать логическую и физическую среду данных предприятия.
6. Создавать хранимые процедуры и триггеры на базах данных.
7. Применять стандартные методы защиты информационных объектов.
8. Выполнять стандартные процедуры резервного копирования и мониторинга выполнения этой процедуры.
9. Выполнять процедуру восстановления данных и вести мониторинг выполнения этой процедуры.
10. Обеспечивать информационную безопасность на уровне автоматизированной системы.

Усвоенные знания:

1. Основные виды угроз и методы их профилактики.
2. Основные положения теории защиты информации, хранилищ данных, баз знаний.
3. Основные принципы построения комплексной системы защиты информации, принципы структуризации и нормализации данных.
4. Основные принципы построения концептуальной, логической и физической модели данных.
5. Общий подход к организации представлений, таблиц, индексов и кластеров;
6. Методы организации целостности данных.
7. Основные виды компьютерных преступлений, способы контроля доступа к данным и управления привилегиями.
8. Основные методы и средства организации комплексной защиты данных, защиты информации.
9. Правовые основы обеспечения информационной безопасности.

10. Основные виды вирусов, заражаемые объекты и способы распространения.

11. Виды, назначение и функции антивирусных программ.

II. ИНСТРУКЦИЯ ДЛЯ ЭКЗАМЕНУЮЩЕГОСЯ

Инструкция для обучающихся

Уважаемый студент,
Вам предлагается теоретический вопрос и практическое задание

Время выполнения всех заданий – 2 академических часа без перерыва

Задания – экзаменационные билеты (Прилагаются).

Оборудование: Бумага, ручка, вариант задания (билет).

III. ЗАДАНИЕ ДЛЯ ЭКЗАМЕНУЮЩЕГОСЯ

Задания представлены в ПРИЛОЖЕНИИ А.

Критерии оценки заданий представлены в ПРИЛОЖЕНИИ Б.

IV. ПАКЕТ ЭКЗАМЕНАТОРА

IV а. УСЛОВИЯ ПРОВЕДЕНИЯ ЭКЗАМЕНА

Экзамен проводится по подгруппам в количестве 15 человек (или целой группой).

Количество вариантов задания для экзаменуемого – каждому 1

Задания предусматривают одновременную проверку усвоенных знаний и освоенных умений по всем профессионально значимым темам программы.

Ответы предоставляются письменно/устно/ в электронном виде на электронных носителях.

Время выполнения задания - 2 академических часа.

IV б. ЗАДАНИЕ ДЛЯ ЭКЗАМЕНУЮЩЕГОСЯ

Задания представлены в ПРИЛОЖЕНИИ А.

IV в. ЭТАЛОНЫ ОТВЕТОВ

Эталоны ответов представлены в ПРИЛОЖЕНИИ В. *(представляются ответы на расчетные задачи, краткая схема ответа и т.д.)*

IV г. КРИТЕРИИ ОЦЕНКИ

Критерии оценки представлены в ПРИЛОЖЕНИИ Б.

IV д. ЭКЗАМЕНАЦИОННАЯ ВЕДОМОСТЬ

Экзамен оформляется экзаменационной ведомостью, которая сдается в деканат

ПРИЛОЖЕНИЕ А

ЭКЗАМЕНАЦИОННЫЕ ЗАДАНИЯ

Экзаменационные билеты

БИЛЕТ № 1

1. Общие проблемы безопасности. Роль и место информационной безопасности.
2. Для выбранного объекта защиты информации описать объект защиты, провести анализ защищенности объекта защиты информации: Комната для переговоров по сделкам на охраняемой территории.

БИЛЕТ № 2

1. Технические средства защиты информации. Технологии хранения, резервного копирования и разграничения доступа к информации.
2. Провести анализ увеличения защищенности объекта защиты информации: Материалы для служебного пользования на твердых носителях в производстве.

БИЛЕТ № 3

1. Основные виды антивирусных программ. Основные методы антивирусной защиты. Состав антивирусной программы.
2. Для выбранного объекта защиты информации описать объект защиты, провести анализ защищенности объекта защиты информации: Материалы для служебного пользования на твердых носителях в архиве.

БИЛЕТ № 4

1. Криптография, криптология и криптоанализ. Классификация криптоалгоритмов. Процесс криптографического закрытия данных (программное и аппаратное). Требования к алгоритму шифрования.
2. Провести анализ увеличения защищенности объекта защиты информации: Компьютер, хранящий конфиденциальную информацию о разработках предприятия.

БИЛЕТ № 5

1. Меры обеспечения защиты информации.

2. Для выбранного объекта защиты информации описать объект защиты, провести анализ защищенности объекта защиты информации: Средства телекоммуникации (радиотелефоны, мобильные телефоны, пейджеры).

БИЛЕТ № 6

1. Исторический обзор криптографических методов защиты информации.
2. Провести анализ увеличения защищенности объекта защиты информации: Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях.

БИЛЕТ № 7

1. Модель угроз безопасности информации.
2. Для выбранного объекта защиты информации описать объект защиты, провести анализ защищенности объекта защиты информации: Сведения для средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.).

БИЛЕТ № 8

1. Основные принципы построения систем видеонаблюдения.
2. Провести анализ увеличения защищенности объекта защиты информации: Сеть с выделенным сервером с выходом в Интернет.

БИЛЕТ № 9

1. Угрозы и нарушители безопасности информации.
2. Для выбранного объекта защиты информации описать объект защиты, провести анализ защищенности объекта защиты информации: Компьютерная сеть материальной группы.

БИЛЕТ № 10

1. Программно-математические средства защиты информации. Контроль доступа к информации, ее подлинности и целостности. Обнаружение вторжения и контроль активности.
2. Провести анализ увеличения защищенности объекта защиты информации: Сеть с выделенным сервером без выхода в Интернет.

БИЛЕТ № 11

1. Методы контроля и разграничения доступа.
2. Для выбранного объекта защиты информации описать объект защиты, провести анализ защищенности объекта защиты информации: Почтовый сервер.

БИЛЕТ № 12

1. Классификация компьютерных вирусов. Способы распространения и среда обитания вирусов. Методы защиты. Меры профилактики.
2. Провести анализ увеличения защищенности объекта защиты информации: Комната для переговоров по сделкам на неохраямой территории.

БИЛЕТ № 13

1. Административные методы защиты информации. Политика безопасности. Разграничение доступа к информации. Идентификация субъектов и контроль за их действиями.
2. Для выбранного объекта защиты информации описать объект защиты, провести анализ защищенности объекта защиты информации: Одноранговая локальная сеть с выходом в Интернет.

БИЛЕТ № 14

1. Правовые методы защиты информации за рубежом. Политика безопасности организации.
2. Провести анализ увеличения защищенности объекта защиты информации: Материалы по недвижимости (твердая копия, фотографии, электронные носители и др.).

БИЛЕТ № 15

1. Компьютерные преступления. Организационно-технические меры и программно-технические аспекты борьбы с компьютерной преступностью.
2. Для выбранного объекта защиты информации описать объект защиты, провести анализ защищенности объекта защиты информации: Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.

БИЛЕТ № 16

1. Угрозы безопасности информации. Классификация угроз. Методы профилактики угроз.
2. Провести анализ увеличения защищенности объекта защиты информации: Сервер в бухгалтерии.

БИЛЕТ № 17

1. Основные принципы защиты информации. Комплексный подход к построению системы безопасности и защите информации.
2. Для выбранного объекта защиты информации описать объект защиты, провести анализ защищенности объекта защиты информации: Судебные материалы (твердая копия).

БИЛЕТ № 18

1. Способы защиты информации средствами ОС, идентификация пользователя в ОС, разграничения прав пользователей в клиентских ОС.
2. Провести анализ увеличения защищенности объекта защиты информации: Одиночно стоящий компьютер в бухгалтерии.

БИЛЕТ № 19

1. Политика государства в области информационной безопасности.
2. Для выбранного объекта защиты информации описать объект защиты, провести анализ защищенности объекта защиты информации: Веб-сервер.

БИЛЕТ № 20

1. Компьютерное пиратство. Виды нелегального использования продуктов интеллектуальной деятельности. Способы защиты информационных продуктов от незаконного копирования и взлома. Права и обязанности субъектов в области защиты информации.
2. Провести анализ увеличения защищенности объекта защиты информации: Сведения по общественно-полезным организациям (красный крест и др.).

ПРИЛОЖЕНИЕ Б

КРИТЕРИИ ОЦЕНКИ

Условием положительной аттестации (**«отлично»**) на экзамене является самостоятельное и уверенное применение знаний в практической деятельности, полное изложение полученных знаний при ответе на теоретическое задание, в соответствии с требованиями учебной программы, формулировка выводов и обобщений. Допускаются единичные несущественные ошибки, самостоятельно исправленные студентом.

Практическая часть уровня **«С»** билета выполнена.

Студент, получает оценку **«хорошо»**, если при изложении полученных знаний возникают отдельные несущественные ошибки, исправляемые студентом по указанию преподавателя, и выполнение заданий осуществляется с незначительной помощью преподавателя.

Практическая часть уровня **«В»** билета выполнена.

Студент, получает оценку **«удовлетворительно»**, если изложение полученных знаний неполное, что, в целом, не препятствует усвоению последующего программного материала, допускаются отдельные существенные ошибки, исправляемые с помощью преподавателя, возникают затруднения при выделении существенных признаков изученного и формулировке выводов.

Выявлены существенные затруднения в выполнении практической части уровня **«А»** билета.

Студент, получает оценку **«неудовлетворительно»** за работу, выполненную в не полном объеме (менее 50% правильно выполненных заданий от общего объема работы).

Практическая часть билета не выполнена.

ПРИЛОЖЕНИЕ В

ЭТАЛОНЫ ОТВЕТОВ

Ответы к теоретическим вопросам билета

Схема ответа

1. Общие проблемы безопасности. Роль и место информационной безопасности. Национальная безопасность. Государственная, военная, экономическая, информационная, экологическая, безопасность личности и информационные технологии, виды безопасности, классификация средств шпионажа, СМИ и интернет манипуляция сознанием.
2. Угрозы безопасности информации. Классификация угроз. Методы профилактики угроз. Понятие угрозы безопасности информации. Виды угроз безопасности информации. Источники угроз безопасности информации. Нарушители безопасности информации. Виды и цели нарушителей. Потенциал и возможности нарушителей. Способы реализации угроз нарушителем.
3. Основные принципы защиты информации. Комплексный подход к построению системы безопасности и защите информации. Понятие информации. Доступ к информации. Информационные системы. Обработка информации. Защита информации. Информационная безопасность
4. Политика государства в области информационной безопасности. Стратегия национальной безопасности. Доктрина информационной безопасности. Законодательство в области защиты информации. Государственная тайна. Коммерческая тайна. Персональные данные
5. Административные методы защиты информации. Политика безопасности. Разграничение доступа к информации. Идентификация субъектов и контроль за их действиями. Законодательные меры защиты информации. Административные меры защиты информации. Управление рисками. Политика безопасности организации. Управление персоналом. Планирование действий в чрезвычайных ситуациях. Организационно-технические меры защиты информации. Физическая защита объекта информатизации. Защита поддерживающей инфраструктуры.
6. Правовые методы защиты информации за рубежом. Политика безопасности организации. Понятие политики безопасности. Назначение и содержание политики безопасности. Вопросы, рассматриваемые в политике безопасности. Организационные аспекты информационной безопасности. Управление активами. Безопасность, связанная с управлением персоналом. Физическая безопасность. Управление доступом. Вопросы эксплуатации информационных систем. Управление инцидентами и непрерывностью бизнеса. Соответствие требованиям обязательств организации. Жизненный цикл политики безопасности.
7. Программно-математические средства защиты информации. Контроль доступа к информации, ее подлинности и целостности. Обнаружение вторжения и контроль активности. Сервисы безопасности. Антивирусная защита. Типы вредоносных программ. Принципы обнаружения вредоносных программ. Выбор антивирусных средств. Межсетевое экранирование. Системы предотвращения утечки информации. Протоколирование и аудит.
8. Технические средства защиты информации. Технологии хранения, резервного копирования и разграничения доступа к информации.
9. Угрозы и нарушители безопасности информации. Назначение модели угроз ИБ. Идентификация угроз безопасности информации и их источников. Модель нарушителя. Принцип оценки актуальности угроз. Оценка возможности реализации угрозы. Оценка степени ущерба. Оценка актуальности угрозы.
10. Основные принципы построения систем видеонаблюдения.

Особенности и принципы построения систем видеонаблюдения. Выбор технологических решений, способы прокладки кабеля, тип, назначение и параметры оборудования и материалов, планируемый бюджет.

11. Модель угроз безопасности информации.

Оценка актуальности угрозы. Назначение модели угроз ИБ. Идентификация угроз безопасности информации и их источников.

12. Меры обеспечения защиты информации.

Организация защиты информации (ЗИ). Организационные меры ЗИ. Законодательные меры ЗИ. Административные меры ЗИ. Организационно-технические меры ЗИ. Программно-технические средства ЗИ. Криптографические методы ЗИ. Стеганографические методы ЗИ. Методы и средства технической ЗИ. Исторический обзор стеганографии. Основные понятия стеганографии. Основные угрозы безопасности стеганографических систем. Типы нарушителей безопасности стеганографических систем. Типы атак на стеганографические системы. Компьютерная и цифровая стеганография. Сфера применения методов стеганографической защиты информации.

13. Методы контроля и разграничения доступа.

Основные понятия контроля доступа субъектов. Аутентификация субъектов доступа. Аутентификация на основе знания. Аутентификация на основе владения. Аутентификация на основе признаков или действий. Разграничение доступа. Дискреционная модель разграничения доступа. Мандатная модель разграничения доступа. Ролевая модель разграничения доступа.

14. Исторический обзор криптографических методов защиты информации.

Понятие шифра. Шифр простой замены и его анализ. Шифры перестановки и их анализ.

Варианты усложнения шифра простой замены. Шифр многоалфавитной замены и его анализ.

Требования к шифрам - принцип Керхгофса. Шифровальные машины и подходы к их анализу. Идеальный шифр и классы стойкости шифров.

15. Криптография, криптология и криптоанализ. Классификация криптоалгоритмов. Процесс криптографического закрытия данных (программное и аппаратное). Требования к алгоритму шифрования.

Требования к современным криптографическим системам. Шифры на основе сети Фейстеля.

Шифры на основе SP-сети. Асимметричные системы шифрования. Схемы электронной цифровой подписи. Хэш-функции. Криптографические протоколы. Перспективы криптографии.

16. Классификация компьютерных вирусов. Способы распространения и среда обитания вирусов. Методы защиты. Меры профилактики.

17. Основные виды антивирусных программ. Основные методы антивирусной защиты. Состав антивирусной программы.

Резидентный монитор. Модуль проверки электронной почты и дополнительные плагины для The Bat!, Outlook. Планировщик заданий. Модуль обновления через Интернет. Хранилище (карантин) для зараженных файлов. Модуль создания аварийного диска с DOS-версией программы, обнаружение потенциально нежелательных программ.

18. Компьютерные преступления. Организационно-технические меры и программно-технические аспекты борьбы с компьютерной преступностью.

Основные понятия технической защиты информации. Назначение систем обнаружения и предотвращения компьютерных атак. Понятие компьютерной атаки. Требования к системам обнаружения и предотвращения компьютерных атак. Классификация систем обнаружения и предотвращения компьютерных атак. Технические каналы утечки информации. Акустический канал утечки информации. Оптический канал утечки информации. Радиоэлектронный канал утечки информации. Принципы осуществления технической разведки.

Принципы защиты от технической разведки.

19. Способы защиты информации средствами ОС, идентификация пользователя в ОС, разграничения прав пользователей в клиентских ОС.

Системы анализа защищенности. Системы обнаружения атак. Системы контроля целостности. Системы анализа журналов регистрации. Размещение систем обнаружения и предотвращения атак в информационной системе. Критерии выбора систем обнаружения и предотвращения компьютерных атак.

20. Компьютерное пиратство. Виды нелегального использования продуктов интеллектуальной деятельности. Способы защиты информационных продуктов от незаконного копирования и взлома. Права и обязанности субъектов в области защиты информации.

Ответы на практические задания билета

Схема ответа

1. Для выбранного объекта защиты информации описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:
 - a. виды угроз;
 - b. характер происхождения угроз;
 - c. классы каналов несанкционированного получения информации;
 - d. источники появления угроз;
 - e. причины нарушения целостности информации;
 - f. потенциально возможные злоумышленных действий;
 - g. определить класс защиты информации.
2. Провести анализ увеличения защищенности объекта защиты информации по следующим разделам:
 - a. определить требования к защите информации;
 - b. классифицировать автоматизированную систему;
 - c. определить факторы, влияющие на требуемый уровень защиты информации;
 - d. выбрать или разработать способы и средства защиты информации;
 - e. построить архитектуру систем защиты информации;
 - f. сформулировать рекомендации по увеличению уровня защищенности.