МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Частное учреждение высшего образования
«Высшая школа предпринимательства (институт)»
(ЧУВО «ВШП»)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.04 «Информационная безопасность»

Направление подготовки: 09.03.02 Информационные системы и технологии

Направленность (профиль) программы бакалавриата
«Информационные системы в экономике»

ОДОБРЕНО
Ученым советом ЧУВО «ВШП»
Протокол заседания
№01-02/23 от 15 мая 2023 г.

УТВЕРЖДАЮ
Ректор ЧУВО «ВШП»
15 мая 2023 г.
Ректор _____ Аллабян М.Г.

Документ подписан электронной цифровой подписью
VSHP EDS GEN 1, уникальный ключ документа:
8F30-29EE-EB2F-GNI5
Организация: ЧУВО «ВШП», ИНН: 6903013604
Дата подписания: 15.05.2023
Подписал: Аллабян М. Г.

Тверь, 2023

Рабочая программа учебной дисциплины **Б1.О.04 Информационная безопасность**, компонента основной профессиональной образовательной программы высшего образования — программы бакалавриата по направлению подготовки **09.03.02 Информационные системы и технологии** направленность (профиль) «**Информационные системы в экономике**», направлена на обеспечение у обучающегося способности осуществлять профессиональную деятельность в соответствующей области и сферах профессиональной деятельности, в том числе на их практическую подготовку с учётом рабочей программы воспитания и календарного плана воспитательной работы Частном учреждении высшего образования «**Высшая школа предпринимательства (институт)**» *(далее — **ЧУВО «ВШП»**)*.

1. ОБЛАСТЬ ПРИМЕНЕНИЯ И НОРМАТИВНЫЕ ССЫЛКИ

Настоящая рабочая программа учебной дисциплины устанавливает требования к результатам обучения студента и определяет содержание и виды учебных занятий и отчетности.

Программа предназначена для преподавателей и студентов направления подготовки 09.03.02 Информационные системы и технологии.

Программа учебной дисциплины разработана в соответствии с ФГОС ВО, утвержденного приказом Минобрнауки России от 19.09.2017 № 926 «Об утверждении федерального государственного образовательного стандарта высшего образования - бакалавриата по направлению подготовки 09.03.02 Информационные системы и технологии», основной профессиональной образовательной программой высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии, направленность (профиль) Информационные системы в экономике.

2. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Целью изучения дисциплины «Информационная безопасность» является изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах

Для этого в рамках дисциплины решаются следующие задачи:

- изучение концепции инженерно-технической защиты информации;
- изучение теоретических основ инженерно - технической защиты информации;
- изучение физических основ инженерно-технической защиты информации;
- изучение технических средств добывания и защиты информации;
- изучение организационных основ инженерно-технической защиты информации;
- изучение методического обеспечения инженерно-технической защиты информации.

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина является компонентом обязательной части Блока 1 основной профессиональной образовательной программы высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии, направленность (профиль) — Информационные системы в экономике.

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ В РАМКАХ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс освоения учебной дисциплины направлен на формирование у обучающихся следующих компетенций.

В результате освоения учебной дисциплины обучающийся должен демонстрировать следующие результаты обучения: УК-2, ОПК-1, ОПК-3.

Таблица 1. Результаты обучения

Код компетенции	Наименование компетенции	Индекс и наименование индикатора содержания компетенции	Дескрипторы – основные признаки освоения (показатели достижения результата)
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их	УК-2.1 Способен определять круг задач в рамках поставленной цели	Знать: - Методы и инструменты анализа задач, постановки целей и планирования. Уметь: - Определять задачи, формулировать цели и приоритеты. Владеть:

	решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений		- Навыками постановки задач и планирования.
		УК-2.2 Способен выбирать оптимальные способы решения задач, исходя из правовых норм, ресурсов и ограничений	Знать: - Основы права, ресурсного и ограничительного анализа. Уметь: - Выбирать и обосновывать оптимальные способы решения задач. Владеть: - Навыками принятия решений в условиях ограниченных ресурсов и правовых ограничений.
ОПК-1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности.	ОПК-1.1 Способен применять естественнонаучные и общеинженерные знания в профессиональной деятельности	Знать: - Основные законы и концепции естественных наук, применимые к информационной безопасности. - Принципы работы инженерных систем, связанных с защитой информации. Уметь: - Использовать естественнонаучные знания для анализа уязвимостей в информационных системах. - Применять общеинженерные принципы при разработке и внедрении систем защиты информации. Владеть: - Методами интеграции естественнонаучных знаний для решения задач информационной безопасности. - Навыками междисциплинарного подхода к защите информации.
		ОПК-1.2 Способен применять методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	Знать: - Основы математического анализа и моделирования, используемые в информационной безопасности. - Принципы теоретического и экспериментального исследования для оценки безопасности информационных систем. Уметь: - Применять математические методы для анализа и оценки рисков информационной безопасности. - Создавать и использовать модели для предсказания и предотвращения угроз информационной безопасности. Владеть: - Инструментами математического анализа и моделирования для решения задач информационной безопасности. - Методами проведения теоретических и экспериментальных исследований в области информационной безопасности.
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с	ОПК-3.1 Способен решать стандартные задачи профессиональной деятельности с использованием информационно-коммуни	Знать: - Основные информационно-коммуникационные технологии, применяемые для защиты информации. - Принципы работы с программным и аппаратным обеспечением,

	применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	кационных технологий (далее ИКТ)	используемым в информационной безопасности. Уметь: - Использовать ИКТ для обнаружения и предотвращения угроз информационной безопасности. - Применять специализированное программное обеспечение для анализа безопасности информационных систем. Владеть: - Навыками работы с современными ИКТ в контексте информационной безопасности. - Инструментами и методами ИКТ для решения задач в области защиты информации.
		ОПК-3.2 Способен учитывать основные требования информационной безопасности при решении профессиональных задач	Знать: - Основные требования и стандарты информационной безопасности. - Типовые угрозы и уязвимости информационных систем. Уметь: - Применять методы и средства для обеспечения конфиденциальности, целостности и доступности информации. - Разрабатывать и внедрять меры по защите информации в соответствии с нормативными требованиями. Владеть: - Техниками обеспечения информационной безопасности при решении профессиональных задач. - Средствами мониторинга и анализа для поддержания высокого уровня информационной безопасности.

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Объем дисциплины в зачетных единицах с указанием количества академических часов

Общая трудоемкость учебной дисциплины составляет 4 зачетные единицы, 144 часа, включая все формы контактной и самостоятельной работы обучающихся.

Объем дисциплины по учебному плану составляет –
4 зачётных единицы = 144 академических часа.
Контактная работа обучающегося (студенты) с научно-педагогическим работником организации (всего) - 48 академических часов,
в том числе:
Лекционные занятия (Лек.) - 20 академических часов,
Практические занятия (Пр.) - 26 академических часов,
Консультации (Конс.) - 2 академических часа.
Самостоятельная работа обучающегося (студента):
Самостоятельная работа (СР) - 60 академический час,
Текущий контроль успеваемости
и промежуточно-заочная аттестация обучающегося (студента):
Часы на контроль - 36 академических часов.

Таблица 2. Объём дисциплины

№ п/п	Раздел/тема дисциплины	Семестр/ курс	Виды учебной деятельности, включая самостоятельную работу обучающихся (студентов), и трудоёмкость (в ак. часах)				Коды формируемых компетенций
			Виды учебных занятий по дисциплине			Самостоятельная работа	
			Лек.	Пр.	Конс.	СР	
1	**Тема 1.** Введение в информационную безопасность	1 семестр/ 1 курс	1	2	-	5	УК-2.1, ОПК-3.2
2	**Тема 2.** Принципы и модели информационной безопасности	1 семестр/ 1 курс	2	2	-	5	УК-2.2, ОПК-3.2
3	**Тема 3.** Криптографические методы защиты информации	1 семестр/ 1 курс	2	2	-	5	ОПК-1.1, ОПК-1.2
4	**Тема 4.** Управление доступом и аутентификация	1 семестр/ 1 курс	2	2	-	5	УК-2.2, ОПК-3.1
5	**Тема 5.** Безопасность сетевых технологий	1 семестр/ 1 курс	2	4	-	5	ОПК-3.1, ОПК-3.2
6	**Тема 6.** Защита операционных систем и приложений	1 семестр/ 1 курс	2	2	-	5	ОПК-3.1, ОПК-3.2
7	**Тема 7.** Обеспечение безопасности баз данных	1 семестр/ 1 курс	2	2	-	5	ОПК-3.1, ОПК-3.2
8	**Тема 8** Политики и стандарты информационной безопасности	1 семестр/ 1 курс	2	2	-	5	УК-2.1, ОПК-3.2
9	**Тема 9** Управление инцидентами информационной безопасности	1 семестр/ 1 курс	1	2	-	5	УК-2.1, ОПК-3.2
10	**Тема 10** Социальная инженерия и психологические аспекты информационной безопасности	1 семестр/ 1 курс	2	2	-	5	УК-2.1, ОПК-3.1
11	**Тема 11** Аудит и оценка информационной безопасности	1 семестр/ 1 курс	2	2	-	5	УК-2.2, ОПК-3.2
12	**Тема 12** Итоговое занятие	1 семестр/ 1 курс		2	2	5	УК-2.1, УК-2.2, ОПК-1.1, ОПК-1.2, ОПК-3.1, ОПК-3.2
ИТОГО аудиторных часов/СР:		1 семестр/ 1 курс	**48 ак. часов**			**60 ак. часа**	-
Часы на контроль		1 семестр/ 1 курс	**36 ак. час (форма промежуточной аттестации – экзамен – 1 семестр)**				

ВСЕГО ак. часов:	1 семестр/ 1 курс	**144 академических часа**

5.2. Тематическое содержание дисциплины

* количество академических часов и виды занятий представлены в таблице № 2.

Тема 1: Введение в информационную безопасность

Основные понятия и термины. История развития информационной безопасности. Актуальность и значение информационной безопасности в современном мире. Основные угрозы и уязвимости информационных систем.

Тема 2: Принципы и модели информационной безопасности

Принципы обеспечения информационной безопасности. Основные модели информационной безопасности: модель конфиденциальности (Bell-LaPadula), модель целостности (Biba), модель безопасности на основе мандатного управления доступом (MAC). Модели управления доступом: DAC, MAC, RBAC. Применение моделей на практике.

Тема 3: Криптографические методы защиты информации

Основы криптографии: симметричные и асимметричные алгоритмы шифрования. Принципы работы криптографических систем. Примеры использования криптографии для защиты информации.

Тема 4: Управление доступом и аутентификация

Механизмы управления доступом: внедрение моделей DAC, MAC, RBAC в информационные системы. Методы аутентификации пользователей: пароли, биометрия, токены. Политики управления доступом. Практическое применение методов аутентификации и авторизации.

Тема 5: Безопасность сетевых технологий

Основы сетевой безопасности. Протоколы безопасности: SSL/TLS, IPSec. Методы защиты сетевых соединений: VPN, firewall, IDS/IPS. Угрозы и атаки на сетевую инфраструктуру.

Тема 6: Защита операционных систем и приложений

Методы и средства защиты операционных систем. Антивирусные программы и их работа. Обеспечение безопасности приложений: основные уязвимости и методы их устранения.

Тема 7: Обеспечение безопасности баз данных

Основы защиты баз данных. Методы контроля доступа и целостности данных. Угрозы безопасности баз данных и способы их нейтрализации. Примеры реализации безопасных баз данных.

Тема 8: Политики и стандарты информационной безопасности

Основные стандарты информационной безопасности: ISO/IEC 27001, NIST. Политики безопасности: разработка и внедрение. Роль стандартов и политик в управлении информационной безопасностью.

Тема 9: Управление инцидентами информационной безопасности

Процедуры управления инцидентами. Методы выявления, анализа и реагирования на инциденты. Документирование и отчетность по инцидентам. Примеры реальных инцидентов и их анализ.

Тема 10: Социальная инженерия и психологические аспекты информационной безопасности

Понятие социальной инженерии. Основные методы социальной инженерии и способы их

нейтрализации. Психологические аспекты информационной безопасности. Обучение и повышение осведомленности сотрудников.

Тема 11: Аудит и оценка информационной безопасности
Основы аудита информационной безопасности. Методики оценки защищенности информационных систем. Инструменты и методы проведения аудита. Примеры аудиторских проверок и отчетов.

Тема 12: Итоговое занятие
Повторение и обобщение пройденного материала. Решение типовых задач и вопросов для экзамена. Подготовка к экзамену: ключевые темы и типичные ошибки.

5.2.1 Содержание практических занятий

Таблица 3

№ п/п	Наименование темы (раздела) дисциплины	Содержание практического занятия
1	**Практическое занятие 1: Введение в информационную безопасность**	Задание: Изучение основных понятий и терминов информационной безопасности. Подготовка отчета по основным угрозам и уязвимостям информационных систем. Цель: Ознакомиться с ключевыми понятиями и терминами, развить навыки анализа и классификации угроз информационной безопасности.
2	**Практическое занятие 2: Принципы и модели информационной безопасности**	Задание: Изучение моделей информационной безопасности (Bell-LaPadula, Biba, MAC). Сравнительный анализ моделей на примере реальных кейсов. Цель: Понять основные принципы и модели информационной безопасности, научиться применять их для анализа и разработки систем защиты.
3	**Практическое занятие 3: Криптографические методы защиты информации**	Задание: Работа с криптографическими алгоритмами (AES, RSA). Выполнение шифрования и расшифрования данных с использованием программных инструментов. Цель: Освоить базовые криптографические методы, понять их применение для защиты информации.
4	**Практическое занятие 4: Управление доступом и аутентификация**	Задание: Настройка и применение моделей управления доступом (DAC, MAC, RBAC). Реализация различных методов аутентификации пользователей. Цель: Научиться применять модели управления доступом и аутентификации для обеспечения безопасности информационных систем.
5	**Практическое занятие 5: Безопасность сетевых технологий**	Задание: Настройка и тестирование VPN, firewall, IDS/IPS. Выполнение анализа сетевого трафика для выявления угроз. Цель: Освоить методы защиты сетевых соединений, научиться использовать инструменты для анализа и защиты сетевой инфраструктуры.
6	**Практическое занятие 6: Защита операционных систем и приложений**	Задание: Установка и настройка антивирусных программ. Проведение тестов на уязвимости приложений и операционных систем. Цель: Научиться защищать операционные системы и приложения от угроз, выявлять и устранять уязвимости.
7	**Практическое занятие 7: Обеспечение безопасности баз**	Задание: Настройка механизмов контроля доступа и целостности данных в базах данных. Выполнение тестирования безопасности баз данных. Цель: Понять методы обеспечения безопасности баз данных, научиться применять их на практике.

	данных	
8	**Практическое занятие 8: Политики и стандарты информационной безопасности**	Задание: Разработка и внедрение политики безопасности для организации. Анализ соответствия политики стандартам информационной безопасности (ISO/IEC 27001). Цель: Научиться разрабатывать и внедрять политики безопасности, понимать роль стандартов в управлении информационной безопасностью.
9	**Практическое занятие 9: Управление инцидентами информационной безопасности**	Задание: Разработка плана реагирования на инциденты. Проведение симуляции инцидента и документирование действий. Цель: Освоить методы управления инцидентами, научиться разрабатывать планы реагирования и документировать инциденты.
10	**Практическое занятие 10: Социальная инженерия и психологические аспекты информационной безопасности**	Задание: Проведение анализа уязвимостей, связанных с социальной инженерией. Разработка мероприятий по повышению осведомленности сотрудников. Цель: Понять методы социальной инженерии, научиться разрабатывать меры по их предотвращению и обучению сотрудников.
11	**Практическое занятие 11: Аудит и оценка информационной безопасности**	Задание: Проведение аудита информационной безопасности организации. Подготовка аудиторского отчета с рекомендациями по улучшению безопасности. Цель: Освоить методики проведения аудита, научиться оценивать защищенность информационных систем и готовить рекомендации.
12	**Практическое занятие 12: Итоговое занятие**	Задание: Решение типовых задач и вопросов для подготовки к экзамену. Обсуждение ключевых тем и разбор сложных вопросов. Цель: Повторение и обобщение пройденного материала для успешной сдачи экзамена.

5.2.2 Содержание самостоятельной работы

Таблица 4

№ п/п	Наименование темы (раздела) дисциплины	Содержание самостоятельной работы	Форма контроля
1	**1. Изучение литературы по введению в информационную безопасность**	Задание: Прочитать рекомендованные главы из учебников по основным понятиям и терминам информационной безопасности. Изучить основные угрозы и уязвимости информационных систем.	Подготовить реферат
2	**2. Изучение принципов и моделей информационной безопасности**	Задание: Прочитать главы из учебников и статей по моделям информационной безопасности (Bell-LaPadula, Biba, MAC). Изучить их применение на практике.	Ответы на контрольные вопросы.
3	**3. Изучение криптографических методов защиты информации**	Задание: Изучить учебные материалы по симметричным и асимметричным алгоритмам шифрования (AES, RSA). Выполнить задания по шифрованию и расшифрованию данных.	Ответы на контрольные вопросы, решение практических задач.
4	**4. Изучение**	Задание: Прочитать главы из учебников по моделям	Ответы на

	механизмов управления доступом и аутентификации	управления доступом (DAC, MAC, RBAC) и методам аутентификации (пароли, биометрия, токены). Изучить их внедрение и применение.	контрольные вопросы
5	**5. Изучение безопасности сетевых технологий**	Задание: Изучить учебные материалы по сетевой безопасности и протоколам безопасности (SSL/TLS, IPSec). Настроить и протестировать VPN, firewall, IDS/IPS.	Ответы на контрольные вопросы, доклад.
6	**6. Изучение методов защиты операционных систем и приложений**	Задание: Изучить учебные материалы по методам защиты операционных систем и антивирусным программам. Провести тестирование на уязвимости.	Выполнение практического задания.
7	**7. Изучение методов обеспечения безопасности баз данных**	Задание: Прочитать главы из учебников по защите баз данных. Настроить механизмы контроля доступа и целостности данных.	Ответы на контрольные вопросы.
8	**8. Изучение политик и стандартов информационной безопасности**	Задание: Изучить учебные материалы по основным стандартам информационной безопасности (ISO/IEC 27001, NIST). Разработать политику безопасности для организации.	Ответы на контрольные вопросы, выполнение практического задания.
9	**9. Изучение управления инцидентами информационной безопасности**	Задание: Изучить учебные материалы по процедурам управления инцидентами. Разработать план реагирования на инциденты.	Тест.
10	**10. Изучение социальной инженерии и психологических аспектов информационной безопасности**	Задание: Изучить учебные материалы по методам социальной инженерии. Разработать мероприятия по повышению осведомленности сотрудников.	Ответы на контрольные вопросы.
11	**11. Изучение аудита и оценки информационной безопасности**	Задание: Прочитать главы из учебников по методикам проведения аудита информационной безопасности. Подготовить аудиторский отчет.	Ответы на контрольные вопросы, выполнение практического задания.
12	**12. Подготовка к экзамену**	Задание: Решение типовых задач и контрольных вопросов из учебников и методических пособий для подготовки к экзамену.	Экзамен.

6.Оценочные материалы по дисциплине

Оценочные материалы находятся в документе «Оценочные материалы по дисциплине «Информационная безопасность».

7.Методические материалы для обучающихся по освоению дисциплины (модуля)

А) Рекомендации обучающемуся (студенту) по работе с конспектом после лекции

Какими бы замечательными качествами в области методики ни обладал лектор, какое бы большое значение на занятиях ни уделял лекции слушатель, глубокое понимание материала достигается только путем самостоятельной работы над ним. Самостоятельную работу следует начинать с доработки конспекта, желательно в тот же день, пока время не стерло содержание лекции из памяти (через 10 часов после лекции в памяти остается не более 30-40 % материала). С целью доработки необходимо в первую очередь прочитать записи, восстановить текст в памяти, а также исправить описки, расшифровать не принятые ранее сокращения, заполнить пропущенные места, понять текст, вникнуть в его смысл. Далее прочитать материал по рекомендуемой литературе, разрешая в ходе чтения, возникшие ранее затруднения, вопросы, а также дополнения и исправляя свои записи. Записи должны быть наглядными, для чего следует применять различные способы выделений. В ходе доработки конспекта углубляются, расширяются и закрепляются знания, а также дополняется, исправляется и совершенствуется конспект. Подготовленный конспект и рекомендуемая литература используется при подготовке к практическому занятию. Подготовка сводится к внимательному прочтению учебного материала, к выводу с карандашом в руках всех утверждений и формул, к решению примеров, задач, к ответам на вопросы, предложенные в конце лекции преподавателем или помещенные в рекомендуемой литературе. Примеры, задачи, вопросы по теме являются материалом самоконтроля. Непременным условием глубокого усвоения учебного материала является знание основ, на которых строится изложение материала. Обычно преподаватель напоминает, какой ранее изученный материал и в какой степени требуется подготовить к очередному занятию. Эта рекомендация, как и требование систематической и серьезной работы над всем лекционным курсом, подлежит безусловному выполнению. Потери логической связи как внутри темы, так и между ними приводит к негативным последствиям: материал учебной дисциплины перестает основательно восприниматься, а творческий труд подменяется утомленным переписыванием. Обращение к ранее изученному материалу не только помогает восстановить в памяти известные положения, выводы, но и приводит разрозненные знания в систему, углубляет и расширяет их. Каждый возврат к старому материалу позволяет найти в нем что-то новое, переосмыслить его с иных позиций, определить для него наиболее подходящее место в уже имеющейся системе знаний. Неоднократное обращение к пройденному материалу является наиболее рациональной формой приобретения и закрепления знаний. Очень полезным, но, к сожалению, еще мало используемым в практике самостоятельной работы, является предварительное ознакомление с учебным материалом. Даже краткое, беглое знакомство с материалом очередной лекции дает многое. Обучающиеся (студенты) получают общее представление о её содержании и структуре, о главных и второстепенных вопросах, о терминах и определениях. Все это облегчает работу на лекции и делает ее целеустремленной.

Б) Рекомендации обучающемуся (студенту) по подготовке к занятиям семинарского типа

Обучающийся (студент) должен чётко уяснить, что именно с лекции начинается его подготовка к лабораторному/ практическому/ семинарскому/ методическому/ клиническому практическому занятию. Вместе с тем, лекция лишь организует мыслительную деятельность, но не обеспечивает глубину усвоения программного материала. При подготовке к такому виду занятий можно выделить 2 этапа:

1-й - организационный,

2-й - закрепление и углубление теоретических знаний.

На первом этапе обучающийся (студент) планирует свою самостоятельную работу, которая включает:

- уяснение задания на самостоятельную работу;

- подбор рекомендованной литературы;

- составление плана работы, в котором определяются основные пункты предстоящей подготовки.

Составление плана дисциплинирует и повышает организованность в работе. Второй этап включает непосредственную подготовку обучающегося (студента) к занятию. Начинать надо с

изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы обучающийся (студент) должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Заканчивать подготовку следует составлением плана (перечня основных пунктов) по изучаемому материалу (вопросу). Такой план позволяет составить концентрированное, сжатое представление по изучаемым вопросам. В процессе подготовки к семинарскому занятию рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь. При необходимости следует обращаться за консультацией к преподавателю. Идя на консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения. В начале семинарского занятия обучающиеся (студента) под руководством преподавателя более глубоко осмысливают теоретические положения по теме занятия, раскрывают и объясняют основные явления и факты. В процессе творческого обсуждения и дискуссии вырабатываются умения и навыки использовать приобретенные знания для решения практических задач.

В) Рекомендации по самостоятельной работе обучающегося (студента) над изучаемым материалом

Успешное освоение данного курса базируется на рациональном сочетании нескольких видов учебной деятельности - лекций, семинарских занятий, самостоятельной работы. При этом самостоятельную работу следует рассматривать одним из главных звеньев полноценного высшего образования, на которую отводится значительная часть учебного времени.

Самостоятельная работа студентов складывается из следующих составляющих:

- работа с основной и дополнительной литературой, с материалами интернета и конспектами лекций;
- внеаудиторная подготовка к контрольным работам, выполнение докладов, рефератов и курсовых работ;
- выполнение самостоятельных практических работ;
- подготовка к экзаменам (зачетам) непосредственно перед ними.

Для правильной организации работы необходимо учитывать порядок изучения разделов курса, находящихся в строгой логической последовательности. Поэтому хорошее усвоение одной части дисциплины является предпосылкой для успешного перехода к следующей. Задания, проблемные вопросы, предложенные для изучения дисциплины, в том числе и для самостоятельного выполнения, носят междисциплинарный характер и базируются, прежде всего, на причинно-следственных связях между компонентами окружающего нас мира. В течение семестра, необходимо подготовить рефераты (проекты) с использованием рекомендуемой основной и дополнительной литературы и сдать рефераты для проверки преподавателю. Важным составляющим в изучении данного курса является решение ситуационных задач и работа над проблемно-аналитическими заданиями, что предполагает знание соответствующей научной терминологии и т.д.

Для лучшего запоминания материала целесообразно использовать индивидуальные особенности и разные виды памяти: зрительную, слуховую, ассоциативную. Успешному запоминанию также способствует приведение ярких свидетельств и наглядных примеров. Учебный материал должен постоянно повторяться и закрепляться.

При выполнении докладов, творческих, информационных, исследовательских проектов особое внимание следует обращать на подбор источников информации и методику работы с ними.

Для успешной сдачи экзамена (зачета) рекомендуется соблюдать следующие правила:

1. Подготовка к экзамену (зачету) должна проводиться систематически, в течение

всего семестра.

2. Интенсивная подготовка должна начаться не позднее, чем за месяц до экзамена.

3. Время непосредственно перед экзаменом (зачетом) лучше использовать таким образом, чтобы оставить последний день свободным для повторения курса в целом, для систематизации материала и доработки отдельных вопросов.

На экзамене высокую оценку получают студенты, использующие данные, полученные в процессе выполнения самостоятельных работ, а также использующие собственные выводы на основе изученного материала.

Учитывая значительный объем теоретического материала, студентам рекомендуется регулярное посещение и подробное конспектирование лекций.

8. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники и учебные пособия, иная учебная литература, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

а) для слабовидящих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- задания для выполнения, а также инструкция о порядке проведения промежуточной аттестации оформляются увеличенным шрифтом;
- задания для выполнения на промежуточной аттестации зачитываются ассистентом;
- письменные задания выполняются на бумаге, надиктовываются ассистенту;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- студенту для выполнения задания при необходимости предоставляется увеличивающее устройство;

в) для глухих и слабослышащих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- промежуточно-заочная аттестация проводится в письменной форме;
- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости поступающим предоставляется звукоусиливающая аппаратура индивидуального пользования;
- по желанию студента промежуточно-заочная аттестация может проводиться в письменной форме;

д) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента промежуточно-заочная аттестация проводится в устной форме.

Примечание:

а) Для обучающегося (бакалавра), осваивающего учебную дисциплину, обязательный компонент основной профессиональной образовательной программы высшего образования — программы бакалавриата по направлению подготовки **09.03.02 Информационные системы и технологии** (направленность (профиль) «Информационные системы в экономике»), форма обучения — очно-заочная), одобренной на заседании Учёного совета образовательной

организации, утверждённой ректором Частного образовательного учреждения высшего образования «Высшая школа предпринимательства», **по индивидуальному учебному плану** (*при наличии факта зачисления в образовательную организацию такого обучающегося (бакалавра)*), **Институт:**

- разрабатывает, согласовывает с участниками образовательных отношений и утверждает в установленном порядке согласно соответствующему локальному нормативному акту **индивидуальный учебный план** конкретного обучающегося (бакалавра) (*учебный план, обеспечивающий освоение конкретной основной образовательной программы высшего образования на основе индивидуализации её содержания с учётом особенностей и образовательных потребностей конкретного обучающегося (бакалавра)*);

- устанавливает для конкретного обучающегося (бакалавра) по индивидуальному учебному плану **одинаковые дидактические единицы** — элементы содержания учебного материала, изложенного в виде утверждённой в установленном образовательной организацией порядке согласно соответствующему локальному нормативному акту рабочей программы учебной дисциплины, обязательного компонента разработанной и реализуемой Институтом основной профессиональной образовательной программы высшего образования — программы бакалавриата по направлению подготовки **09.03.02 Информационные системы и технологии** (направленность (профиль) «Информационные системы в экономике»), форма обучения — очно-заочная), как и для обучающего (бакалавра), осваивающего основную образовательную программу высшего образования в учебной группе;

- определяет в индивидуальном учебном плане конкретного обучающегося (бакалавра) **объём учебной дисциплины** с указанием количества академических часов/ ЗЕТ, выделенных на его контактную работу (групповую и (или) индивидуальную работу) с руководящими и (или) научно-педагогическими работниками, реализующими основную образовательную программу высшего образования;

- определяет в индивидуальном учебном плане конкретного обучающегося (бакалавра) количество академических часов/ ЗЕТ по учебной дисциплине, выделенных на его самостоятельную работу (*при необходимости*).

б) Для обучающегося (бакалавра) с ограниченными возможностями здоровья и инвалида, осваивающего учебную дисциплину, обязательный компонент основной профессиональной образовательной программы высшего образования — программы бакалавриата по направлению подготовки **09.03.02 Информационные системы и технологии** (направленность (профиль) «Информационные системы в экономике»), форма обучения — очно-заочная), одобренной на заседании Учёного совета образовательной организации, утверждённой ректором Частного образовательного учреждения высшего образования «Высшая школа предпринимательства», (*при наличии факта зачисления в образовательную организацию такого обучающегося (бакалавра) с учётом конкретной (конкретных) нозологии (нозологий)*), **Институт:**

- разрабатывает, согласовывает с участниками образовательных отношений и утверждает в установленном порядке согласно соответствующему локальному нормативному акту **индивидуальный учебный план** конкретного обучающегося (бакалавра) с ограниченными возможностями здоровья/ инвалида (*при наличии факта зачисления в образовательную организацию такого обучающегося (бакалавра) с учётом конкретной (конкретных) нозологии (нозологий)*) (*учебный план, обеспечивающий освоение конкретной основной образовательной программы высшего образования на основе индивидуализации её содержания с учётом особенностей и образовательных потребностей конкретного обучающегося (бакалавра)*);

- устанавливает для конкретного обучающегося (бакалавра) с ограниченными возможностями здоровья содержание образования (**одинаковые дидактические единицы** — элементы содержания учебного материала, как и для обучающего (бакалавра), осваивающего основную образовательную программу высшего образования в учебной группе) и условия организации обучения, изложенного в виде утверждённой в установленном Институтом порядке согласно соответствующему локальному нормативному акту рабочей программы учебной

дисциплины, обязательного компонента разработанной и реализуемой им адаптированной основной профессиональной образовательной программы высшего образования - программы бакалавриата по направлению подготовки **09.03.02 Информационные системы и технологии** (направленность (профиль) «Информационные системы в экономике»), форма обучения — очно-заочная), а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида (для конкретного обучающегося (бакалавра) с ограниченными возможностями здоровья/ инвалида (*при наличии факта зачисления в образовательную организацию такого обучающегося (бакалавра) с учётом конкретной (конкретных) нозологии (нозологий)*);

- определяет в индивидуальном учебном плане конкретного обучающегося бакалавра) с ограниченными возможностями здоровья/ инвалида (*при наличии факта зачисления такого обучающегося (бакалавра) с учётом конкретной (конкретных) нозологии (нозологий)*) **объём учебной дисциплины** с указанием количества академических часов/ ЗЕТ, выделенных на его контактную работу (групповую и (или) индивидуальную работу) с руководящими и (или) научно-педагогическими работниками, реализующими основную образовательную программу высшего образования;

- определяет в индивидуальном учебном плане конкретного обучающегося (бакалавра) с ограниченными возможностями здоровья/ инвалида (*при наличии факта зачисления в образовательную организацию такого обучающегося (бакалавра) с учётом конкретной (конкретных) нозологии (нозологий)*) количество академических часов/ ЗЕТ по учебной дисциплине, выделенных на его самостоятельную работу (*при необходимости*).

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Мельников В.П., Информационная безопасность [Электронный ресурс] : учебник / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева. - М. : КноРус, 2023. - 371 с. - ISBN 978-5-406-11960-0. - Режим доступа: https://book.ru/book/950148
2. Бабаш А.В., Информационная безопасность. Лабораторный практикум + еПриложение [Электронный ресурс] : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М. : КноРус, 2023. - 131 с. - ISBN 978-5-406-11731-6. - Режим доступа: https://book.ru/book/949452

Дополнительная литература:

1. Николаев Н.С., Управление информационной безопасностью [Электронный ресурс] : учебник / Н.С. Николаев. - М. : КноРус, 2021. - 188 с. - ISBN 978-5-406-07325-4. - Режим доступа: https://book.ru/book/939841

9.2 Используемое программное обеспечение (*комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства в соответствии с п.4.3.2. ФГОС ВО 09.03.02*):

1. Microsoft Windows 11 Pro или аналогичная ОС, включая дистрибутивы Linux, например Debian, Ubuntu, OpenSuse, в том числе отечественного производства, например ОС Astra Linux Common Edition (Разработчик: АО «НПО РусБИТех»), ОС «РОСА» (Разработчик: «НТЦ ИТ РОСА»).
2. Microsoft Office 365 или аналогичный офисный пакет, например OpenOffice, LibreOffice, ONLYOFFICE, в том числе отечественного производства, например МойОфис (Разработчик: ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»).
3. Adobe Reader или аналогичный просмотрщик PDF, например Okular, Foxit Reader, в том числе отечественного производства, например Окуляр ГОСТ (Разработчик: ООО «Лаборатория 50»).

4. Google Chrome или аналогичный веб-браузер, например Microsoft Edge, Mozilla Firefox, в том числе отечественного производства, например Яндекс.Браузер (Разработчик: ООО «ЯНДЕКС»).

9.3 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля) *(в соответствии с п.4.3.4. ФГОС ВО 09.03.02)*

1. Электронно-библиотечная система BOOK.RU [Электронный ресурс]. - Режим доступа: https://book.ru/

9.4 Базы данных, информационно-справочные и поисковые системы *(в соответствии с п.4.3.4. ФГОС ВО 09.03.02)*

1. КонсультантПлюс: справочно-поисковая система [Электронный ресурс]. - http://www.consultant.ru
2. Мировая цифровая библиотека: http://wdl.org/ru
3. Научная электронная библиотека «Scopus»: https://www.scopus.com
4. Научная электронная библиотека ScienceDirect: http://www.sciencedirect.com
5. Научная электронная библиотека «eLIBRARY»: https://elibrary.ru
6. Портал «Гуманитарное образование» http://www.humanities.edu.ru
7. Федеральный портал «Российское образование» http://www.edu.ru
8. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» http://school-collection.edu.ru
9. Поисковые системы Yandex, Rambler и др.
10. Электронная библиотека Российской Государственной Библиотеки (РГБ): http://elibrary.rsl.ru
11. Электронно-библиотечная система http://www.sciteclibrary.ru

10. Материально-техническое обеспечение дисциплины

Помещения для проведения всех видов работы, предусмотренных учебным планом, укомплектованы необходимым оборудованием и техническими средствами обучения.

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно- наглядных пособий и используемого программного обеспечения	**Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)**
Специализированная многофункциональная учебная аудитория для проведения учебных занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, в том числе, для организации практической подготовки обучающийся, с перечнем основного оборудования: - Столы для обучающихся; - Стулья для обучающихся; - Стол педагогического работника; - Стул педагогического работника; - Компьютеры с возможностью	170001, Россия, город Тверь, улица Спартака, дом 26а

подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду лицензиата; - Маркерная или меловая доска; - Проектор.	
Специализированная многофункциональная учебная аудитория для проведения учебных занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, в том числе, для организации практической подготовки обучающийся, с перечнем основного оборудования: - Столы для обучающихся; - Стулья для обучающихся; - Стол педагогического работника; - Стул педагогического работника; - Компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду лицензиата; - Маркерная или меловая доска; - Проектор.	170001, Россия, город Тверь, улица Спартака, дом 26а
Помещение для самостоятельной работы обучающихся с перечнем основного оборудования: - Столы для обучающихся; - Стулья для обучающихся; - Стол педагогического работника; - Стул педагогического работника; - Компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду лицензиата; - Маркерная или меловая доска; - Проектор.	170001, Россия, город Тверь, улица Спартака, дом 26а
Помещение для практических занятий на персональных компьютерах: - Столы для обучающихся; - Стулья для обучающихся; - Стол педагогического работника; - Стул педагогического работника; - Компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду лицензиата;	170001, Россия, город Тверь, улица Спартака, дом 26а

- Ноутбуки с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду лицензиата; - Маркерная или меловая доска; - Проектор.	

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Частное учреждение высшего образования
«Высшая школа предпринимательства (институт)»
(ЧУВО «ВШП»)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
по дисциплине
Б1.О.04 «Информационная безопасность»

Направление подготовки: 09.03.02 Информационные системы и технологии
Направленность (профиль) программы бакалавриата
«Информационные системы в экономике»

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ В РАМКАХ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс освоения учебной дисциплины направлен на формирование у обучающихся следующих компетенций.

В результате освоения учебной дисциплины обучающийся должен демонстрировать следующие результаты обучения: УК-2, ОПК-1, ОПК-3.

Код компетенции	**Наименование компетенции**	**Индекс и наименование индикатора содержания компетенции**	**Дескрипторы – основные признаки освоения (показатели достижения результата)**
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Способен определять круг задач в рамках поставленной цели	Знать: - Методы и инструменты анализа задач, постановки целей и планирования. Уметь: - Определять задачи, формулировать цели и приоритеты. Владеть: - Навыками постановки задач и планирования.
		УК-2.2 Способен выбирать оптимальные способы решения задач, исходя из правовых норм, ресурсов и ограничений	Знать: - Основы права, ресурсного и ограничительного анализа. Уметь: - Выбирать и обосновывать оптимальные способы решения задач. Владеть: - Навыками принятия решений в условиях ограниченных ресурсов и правовых ограничений.
ОПК-1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности.	ОПК-1.1 Способен применять естественнонаучные и общеинженерные знания в профессиональной деятельности	Знать: - Основные законы и концепции естественных наук, применимые к информационной безопасности. - Принципы работы инженерных систем, связанных с защитой информации. Уметь: - Использовать естественнонаучные знания для анализа уязвимостей в информационных системах. - Применять общеинженерные принципы при разработке и внедрении систем защиты информации. Владеть: - Методами интеграции естественнонаучных знаний для решения задач информационной безопасности. - Навыками междисциплинарного подхода к защите информации.
		ОПК-1.2 Способен применять методы математического анализа и моделирования, теоретического и экспериментального исследования в	Знать: - Основы математического анализа и моделирования, используемые в информационной безопасности. - Принципы теоретического и экспериментального исследования для оценки безопасности информационных систем. Уметь:

		профессиональной деятельности	- Применять математические методы для анализа и оценки рисков информационной безопасности. - Создавать и использовать модели для предсказания и предотвращения угроз информационной безопасности. Владеть: - Инструментами математического анализа и моделирования для решения задач информационной безопасности. - Методами проведения теоретических и экспериментальных исследований в области информационной безопасности.
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК-3.1 Способен решать стандартные задачи профессиональной деятельности с использованием информационно-коммуникационных технологий (далее ИКТ)	Знать: - Основные информационно-коммуникационные технологии, применяемые для защиты информации. - Принципы работы с программным и аппаратным обеспечением, используемым в информационной безопасности. Уметь: - Использовать ИКТ для обнаружения и предотвращения угроз информационной безопасности. - Применять специализированное программное обеспечение для анализа безопасности информационных систем. Владеть: - Навыками работы с современными ИКТ в контексте информационной безопасности. - Инструментами и методами ИКТ для решения задач в области защиты информации.
		ОПК-3.2 Способен учитывать основные требования информационной безопасности при решении профессиональных задач	Знать: - Основные требования и стандарты информационной безопасности. - Типовые угрозы и уязвимости информационных систем. Уметь: - Применять методы и средства для обеспечения конфиденциальности, целостности и доступности информации. - Разрабатывать и внедрять меры по защите информации в соответствии с нормативными требованиями. Владеть: - Техниками обеспечения информационной безопасности при решении профессиональных задач. - Средствами мониторинга и анализа для поддержания высокого уровня информационной безопасности.

КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

(признак, на основании которого, проводится оценка по выбранному показателю)

Показатель оценивания компетенций	*Результат обучения*	*Критерии оценивания компетенций*
Высокий уровень (отлично)	**Знать**	Обучающийся продемонстрировал: глубокие исчерпывающие знания и понимание учебного материала; содержательные, полные, правильные и конкретные ответы на все вопросы, включая дополнительные; свободное владение основной и дополнительной литературой, рекомендованной учебной программой дисциплины.
	Уметь	Обучающийся продемонстрировал: понимание учебного материала; умение свободно решать практические задания (ситуационные задачи), которые следует выполнить или описание результата, который нужно получить и др.; логически последовательные, содержательные, полные, правильные и конкретные ответы (решения) на все поставленные задания (вопросы), включая дополнительные; свободное владение основной и дополнительной литературой, рекомендованной учебной программой дисциплины.
	Владеть	Обучающийся продемонстрировал: понимание учебного материала; умение свободно решать комплексные практические задания (решения задач по нестандартным ситуациям); логически последовательные, полные, правильные и конкретные ответы в ходе защиты задания, включая дополнительные уточняющие вопросы (задания); свободное владение основной и дополнительной литературой, рекомендованной учебной программой дисциплины.
Средний уровень (хорошо)	**Знать**	Обучающийся продемонстрировал: твердые и достаточно полные знания учебного материала; правильное понимание сущности и взаимосвязи рассматриваемых процессов и явлений; последовательные, правильные, конкретные ответы на поставленные вопросы при свободном устранении замечаний по отдельным вопросам; достаточное владение литературой, рекомендованной учебной программой дисциплины
	Уметь	Обучающийся продемонстрировал: понимание учебного материала; логически последовательные, правильные и конкретные ответы (решения) на основные задания (вопросы), включая дополнительные; устранение замечаний по отдельным элементам задания (вопроса); владение основной и дополнительной литературой, рекомендованной учебной программой дисциплины
	Владеть	Обучающийся продемонстрировал: понимание учебного материала; продемонстрировал логически последовательные, достаточно полные, правильные ответы, включая дополнительные; самостоятельно устранил замечания по отдельным элементам задания (вопроса); владение основной и дополнительной литературой, рекомендованной учебной программой дисциплины
Достаточный уровень (удовлетворительно)	**Знать**	Обучающийся продемонстрировал: твердые знания и понимание основного учебного материала; правильные, без грубых ошибок, ответы на поставленные вопросы при устранении неточностей и несущественных ошибок в освещении отдельных положений при наводящих вопросах преподавателя; недостаточно полное владение литературой, рекомендованной учебной программой дисциплины
	Уметь	Обучающийся продемонстрировал: понимание основного учебного материала; правильные, без грубых ошибок, ответы (решения) на основные задания (вопросы), включая дополнительные, устранение, при наводящих вопросах преподавателя, замечаний по отдельным элементам задания

		(вопроса); недостаточное полное владение литературой, рекомендованной учебной программой дисциплины
	Владеть	Обучающийся понимание основного учебного материала; без грубых ошибок дал ответы на поставленные вопросы при устранении неточностей и ошибок в решениях в ходе защиты задания (проекта, портфолио) при наводящих вопросах преподавателя; недостаточно полное владение литературой, рекомендованной учебной программой дисциплины

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

При проведении промежуточной аттестации в **ЧУВО «ВШП»** используются традиционные формы аттестации:

Форма промежуточной аттестации	**Шкала оценивания**
ЗАЧЕТ	«зачтено», «незачтено»
ЭКЗАМЕН	«отлично», «хорошо», «удовлетворительно», «неудовлетворительно»

КРИТЕРИИ И ПРОЦЕДУРЫ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ

Для оценивания результатов обучения в виде **ЗНАНИЙ** используются следующие процедуры и технологии:

- тестирование.

Для оценивания результатов обучения в виде **УМЕНИЙ и ВЛАДЕНИЙ** используются следующие процедуры и технологии:

- устный или письменный ответ на вопрос.
- практические задания, включающие одну или несколько задач (вопросов) в виде краткой формулировки действий (комплекса действий), которые следует выполнить, или описать результат, который нужно получить.

Критерии оценивания результата обучения по дисциплине (модулю)

Результат обучения по дисциплине (модулю)	ШКАЛА ОЦЕНИВАНИЯ				**Процедуры оценивания**
	«отлично»	«хорошо»	«удовлетворительно»	«неудовлетворительно»	
УК-2, ОПК-1, ОПК-3 **Знать:**	Обучаемый продемонстрировал: глубокие исчерпывающие знания и понимание учебного материала; содержательные, полные, правильные и конкретные ответы на все вопросы, включая дополнительные; свободное владение основной и дополнительной литературой, рекомендованной учебной	Обучаемый продемонстрировал: твердые и достаточно полные знания учебного материала; правильное понимание сущности и взаимосвязи рассматриваемых процессов и явлений; последовательные, правильные, конкретные ответы на поставленные вопросы при свободном устранении	Обучаемый продемонстрировал: твердые знания и понимание основного учебного материала; правильные, без грубых ошибок, ответы на поставленные вопросы при устранении неточностей и несущественных ошибок в освещении отдельных положений при наводящих вопросах преподавателя; недостаточно полное владение	Обучаемый продемонстрировал неправильные ответы на основные вопросы; грубые ошибки в ответах; непонимание сущности излагаемых вопросов; неуверенные и неточные ответы на дополнительные вопросы; не владеет основной литературой, рекомендованной учебной программой дисциплины.	Тестовые задания

	программой дисциплины.	замечаний по отдельным вопросам; достаточное владение литературой.	литературой, рекомендованной учебной программой дисциплины.		
УК-2, ОПК-1, ОПК-3 **Уметь:**	Обучаемый продемонстрировал: понимание учебного материала, содержательные, полные, правильные и конкретные ответы на все поставленные вопросы, включая дополнительные; свободное владение основной и дополнительной литературой, рекомендованной учебной программой дисциплины	Обучаемый продемонстрировал: понимание учебного материала; логически последовательные, правильные и конкретные ответы на основные задания/вопросы, включая дополнительные; устранение замечаний по отдельным элементам задания; владение основной и дополнительной литературой, рекомендованной учебной программой дисциплины	Обучаемый продемонстрировал: понимание основного учебного материала; правильные, без грубых ошибок, ответы на основные вопросы, включая дополнительные, устранение, при наводящих вопросах преподавателя, замечаний по отдельным элементам задания; недостаточное полное владение литературой, рекомендованной учебной программой дисциплины	Обучаемый продемонстрировал: непонимание основного учебного материала; не дал правильные ответы на основные вопросы, включая дополнительные; не устранил, при наводящих вопросах преподавателя, замечания и грубые ошибки по вопросу; не владеет основной учебной литературой, рекомендованной учебной программой дисциплины	Вопросы Практические задания
УК-2, ОПК-1, ОПК-3 **Владеть:**	Обучаемый продемонстрировал: понимание учебного материала; правильные и конкретные ответы, включая дополнительны е уточняющие вопросы; свободное владение основной и дополнительной литературой, рекомендованной учебной программой дисциплины	Обучаемый продемонстрировал: понимание учебного материала; продемонстрировал логически последовательные, достаточно полные, верные ответы; самостоятельно устранил замечания по отдельным элементам; владение основной и дополнительной литературой, рекомендованной учебной программой дисциплины	Обучаемый продемонстрировал: понимание основного учебного материала; без грубых ошибок дал ответы на поставленные вопросы, в том числе при наводящих вопросах преподавателя; недостаточно полное владение литературой, рекомендованной учебной программой дисциплины	Обучаемый продемонстрировал: непонимание основного учебного материала; дал неправильные ответы на поставленные вопросы; не владеет основной учебной литературой, рекомендованной учебной программой дисциплины	Вопросы Практические задания

1. Оценочные материалы для самостоятельной работы обучающихся (студентов)

1.1 Реферат

Реферат позволит студентам углубиться в понимание принципов и методов обеспечения информационной безопасности, а также их значимость и применение в современных информационных системах. Реферат покрывает компетенции УК-2.1, УК-2.2, ОПК-1.1, ОПК-1.2, ОПК-3.1, ОПК-3.2.

Примерная тематика рефератов:

1. **История и эволюция информационной безопасности**
   - Исследуйте ключевые этапы развития информационной безопасности от первых методов защиты информации до современных технологий и стандартов.
2. **Модели и принципы информационной безопасности**
   - Проанализируйте основные модели информационной безопасности (Bell-LaPadula, Biba, MAC) и их применение в современных системах.
3. **Криптографические методы защиты информации**
   - Рассмотрите различные криптографические методы, их архитектуру и применение для защиты данных.
4. **Управление доступом и аутентификация в информационных системах**
   - Изучите модели управления доступом (DAC, MAC, RBAC) и методы аутентификации (пароли, биометрия, токены).
5. **Сетевая безопасность: протоколы и методы защиты**
   - Проанализируйте основные протоколы и методы защиты сетевых соединений, такие как SSL/TLS, IPSec, VPN, firewall, IDS/IPS.
6. **Защита операционных систем и приложений**
   - Обсудите методы и средства защиты операционных систем и приложений, включая антивирусные программы и тестирование на уязвимости.
7. **Безопасность баз данных**
   - Исследуйте методы обеспечения безопасности баз данных, включая механизмы контроля доступа и целостности данных.
8. **Политики и стандарты информационной безопасности**
   - Рассмотрите основные стандарты информационной безопасности (ISO/IEC 27001, NIST) и разработку политик безопасности.
9. **Управление инцидентами информационной безопасности**
   - Проанализируйте процедуры управления инцидентами, методы выявления, анализа и реагирования на инциденты.
10. **Социальная инженерия и методы защиты от нее**
    - Исследуйте методы социальной инженерии и способы их нейтрализации, а также психологические аспекты информационной безопасности.
11. **Аудит и оценка информационной безопасности**
    - Рассмотрите методы проведения аудита информационной безопасности и оценку защищенности информационных систем.
12. **Будущее информационной безопасности: новые тенденции и технологии**
    - Исследуйте современные тренды и перспективы развития информационной безопасности, включая квантовые вычисления и нейросетевые технологии.

Цель написания рефератов: Углубить понимание и критическое осмысление роли информационной безопасности в информационных системах, развивая аналитические и научные навыки студентов.

Структура реферата:

- **Введение:**
  - Краткое описание темы и целей реферата.
  - Актуальность темы.
- **Основная часть:**
  - Теоретические основы темы.
  - История и эволюция (если применимо).
  - Применение в современной экономике/бизнесе.
  - Примеры и кейсы.
  - Проблемы и вызовы.
  - Перспективы и тенденции развития.
- **Заключение:**
  - Выводы по результатам исследования.
  - Значение информационной безопасности для современных информационных систем.
- **Список использованных источников:**
  - Перечень использованной литературы и интернет-ресурсов.

Критерии оценивания:

- **Структура и логика изложения (20%):**
  - Четкая структура работы (введение, основная часть, заключение).
  - Логичность и последовательность изложения материала.
- **Содержание (40%):**
  - Полнота раскрытия темы.
  - Описание основных этапов развития операционных систем.
  - Анализ современных тенденций.
  - Примеры применения операционных систем в информационных системах.
- **Аналитическая часть (20%):**
  - Глубина анализа роли операционных систем в информационных системах.
  - Наличие собственных выводов и оценок.
- **Оформление (10%):**
  - Соответствие требованиям к оформлению рефератов (шрифт, отступы, заголовки и т.д.).
  - Корректное оформление ссылок и списка литературы.
- **Язык и стиль (10%):**
  - Грамотность и точность изложения.
  - Научный стиль текста.

Требования к объему:

Объем реферата должен составлять 10-15 страниц печатного текста (шрифт Times New Roman, размер 12, интервал 1.5, поля 2 см со всех сторон).

2. Оценочные материалы для оценки текущей аттестации обучающихся (студентов)

2.1 Тестовые задания для текущего контроля успеваемости в виде ЗНАНИЙ

В тестовом задании вопросы, которые имеют закрытый характер.
Правильные ответы выделены знаком +.

1. Какова основная цель информационной безопасности? (УК-2.2)
    - Защита данных от несанкционированного доступа и изменения +
    - Оптимизация вычислительных процессов
    - Ускорение работы программного обеспечения
    - Обеспечение удобства использования информационных систем
2. Какие задачи решает информационная безопасность? (ОПК-3.2)
    - Обеспечение конфиденциальности, целостности и доступности данных +
    - Оптимизация вычислительных процессов
    - Увеличение объема хранимых данных
    - Повышение скорости передачи данных
3. Какой компонент информационной безопасности отвечает за защиту информации от несанкционированного доступа? (ОПК-3.2)
    - Управление доступом +
    - Шифрование
    - Аудит
    - Мониторинг
4. Какой из следующих алгоритмов используется для симметричного шифрования? (ОПК-1.1)
    - AES +
    - RSA
    - ECC
    - SHA-256
5. Какой из следующих алгоритмов используется для асимметричного шифрования? (ОПК-1.1)
    - RSA +
    - AES
    - DES
    - MD5
6. Какие основные методы аутентификации используются в информационных системах? (УК-2.1)
    - Пароли, биометрия, токены +
    - Логины, IP-адреса, MAC-адреса
    - Электронная почта, телефонные номера, домашние адреса
    - Социальные сети, мессенджеры, форумы
7. Что означает аббревиатура RBAC в контексте управления доступом? (УК-2.2)
    - Role-Based Access Control +
    - Risk-Based Access Control
    - Resource-Based Access Control
    - Rule-Based Access Control
8. Какие протоколы используются для обеспечения безопасности сетевых соединений? (ОПК-3.1)
    - SSL/TLS, IPSec +
    - HTTP, FTP
    - SMTP, POP3
    - DHCP, DNS

9. Какие антивирусные методы наиболее эффективны для защиты операционных систем? (ОПК-1.2)
    - Сигнатурный анализ и эвристический анализ +
    - Блокировка портов и IP-адресов
    - Виртуализация и контейнеризация
    - Использование старых версий ПО
10. Что включает в себя процедура управления инцидентами информационной безопасности? (УК-2.1)
    - Выявление, анализ и реагирование на инциденты +
    - Обновление ПО и оборудования
    - Обучение персонала
    - Разработка новых приложений
11. Какие методы социальной инженерии используются злоумышленниками? (УК-2.2)
    - Фишинг, вишинг, предтекстинг +
    - Шифрование, хэширование, аутентификация
    - Анализ логов, мониторинг трафика, контроль доступа
    - Разработка приложений, тестирование ПО, оптимизация систем
12. Какие методы можно использовать для защиты от социальной инженерии? (ОПК-3.2)
    - Обучение сотрудников и повышение осведомленности +
    - Установка антивирусного ПО
    - Использование симметричного шифрования
    - Оптимизация сетевых маршрутов
13. Что включает в себя аудит информационной безопасности? (ОПК-1.2)
    - Оценка защищенности систем и выявление уязвимостей +
    - Обновление программного обеспечения
    - Разработка новых приложений
    - Настройка сетевых маршрутов
14. Какой из следующих методов относится к математическому анализу в информационной безопасности? (ОПК-1.1)
    - Анализ рисков и угроз +
    - Установка антивирусного ПО
    - Настройка VPN
    - Обновление операционной системы
15. Какие компоненты включаются в управление доступом к информационным системам? (УК-2.1)
    - Политики доступа и права пользователей +
    - Виртуализация и контейнеризация
    - Оптимизация сетевых маршрутов
    - Репликация и шардирование

Критерии оценки результатов теста

1. **"Неудовлетворительно" (0-39%)**
    - Студент ответил правильно на менее 40% вопросов.
    - Значительные пробелы в знаниях по большинству тем.
    - Неправильное понимание ключевых понятий и принципов.
    - Неспособность применить теоретические знания на практике.
2. **"Удовлетворительно" (40-59%)**
    - Студент ответил правильно на 40-59% вопросов.
    - Основные понятия и принципы поняты частично, есть ошибки в ответах.
    - Знания по большинству тем на базовом уровне, недостаточная глубина понимания.

- Частичная способность применять теоретические знания на практике, нужны дополнительные разъяснения.

3. **"Хорошо" (60-79%)**
   - Студент ответил правильно на 60-79% вопросов.
   - Хорошее понимание ключевых понятий и принципов, незначительные ошибки.
   - Знания по всем темам на достаточном уровне, однако есть некоторые пробелы.
   - Способность применять теоретические знания на практике, но требуется улучшение точности и уверенности.
4. **"Отлично" (80-100%)**
   - Студент ответил правильно на 80-100% вопросов.
   - Полное и правильное понимание всех ключевых понятий и принципов.
   - Глубокие знания по всем темам, минимальные или отсутствующие ошибки.
   - Высокий уровень способности применять теоретические знания на практике, демонстрация уверенности и точности в ответах.

2.2 Вопросы для текущего контроля успеваемости в виде УМЕНИЙ

1. Что такое информационная безопасность и какие задачи она решает? (УК-2.1)
   - Правильный ответ: Информационная безопасность — это защита информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий, обеспечивающая конфиденциальность, целостность и доступность данных.
2. Какие задачи решает управление доступом в контексте информационной безопасности? (ОПК-3.2)
   - Правильный ответ: Управление доступом защищает информацию от несанкционированного доступа, обеспечивая, что доступ к данным имеют только уполномоченные лица.
3. Что такое криптография и какие основные типы шифрования существуют? (ОПК-1.1)
   - Правильный ответ: Криптография — это метод защиты информации посредством шифрования. Основные типы шифрования — симметричное (один ключ для шифрования и расшифрования) и асимметричное (два ключа: один для шифрования, другой для расшифрования).
4. Какой алгоритм используется для симметричного шифрования и в чем его суть? (ОПК-1.1)
   - Правильный ответ: Алгоритм AES используется для симметричного шифрования, где один ключ используется как для шифрования, так и для расшифрования данных.
5. Какой алгоритм используется для асимметричного шифрования и в чем его суть? (ОПК-1.1)
   - Правильный ответ: Алгоритм RSA используется для асимметричного шифрования, где один ключ используется для шифрования, а другой для расшифрования данных.
6. Какие методы аутентификации применяются в информационных системах? (УК-2.1)
   - Правильный ответ: Основные методы аутентификации включают пароли, биометрические данные и токены.
7. Что означает аббревиатура RBAC и как она применяется в управлении доступом? (УК-2.2)
   - Правильный ответ: RBAC (Role-Based Access Control) — это управление доступом на основе ролей, где права доступа назначаются пользователям в зависимости от их роли в организации.
8. Какое устройство выполняет контроль и фильтрацию сетевого трафика? (ОПК-3.1)

    - Правильный ответ: Firewall (межсетевой экран) выполняет контроль и фильтрацию входящего и исходящего сетевого трафика.
9. Какие методы антивирусной защиты наиболее эффективны? (ОПК-1.2)
    - Правильный ответ: Наиболее эффективны сигнатурный анализ и эвристический анализ.
10. Какие этапы включает процедура управления инцидентами информационной безопасности? (УК-2.1)
    - Правильный ответ: Процедура управления инцидентами включает выявление, анализ и реагирование на инциденты.
11. Какие техники социальной инженерии применяют злоумышленники для получения доступа к конфиденциальной информации? (УК-2.2)
    - Правильный ответ: Злоумышленники применяют техники социальной инженерии, такие как фишинг (поддельные электронные письма или сайты для кражи данных), вишинг (телефонные звонки с целью получения личной информации) и претекстинг (создание ложных сценариев для получения информации от пользователей).
12. Как можно защититься от методов социальной инженерии? (ОПК-3.2)
    - Правильный ответ: Для защиты от социальной инженерии необходимо обучать сотрудников и повышать их осведомленность о возможных угрозах.
13. Что включает в себя аудит информационной безопасности? (ОПК-1.2)
    - Правильный ответ: Аудит информационной безопасности включает оценку защищенности систем и выявление уязвимостей.
14. Какие методы относятся к математическому анализу в информационной безопасности? (ОПК-1.1)
    - Правильный ответ: Методы анализа рисков и угроз.
15. Какие компоненты включаются в управление доступом к информационным системам? (УК-2.1)
    - Правильный ответ: Управление доступом включает политики доступа и права пользователей, определяющие, кто и к каким данным имеет доступ.

Критерии оценки ответов на вопросы

- **"Отлично"**
    - **Критерии**:
        - Полное и точное объяснение вопроса.
        - Ответ включает все ключевые аспекты и детали.
        - Примеры, если требуются, приведены и правильно объяснены.
        - Ответ демонстрирует глубокое понимание темы.
- **"Хорошо"**
    - **Критерии**:
        - Корректное объяснение вопроса.
        - Ответ охватывает основные аспекты, но может отсутствовать незначительная деталь или пример.
        - Демонстрируется хорошее, но не полное понимание темы.
- **"Удовлетворительно"**
    - **Критерии**:
        - Общее представление о вопросе.
        - Ответ включает основные аспекты, но содержит неточности или пропуски.
        - Примеры, если требуются, могут отсутствовать или быть неверно объяснены.
        - Демонстрируется базовое понимание темы.
- **"Неудовлетворительно"**
    - **Критерии**:

- Некорректное или неполное объяснение вопроса.
- Отсутствие ключевых аспектов и деталей.
- Примеры, если требуются, отсутствуют или приведены неверные.
- Ответ демонстрирует недостаточное понимание темы.

2.3 Задачи на соответствие понятий для текущего контроля успеваемости в виде ВЛАДЕНИЙ

Правильные ответы расположены в таблицах друг напротив друга, во время тестирования предполагается что порядок данных в рамках каждого столбца будет случайным.

Задача 1: Соотнесите основные модели информационной безопасности с их определениями (УК-2.1, ОПК-3.2)

Чтобы определить правильное соответствие, необходимо понимать основные модели информационной безопасности и их предназначение.

Модель	Определение
A - Модель Белл-ЛаПадула	1 - Обеспечивает контроль доступа на основе уровней секретности и доменов безопасности
B - Модель Biba	2 - Направлена на обеспечение целостности данных и предотвращение их несанкционированного изменения
C - Модель DAC	3 - Управление доступом на основе дискреционных прав владельца ресурса
D - Модель RBAC	4 - Управление доступом на основе ролей пользователей

Правильный ответ: A-1, B-2, C-3, D-4

Задача 2: Соотнесите методы шифрования с их характеристиками (ОПК-1.1, УК-2.2)

Чтобы определить правильное соответствие, необходимо понимать основные методы шифрования и их особенности.

Метод	Характеристика
A - Симметричное	1 - Один ключ используется для шифрования и расшифрования
B - Асимметричное	2 - Два ключа: один для шифрования, другой для расшифрования
C - Хэширование	3 - Односторонний процесс, преобразующий данные в уникальный фиксированный отпечаток
D - Стеганография	4 - Скрытие информации внутри других данных, например, изображений или аудиофайлов

Правильный ответ: A-1, B-2, C-3, D-4

Задача 3: Соотнесите виды атак с их описаниями (ОПК-3.2, УК-2.1)

Чтобы определить правильное соответствие, необходимо понимать основные виды атак и их методы.

Вид атаки	Описание
A - Фишинг	1 - Поддельные электронные письма или сайты для кражи личных данных
B - DDoS	2 - Перегрузка сервера множеством запросов для нарушения его работы
C - Вишинг	3 - Телефонные звонки с целью получения конфиденциальной информации
D - SQL-инъекция	4 - Вставка вредоносного кода в запросы к базе данных

Правильный ответ: A-1, B-2, C-3, D-4

Задача 4: Соотнесите основные протоколы сетевой безопасности с их функциями (ОПК-3.1, УК-2.2)

Чтобы определить правильное соответствие, необходимо понимать функции различных протоколов сетевой безопасности.

Протокол	Функция
A - SSL/TLS	1 - Обеспечивает защиту данных при их передаче в Интернете
B - IPSec	2 - Обеспечивает безопасность на уровне IP-данных, создавая защищенные туннели
C - SSH	3 - Обеспечивает защищенный удаленный доступ и управление серверами
D - HTTPS	4 - Обеспечивает безопасное соединение для веб-сайтов, шифруя HTTP-трафик

Правильный ответ: A-1, B-2, C-3, D-4

Задача 5: Соотнесите основные методы аутентификации с их примерами (УК-2.1, ОПК-3.2)

Чтобы определить правильное соответствие, необходимо понимать различные методы аутентификации и их примеры.

Метод	Пример
A - Парольная	1 - Ввод секретного слова для доступа к учетной записи
B - Биометрическая	2 - Сканирование отпечатков пальцев для подтверждения личности
C - Токены	3 - Использование физического устройства или приложения для генерации одноразовых кодов
D - Многофакторная	4 - Комбинация нескольких методов, например, пароля и отпечатка пальца

Правильный ответ: A-1, B-2, C-3, D-4

Задача 6: Соотнесите элементы информационной безопасности с их целями (УК-2.2, ОПК-1.2)
Чтобы определить правильное соответствие, необходимо понимать цели различных элементов информационной безопасности.

Элемент	Цель
A - Конфиденциальность	1 - Защита информации от несанкционированного доступа
B - Целостность	2 - Защита информации от несанкционированного изменения или уничтожения
C - Доступность	3 - Обеспечение доступности информации для авторизованных пользователей
D - Аутентичность	4 - Проверка подлинности пользователя или информации

Правильный ответ: A-1, B-2, C-3, D-4

Критерии оценки выполнения задач на соответствие понятий

- **Правильность соответствий:**
  - **Отлично (5)**: Все соответствия выполнены правильно.
  - **Хорошо (4)**: 1 ошибка в соответствиях.
  - **Удовлетворительно (3)**: 2 ошибки в соответствиях.
  - **Неудовлетворительно (2)**: 3 и более ошибок в соответствиях.

3. Оценочные материалы для проведения промежуточной аттестации обучающихся (студентов)

3.1 Вопросы для проведения промежуточной аттестации в форме ЭКЗАМЕНА

1. Вопрос: В чем заключается цель информационной безопасности и какие основные задачи она решает? (УК-2.1)
   - Ответ: Цель информационной безопасности заключается в защите информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий, обеспечивая конфиденциальность, целостность и доступность данных. Основные задачи включают защиту данных от несанкционированного доступа, предотвращение утечек информации, обеспечение доступности данных для авторизованных пользователей и защиту от кибератак.
2. Вопрос: Опишите основные модели информационной безопасности и их предназначение. (ОПК-3.2)
   - Ответ: Основные модели информационной безопасности включают модель Белл-ЛаПадула (обеспечивает конфиденциальность), модель Biba (обеспечивает целостность данных), модель DAC (управление доступом на основе дискреционных прав) и модель RBAC (управление доступом на основе ролей пользователей).
3. Вопрос: Объясните различия между симметричным и асимметричным шифрованием. (ОПК-1.1)
   - Ответ: Симметричное шифрование использует один ключ для шифрования и расшифрования данных (например, AES). Асимметричное шифрование использует два ключа: один для шифрования (публичный ключ) и другой для расшифрования (приватный ключ), например, RSA.

4. Вопрос: Какие алгоритмы используются для симметричного и асимметричного шифрования? Приведите примеры. (ОПК-1.1)
    - Ответ: Для симметричного шифрования используются алгоритмы, такие как AES. Для асимметричного шифрования используются алгоритмы, такие как RSA.
5. Вопрос: Как работает метод хэширования и в чем его отличие от шифрования? (ОПК-1.1)
    - Ответ: Хэширование — это односторонний процесс, который преобразует данные в уникальный фиксированный отпечаток (хэш). В отличие от шифрования, хэширование не предназначено для обратимого преобразования данных, а используется для проверки целостности данных.
6. Вопрос: Опишите основные методы аутентификации пользователей в информационных системах. (УК-2.1)
    - Ответ: Основные методы аутентификации включают пароли, биометрические данные (например, отпечатки пальцев, сканирование сетчатки) и токены (физические устройства или приложения для генерации одноразовых кодов).
7. Вопрос: Что такое многофакторная аутентификация и каковы ее преимущества? (УК-2.1)
    - Ответ: Многофакторная аутентификация использует комбинацию нескольких методов аутентификации, таких как пароли и биометрические данные, для повышения безопасности. Преимущества включают более высокий уровень защиты, так как для доступа требуется несколько независимых доказательств подлинности.
8. Вопрос: Объясните, что такое управление доступом на основе ролей (RBAC) и какие преимущества оно предоставляет. (УК-2.2)
    - Ответ: Управление доступом на основе ролей (RBAC) назначает права доступа пользователям в зависимости от их роли в организации. Преимущества включают упрощенное управление доступом, улучшенную безопасность и соответствие требованиям безопасности.
9. Вопрос: Какие протоколы используются для защиты сетевых соединений и как они работают? (ОПК-3.1)
    - Ответ: Протоколы SSL/TLS и IPSec используются для защиты сетевых соединений. SSL/TLS обеспечивает шифрование данных при передаче в Интернете, а IPSec создает защищенные туннели для передачи IP-данных, обеспечивая их целостность и конфиденциальность.
10. Вопрос: Какую роль выполняет межсетевой экран (Firewall) в обеспечении сетевой безопасности? (ОПК-3.1)
    - Ответ: Межсетевой экран (Firewall) контролирует и фильтрует входящий и исходящий сетевой трафик на основе заданных правил безопасности, защищая сеть от несанкционированного доступа и кибератак.
11. Вопрос: Что включает в себя обеспечение безопасности баз данных и какие методы используются? (ОПК-1.2)
    - Ответ: Обеспечение безопасности баз данных включает контроль доступа, шифрование данных и регулярное резервное копирование. Методы включают использование ролей и привилегий для контроля доступа, а также мониторинг активности базы данных для выявления аномалий.
12. Вопрос: Опишите процесс управления инцидентами информационной безопасности и его основные этапы. (УК-2.1)
    - Ответ: Процесс управления инцидентами информационной безопасности включает выявление, анализ, реагирование на инциденты и восстановление. Основные этапы включают обнаружение инцидента, оценку его воздействия, устранение угрозы, восстановление нормальной работы и анализ для предотвращения повторных инцидентов.
13. Вопрос: Какие методы социальной инженерии используются злоумышленниками для получения доступа к конфиденциальной информации? (УК-2.2)

- Ответ: Злоумышленники используют методы социальной инженерии, такие как фишинг (поддельные электронные письма или сайты для кражи данных), вишинг (телефонные звонки с целью получения личной информации) и претекстинг (создание ложных сценариев для получения информации от пользователей).

14. Вопрос: Как можно защититься от методов социальной инженерии? (ОПК-3.2)
    - Ответ: Для защиты от социальной инженерии необходимо обучать сотрудников и повышать их осведомленность о возможных угрозах, проводить регулярные тренировки по безопасности и использовать технические меры, такие как фильтрация электронной почты и мониторинг сетевой активности.
15. Вопрос: Что включает в себя аудит информационной безопасности и какие этапы он включает? (ОПК-1.2)
    - Ответ: Аудит информационной безопасности включает оценку защищенности систем, выявление уязвимостей и разработку рекомендаций по их устранению. Этапы включают планирование аудита, сбор данных, анализ, отчетность и мониторинг выполнения рекомендаций.
16. Вопрос: Какие протоколы и методы используются для создания защищенных виртуальных частных сетей (VPN)? (ОПК-3.1)
    - Ответ: Протоколы IPSec и SSL/TLS используются для создания защищенных виртуальных частных сетей (VPN). Эти протоколы обеспечивают шифрование данных, передаваемых через интернет, и создают защищенные туннели для безопасного обмена информацией.

Критерии оценки ответов на экзамене

- **"Отлично" (5 баллов)**
  - **Критерии**:
    - Полное и точное объяснение вопроса.
    - Ответ включает все ключевые аспекты и детали.
    - Примеры, если требуются, приведены и правильно объяснены.
    - Ответ демонстрирует глубокое понимание темы.
- **"Хорошо" (4 балла)**
  - **Критерии**:
    - Корректное объяснение вопроса.
    - Ответ охватывает основные аспекты, но может отсутствовать незначительная деталь или пример.
    - Демонстрируется хорошее, но не полное понимание темы.
- **"Удовлетворительно" (3 балла)**
  - **Критерии**:
    - Общее представление о вопросе.
    - Ответ включает основные аспекты, но содержит неточности или пропуски.
    - Примеры, если требуются, могут отсутствовать или быть неверно объяснены.
    - Демонстрируется базовое понимание темы.
- **"Неудовлетворительно" (2 балла)**
  - **Критерии**:
    - Некорректное или неполное объяснение вопроса.
    - Отсутствие ключевых аспектов и деталей.
    - Примеры, если требуются, отсутствуют или приведены неверные.
    - Ответ демонстрирует недостаточное понимание темы.