МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
имени И.Т. ТРУБИЛИНА»

Факультет прикладной информатики
Компьютерных технологий и систем

УТВЕРЖДЕНО
Декан
Замотайлова Д.А.
протокол от 25.04.2025 № 7

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Уровень высшего образования: бакалавриат

Направление подготовки: 09.03.03 Прикладная информатика

Направленность (профиль)подготовки: Менеджмент ИТ-проектов, управление жизненным циклом информационных систем

Квалификация (степень) выпускника: бакалавр

Формы обучения: очная, заочная

Год набора (приема на обучение): 2025

Срок получения образования: Очная форма обучения – 4 года
Заочная форма обучения – 4 года 8 месяца(-ев)

Объем: в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

2025

Разработчики:
Доцент, кафедра компьютерных технологий и систем
Алашеев В.В.

Рецензенты:

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлени ю подготовки 09.03.03 Прикладная информатика, утвержденного приказом Минобрнауки от 19.09.2017 № 922, с учетом трудовых функций профессиональных стандартов: "Специалист по информационным системам", утвержден приказом Минтруда России от 13.07.2023 № 586н; "Руководитель проектов в области информационных технологий", утвержден приказом Минтруда России от 27.04.2023 № 369н; "Руководитель проектов в области информационных технологий", утвержден приказом Минтруда России от 18.11.2014 № 893н; "Специалист по информационным системам", утвержден приказом Минтруда России от 18.11.2014 № 896н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - Целью освоения дисциплины «Информационная безопасность» является формирование у обучаемых знаний в области теоретических основ информационной безопасности (ИБ) и защиты информации (ЗИ), умений и навыков практического обеспечения ее защиты, безопасного использования программных средств в системах защиты информации (СЗИ) вычислительных систем и сетей (ВСС).

Задачи изучения дисциплины:

- - изучения теоретических основ информационной безопасности;;
- - отработки умений и навыков ее эффективного практического ¶использования при информатизации экономической деятельности;¶;
- повышения уровня профессиональной культуры и дисциплины, ¶понимания необходимости грамотного применения ИБ в ИТС..

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

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 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Знать:

ОПК-3.1/Зн1 Принципы решения стандартных задач профессиональной деятельности

ОПК-3.1/Зн2 Методы решения стандартных задач профессиональной деятельности

ОПК-3.1/Зн3 Средства решения стандартных задач профессиональной деятельности

ОПК-3.2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Уметь:

ОПК-3.2/Ум1 Решать стандартные задачи профессиональной деятельности на основе информационной и ибилиографической культуры с применением информационно-коммуникационных технологий

ОПК-3.2/Ум2 Решать стандартные задачи профессиональной деятельности на основе информационной и ибилиографической культуры с учетом требований информационной безопасности

ОПК-3.3 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

Владеть:

ОПК-3.3/Нв1 Навыками подготовки аннотаций с учетом требований информационной безопасности

ОПК-3.3/Нв2 Навыками составления рефератов с учетом требований информационной безопасности

ОПК-3.3/Нв3 Навыками составления научных докладов с учетом требований информационной безопасности

ОПК-3.3/Нв4 Навыками составления библиографии по научно-исследовательской работе с учетом требований информационной безопасности

ПК-П3 Способен проектировать ис по видам обеспечения

ПК-П3.1 Знает существующие методы построения моделей социально-экономических и организационно-технических систем, их архитектуры, а также теорию и средства проектирования структур данных и информационных процессов для проектирования ис

Знать:

ПК-П3.1/Зн2 Возможности ис

ПК-П3.1/Зн4 Основы информационной безопасности организации

Уметь:

ПК-П3.1/Ум3 Разрабатывать документы проекта в области ит

ПК-П3.2 Умеет анализировать данные, полученные по результатам моделирования, проектировать ис и проводить верификацию её архитектуры

Знать:

ПК-П3.2/Зн2 Предметная область автоматизации

ПК-П3.2/Зн13 Основы иб организации

Уметь:

ПК-П3.2/Ум1 Проводить переговоры с заинтересованными сторонами в рамках выполнения работ по созданию (модификации) и сопровождению ис

Владеть:

ПК-П3.2/Нв1 Выявление первоначальных требований заказчика к типовой ис на этапе предконтрактных работ

ПК-П3.2/Нв2 Информирование заказчика о возможностях типовой ис на этапе предконтрактных работ

ПК-П3.3 Владеет навыками применения современных инструментальных средств, при разработке моделей и проектировании информационных процессов для разработки ис

Знать:

ПК-П3.3/Зн2 Предметная область автоматизации

ПК-П3.3/Зн3 Возможности ис

Уметь:

ПК-П3.3/Ум1 Анализировать входные данные в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ис

Владеть:

ПК-П3.3/Нв1 Выбор технологии управления требованиями в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ис

ПК-П10 Способен принимать участие в организации ит-инфраструктуры и управлении информационной безопасностью

ПК-П10.1 Знает методы и модели организации ит-инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ис

Знать:

ПК-П10.1/Зн1 Основы юридических отношений между контрагентами

ПК-П10.1/Зн2 Основы информационной безопасности организации

ПК-П10.1/Зн3 Инструменты и методы выдачи и контроля поручений

Уметь:

ПК-П10.1/Ум1 Разрабатывать договоры по проекту в области ит на основе типовой формы

ПК-П10.1/Ум2 Анализировать входные данные проекта в области ит

ПК-П10.1/Ум3 Контролировать исполнение выданных поручений в рамках проекта в области ит

Владеть:

ПК-П10.1/Нв1 Организация подписания договоров о неразглашении информации, полученной от заказчика проекта в области ит, внутри организации

ПК-П10.1/Нв2 Осуществление мероприятий по обеспечению соблюдения договоров о неразглашении информации, полученной от заказчика проекта в области ит

ПК-П10.2 Умеет применять методы и модели организации ит- инфраструктуры; виды угроз и меры по обеспечению информационной безопасности ис

Знать:

ПК-П10.2/Зн6 Источники информации, необходимой для профессиональной деятельности при выполнении работ по созданию (модификации) и сопровождению ис

ПК-П10.2/Зн7 Лучшие практики создания (модификации) и сопровождения ис в экономике

Уметь:

ПК-П10.2/Ум1 Анализировать входные данные в рамках выполнения работ по созданию (модификации) и сопровождению ис

ПК-П10.3 Владеет навыками организации ит- инфраструктуры и управления информационной безопасностью, в т.ч., обеспечения и контроля соответствия технических, программных и коммуникационных средств для функционирования ис, разграничение прав доступа к ис

Знать:

ПК-П10.3/Зн4 Предметная область автоматизации

ПК-П10.3/Зн13 Основы иб организации

Владеть:

ПК-П10.3/Нв1 Настройка ис для оптимального решения задач заказчика в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ис

ПК-П10.3/Нв2 Параметрическая настройка ис в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ис

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Информационная безопасность» относится к обязательной части образовательной программы и изучается в семестре(ах): Очная форма обучения - 4, Заочная форма обучения - 4.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Очная форма обучения

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Внеаудиторная контактная работа (часы)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
Четвертый семестр	108	3	49	1	16	32	59	Зачет с оценкой
Всего	108	3	49	1	16	32	59	

Заочная форма обучения

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Внеаудиторная контактная работа (часы)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
Четвертый семестр	108	3	11	1	4	6	97	Зачет с оценкой
Всего	108	3	11	1	4	6	97	

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Очная форма обучения

Наименование раздела, темы	Всего	Внеаудиторная контактная работа	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Основы информационной безопасности	**27**		**4**	**8**	**15**	ОПК-3.1 ОПК-3.2 ОПК-3.3

Тема 1.1. Основы информационной безопасности. Основные понятия и определения.	9		2	2	5	ПК-П3.1 ПК-П3.2 ПК-П3.3 ПК-П10.1 ПК-П10.2 ПК-П10.3
Тема 1.2. Основные стандарты в области информационнойбезопасности	9		2	2	5	
Тема 1.3. Политика государства в области информационной безопасности.	9			4	5	
Раздел 2. Модель угроз информационной безопасности.	**22**		**4**	**8**	**10**	ОПК-3.1 ОПК-3.2 ОПК-3.3
Тема 2.1. Модель угроз информационной безопасности.	11		2	4	5	ПК-П3.1 ПК-П3.2 ПК-П3.3
Тема 2.2. Методы контроля и разграничения доступа.	11		2	4	5	ПК-П10.1 ПК-П10.2 ПК-П10.3
Раздел 3. Меры обеспечения защиты информации.	**49**	**1**	**6**	**14**	**28**	ОПК-3.1 ОПК-3.2
Тема 3.1. Меры обеспечения защиты информации.	9		2	2	5	ОПК-3.3 ПК-П3.1
Тема 3.2. Криптографические методы защиты информации.	9		2	2	5	ПК-П3.2 ПК-П3.3
Тема 3.3. Техническая защита информации.	10		2	2	6	ПК-П10.1 ПК-П10.2
Тема 3.4. Программно-технические меры защиты информации.	10			4	6	ПК-П10.3
Тема 3.5. Системы обнаружения и предотвращения компьютерных атак.	11	1		4	6	
Раздел 4. Политика безопасности организации.	**10**		**2**	**2**	**6**	ОПК-3.1 ОПК-3.2 ОПК-3.3 ПК-П3.1
Тема 4.1. Политика безопасности организации.	10		2	2	6	ПК-П3.2 ПК-П3.3 ПК-П10.1 ПК-П10.2 ПК-П10.3
Итого	**108**	**1**	**16**	**32**	**59**	

Заочная форма обучения

Наименование раздела, темы		иторная контактная работа	нные занятия	ческие занятия	оятельная работа	уемые результаты ия, соотнесенные с атами освоения мы

	Всего	Внеауд	Лекцио	Практи	Самост	Планир обучени результ програм
Раздел 1. Основы информационной безопасности	**36**		**4**	**2**	**30**	ОПК-3.1 ОПК-3.2 ОПК-3.3
Тема 1.1. Основы информационной безопасности. Основные понятия и определения.	12		2		10	ПК-П3.1 ПК-П3.2 ПК-П3.3 ПК-П10.1 ПК-П10.2 ПК-П10.3
Тема 1.2. Основные стандарты в области информационнойбезопасности	12		2		10	
Тема 1.3. Политика государства в области информационной безопасности.	12			2	10	
Раздел 2. Модель угроз информационной безопасности.	**17**	**1**		**2**	**14**	ОПК-3.1 ОПК-3.2 ОПК-3.3
Тема 2.1. Модель угроз информационной безопасности.	6			2	4	ПК-П3.1 ПК-П3.2 ПК-П3.3
Тема 2.2. Методы контроля и разграничения доступа.	11	1			10	ПК-П10.1 ПК-П10.2 ПК-П10.3
Раздел 3. Меры обеспечения защиты информации.	**50**				**50**	ОПК-3.1 ОПК-3.2 ОПК-3.3
Тема 3.1. Меры обеспечения защиты информации.	10				10	ПК-П3.1 ПК-П3.2 ПК-П3.3 ПК-П10.1 ПК-П10.2 ПК-П10.3
Тема 3.2. Криптографические методы защиты информации.	10				10	
Тема 3.3. Техническая защита информации.	10				10	
Тема 3.4. Программно-технические меры защиты информации.	10				10	
Тема 3.5. Системы обнаружения и предотвращения компьютерных атак.	10				10	
Раздел 4. Политика безопасности организации.	**5**			**2**	**3**	ОПК-3.1 ОПК-3.2 ОПК-3.3 ПК-П3.1 ПК-П3.2 ПК-П3.3 ПК-П10.1 ПК-П10.2 ПК-П10.3
Тема 4.1. Политика безопасности организации.	5			2	3	
Итого	**108**	**1**	**4**	**6**	**97**	

5.2. Содержание разделов, тем дисциплин

Раздел 1. Основы информационной безопасности
(Заочная: Лекционные занятия - 4ч.; Практические занятия - 2ч.; Самостоятельная работа - 30ч.; Очная: Лекционные занятия - 4ч.; Практические занятия - 8ч.; Самостоятельная работа - 15ч.)

Тема 1.1. Основы информационной безопасности. Основные понятия и определения.
(Заочная: Лекционные занятия - 2ч.; Самостоятельная работа - 10ч.; Очная: Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 5ч.)
1. Понятие информации.
2. Доступ, обработка и защита информации.
3. Информационные системы.
4. Информационная безопасность.

Тема 1.2. Основные стандарты в области информационнойбезопасности
(Заочная: Лекционные занятия - 2ч.; Самостоятельная работа - 10ч.; Очная: Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 5ч.)
1. Категории стандартов Российской Федерации.
2. Основные действующие стандарты РФ в области информационной безопасности.
3. Группа стандартов Р ИСО/МЭК 27000.
4. Стандарты в области криптографической защиты.
5. Стандарты Р ИСО/МЭК 15408 "Общие критерии".
6. Руководящие документы уполномоченных органов (регуляторов) Российской Федерации.

Тема 1.3. Политика государства в области информационной безопасности.
(Заочная: Практические занятия - 2ч.; Самостоятельная работа - 10ч.; Очная: Практические занятия - 4ч.; Самостоятельная работа - 5ч.)
1. Стратегия национальной безопасности.
2. Доктрина информационной безопасности.
3. Законодательство в области защиты информации.
4. Государственная тайна.
5. Коммерческая тайна.
6. Персональные данные.

Раздел 2. Модель угроз информационной безопасности.
(Заочная: Внеаудиторная контактная работа - 1ч.; Практические занятия - 2ч.; Самостоятельная работа - 14ч.; Очная: Лекционные занятия - 4ч.; Практические занятия - 8ч.; Самостоятельная работа - 10ч.)

Тема 2.1. Модель угроз информационной безопасности.
(Очная: Лекционные занятия - 2ч.; Практические занятия - 4ч.; Самостоятельная работа - 5ч.; Заочная: Практические занятия - 2ч.; Самостоятельная работа - 4ч.)
1. Назначение и структура модели угроз ИБ.
2. Принцип оценки актуальности угроз.
3. Оценка возможности реализации угроз, степени ущерба и ее актуальности.

Тема 2.2. Методы контроля и разграничения доступа.
(Заочная: Внеаудиторная контактная работа - 1ч.; Самостоятельная работа - 10ч.; Очная: Лекционные занятия - 2ч.; Практические занятия - 4ч.; Самостоятельная работа - 5ч.)
1. Основные понятия контроля доступа субъектов.
2. Аутентификация субъектов доступа.
3. Модели разграничения доступа.

Раздел 3. Меры обеспечения защиты информации.
(Очная: Внеаудиторная контактная работа - 1ч.; Лекционные занятия - 6ч.; Практические занятия - 14ч.; Самостоятельная работа - 28ч.; Заочная: Самостоятельная работа - 50ч.)

Тема 3.1. Меры обеспечения защиты информации.
(Очная: Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 5ч.; Заочная: Самостоятельная работа - 10ч.)
1. Организация защиты информации.
2. Организационные защиты информации.
3. Программно-технические средства защиты информации.

Тема 3.2. Криптографические методы защиты информации.
(Очная: Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 5ч.; Заочная: Самостоятельная работа - 10ч.)
1. Криптографические методы защиты данных.
2. Шифры.
3. Компьютерные вирусы.

Тема 3.3. Техническая защита информации.
(Очная: Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 6ч.; Заочная: Самостоятельная работа - 10ч.)
1. Основные понятия технической защиты инфориации.
2. Технические каналы утечки информации.
3. Принципы осуществления технической разведки.
4. Принципы защиты от технической разведки.

Тема 3.4. Программно-технические меры защиты информации.
(Очная: Практические занятия - 4ч.; Самостоятельная работа - 6ч.; Заочная: Самостоятельная работа - 10ч.)
1. Сервисы безопасности.
2. Антивирусная защита.
3. Межсетевое экранирование.
4. Системы предотвращения утечки информации.
5. Протоколирование и аудит.

Тема 3.5. Системы обнаружения и предотвращения компьютерных атак.
(Очная: Внеаудиторная контактная работа - 1ч.; Практические занятия - 4ч.; Самостоятельная работа - 6ч.; Заочная: Самостоятельная работа - 10ч.)
1. Назначения систем обнаружения и предотвращения компьютерных атак.
2. Понятие компьютерной атаки.
3. Требования к системам обнаружения и предотвращения компьютерных атак.
4. Классификация систем обнаружения и предотвращения компьютерных атак.
5. Критерии выбора систем обнаружения и предотвращения компьютерных атак.

Раздел 4. Политика безопасности организации.
(Очная: Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 6ч.; Заочная: Практические занятия - 2ч.; Самостоятельная работа - 3ч.)

Тема 4.1. Политика безопасности организации.
(Очная: Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 6ч.; Заочная: Практические занятия - 2ч.; Самостоятельная работа - 3ч.)

1. Понятие политики безопасности.
2. Назначение и содержание политики безопасности.
3. Вопросы, рассматриваемые в политике безопасности.
4. Жизненный цикл политики безопасности.

6. Оценочные материалы текущего контроля

Раздел 1. Основы информационной безопасности

Форма контроля/оценочное средство: Кейс-задание

Вопросы/Задания:

1. Дайте определение "Информация" согласно ФЗ-149?

Дать определение

2. Федеральный закон № 149-ФЗ, название?

Название 149-ФЗ

3. Дать определение "Информационная безопасность" и пояснить свойства информации?

Дать развернутый ответ

4. Категории стандартов РФ?

Дать классификацию

5. Суть Стратегии национальной безопасности РФ?

Описать суть документа

Раздел 2. Модель угроз информационной безопасности.

Форма контроля/оценочное средство: Кейс-задание

Вопросы/Задания:

1. Структура модели угроз информационной безопасности.

Описать структуру

2. Типы нарушителя?

Дать определеня

3. Модели разграничения доступа?

Описать модели

Раздел 3. Меры обеспечения защиты информации.

Форма контроля/оценочное средство: Кейс-задание

Вопросы/Задания:

1. Требования к криптографическим средствам защиты

Перечислить требования

2. Перечислите разделы криптографии?

Перечислить разделы

3. Пояснить классические методы шифрования (подстановки, перестановки)?

Перечислить методы с пояснением

4. Свойства компьютерных вирусов?

Перечислить свойства.

5. Технический канал утечки информации, определене.

Дать определение

6. Вредоносная программа согласно УК РФ.

Дать определение

7. Основное назначение систем обнаружения и предотвращения атак?

Основное назначение систем обнаружения и предотвращения атак.

Раздел 4. Политика безопасности организации.

Форма контроля/оценочное средство: Кейс-задание

Вопросы/Задания:

1. Цель разработки политики безопасности

Определить цель

2. Рекомендации по обеспечению эффективности политики безопасности?

Перечислить рекомендации

3. Вопросы рассматриваемые в политики безопасности?

Указать вопросы рассматриваемые в политики безопасности.

7. Оценочные материалы промежуточной аттестации

Очная форма обучения, Четвертый семестр, Зачет с оценкой

Контролируемые ИДК: ОПК-3.1 ОПК-3.2 ОПК-3.3 ПК-П3.1 ПК-П10.1 ПК-П3.2 ПК-П10.2 ПК-П3.3 ПК-П10.3

Вопросы/Задания:

1. Вопросы к зачету

Вопросы к зачету

1. Международные стандарты информационной безопасности.
2. Концепция информационной безопасности страны.
3. Место информационной безопасности в социально-экономических системах.
4. Основные нормативные руководящие документы, касающиеся государственной тайны.
5. Виды возможных нарушений информационной системы.
6. Актуальность проблемы информационной безопасности.
7. Модели безопасности и их применение.
8. Классификация методов ИБ от несанкционированного доступа (НСД).
9. Классификация средств ИБ от НСД.
10. Механизмы ИБ от НСД.
11. Государственные требования к системам ИБ.
12. Концепция ИБ от НСД.
13. Требования к криптографическим средствам систем ЗИ (СЗИ).
14. Показатели защищенности средств вычислительной техники (СВТ) от НСД.
15. Классификация компьютерных систем и требования ИБ к ним.
16. Использование защищенных компьютерных систем (КС).
17. Методы контроля доступа к ресурсам КС.
18. Способы фиксации факта доступа.
19. Структура и функции подсистемы контроля доступа программ и пользователей.
20. Средства активного аудита компьютерных систем.
21. Идентификация и аутентификация субъектов и объектов КС.
22. Основные подходы к защите данных от НСД.
23. Модели управления доступом.
24. Дискреционная (избирательная) и мандатная (полномочная) модель управления доступом.
25. Защита алгоритма шифрования и программно-аппаратные средства шифрования.
26. Построение аппаратных компонент криптозащиты данных.
27. Взаимодействие прикладных программ и программы злоумышленника.
28. Классификация разрушающих программных средств и их воздействий.
29. Компьютерные вирусы (КВ) как класс разрушающих программных воздействий.
30. Сущность, проявление, классификация КВ.

31. Необходимые и достаточные условия недопущения разрушающих программных воздействий.
32. Организационные средства защиты от КВ.
33. Роль морально-этических факторов в устранении угрозы разрушающих программных воздействий.
34. Проблема обеспечение целостности информации.
35. Способы обеспечения целостности информации.
36. Электронная цифровая подпись.
37. Криптографические хэш-функции. Схемы вычисления хэш-функции.
38. Методы криптографии и задачи, решаемые криптографическими средствами в КС.
39. Алгоритмы криптографических преобразований, их характеристики.
40. Методы и средства ограничения доступа к компонентам компьютеров.

Заочная форма обучения, Четвертый семестр, Зачет с оценкой
Контролируемые ИДК: ОПК-3.1 ОПК-3.2 ОПК-3.3 ПК-П3.1 ПК-П10.1 ПК-П3.2 ПК-П10.2 ПК-П3.3 ПК-П10.3
Вопросы/Задания:

1. Вопросы к зачету

Вопросы к зачету
1. Международные стандарты информационной безопасности.
2. Концепция информационной безопасности страны.
3. Место информационной безопасности в социально-экономических системах.
4. Основные нормативные руководящие документы, касающиеся государственной тайны.
5. Виды возможных нарушений информационной системы.
6. Актуальность проблемы информационной безопасности.
7. Модели безопасности и их применение.
8. Классификация методов ИБ от несанкционированного доступа (НСД).
9. Классификация средств ИБ от НСД.
10. Механизмы ИБ от НСД.
11. Государственные требования к системам ИБ.
12. Концепция ИБ от НСД.
13. Требования к криптографическим средствам систем ЗИ (СЗИ).
14. Показатели защищенности средств вычислительной техники (СВТ) от НСД.
15. Классификация компьютерных систем и требования ИБ к ним.
16. Использование защищенных компьютерных систем (КС).
17. Методы контроля доступа к ресурсам КС.
18. Способы фиксации факта доступа.
19. Структура и функции подсистемы контроля доступа программ и пользователей.
20. Средства активного аудита компьютерных систем.
21. Идентификация и аутентификация субъектов и объектов КС.
22. Основные подходы к защите данных от НСД.
23. Модели управления доступом.
24. Дискреционная (избирательная) и мандатная (полномочная) модель управления доступом.
25. Защита алгоритма шифрования и программно-аппаратные средства шифрования.
26. Построение аппаратных компонент криптозащиты данных.
27. Взаимодействие прикладных программ и программы злоумышленника.
28. Классификация разрушающих программных средств и их воздействий.

29. Компьютерные вирусы (КВ) как класс разрушающих программных воздействий.
30. Сущность, проявление, классификация КВ.
31. Необходимые и достаточные условия недопущения разрушающих программных воздействий.
32. Организационные средства защиты от КВ.
33. Роль морально-этических факторов в устранении угрозы разрушающих программных воздействий.
34. Проблема обеспечение целостности информации.
35. Способы обеспечения целостности информации.
36. Электронная цифровая подпись.
37. Криптографические хэш-функции. Схемы вычисления хэш-функции.
38. Методы криптографии и задачи, решаемые криптографическими средствами в КС.
39. Алгоритмы криптографических преобразований, их характеристики.
40. Методы и средства ограничения доступа к компонентам компьютеров.

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Горюхина,, Е. Ю. Информационная безопасность: учебное пособие / Е. Ю. Горюхина,, Л. И. Литвинова,, Н. В. Ткачева,. - Информационная безопасность - Воронеж: Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015. - 221 c. - 2227-8397. - Текст: электронный // IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/72672.html (дата обращения: 19.06.2025). - Режим доступа: по подписке

2. Петров,, С. В. Информационная безопасность: учебное пособие / С. В. Петров,, П. А. Кисляков,. - Информационная безопасность - Саратов: Ай Пи Ар Букс, 2015. - 326 c. - 978-5-906-17271-6. - Текст: электронный // IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/33857.html (дата обращения: 19.06.2025). - Режим доступа: по подписке

Дополнительная литература

1. Сагдеев К. М. Физические основы защиты информации: учебное пособие. направление подготовки 10.03.01 - информационная безопасность. бакалавриат / Сагдеев К. М., Петренко В. И., Чипига А. Ф.. - Ставрополь: СКФУ, 2015. - 394 с. - Текст: электронный. // RuSpLAN: [сайт]. - URL: https://e.lanbook.com/img/cover/book/155272.jpg (дата обращения: 19.06.2025). - Режим доступа: по подписке

2. Горюхина Е. Ю. Информационная безопасность: учебное пособие / Горюхина Е. Ю.. - Воронеж: ВГАУ, 2015. - 220 с. - Текст: электронный. // RuSpLAN: [сайт]. - URL: https://e.lanbook.com/img/cover/book/181761.jpg (дата обращения: 19.06.2025). - Режим доступа: по подписке

8.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. https://elibrary.ru/ - Научная электронная библиотека «eLIBRARY.RU»

Ресурсы «Интернет»

1. http://www.iprbookshop.ru/ - IPRbook

8.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине позволяют:
– обеспечить взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети «Интернет»;
– фиксировать ход образовательного процесса, результатов промежуточной аттестации по дисциплине и результатов освоения образовательной программы;
– организовать процесс образования путем визуализации изучаемой информации посредством использования презентаций, учебных фильмов;
– контролировать результаты обучения на основе компьютерного тестирования.
Перечень лицензионного программного обеспечения:
1 Microsoft Windows - операционная система.
2 Microsoft Office (включает Word, Excel, Power Point) - пакет офисных приложений.
Перечень профессиональных баз данных и информационных справочных систем:
1 Гарант - правовая, https://www.garant.ru/
2 Консультант - правовая, https://www.consultant.ru/
3 Научная электронная библиотека eLibrary - универсальная, https://elibrary.ru/
Доступ к сети Интернет, доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Не используется.

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Не используется.

8.4. Специальные помещения, лаборатории и лабораторное оборудование

Университет располагает на праве собственности или ином законном основании материально-техническим обеспечением образовательной деятельности (помещениями и оборудованием) для реализации программы бакалавриата, специлитета, магистратуры по Блоку 1 "Дисциплины (модули)" и Блоку 3 "Государственная итоговая аттестация" в соответствии с учебным планом.
Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне его. Условия для функционирования электронной информационно-образовательной среды могут быть созданы с использованием ресурсов иных организаций.

Лекционный зал
221гл
Облучатель-рециркулятор воздуха 600 - 1 шт.
401мх
киноэкран ScreeerMedia 180*180 - 0 шт.
Сплит-система настенная QuattroClima Effecto Standard QV/QN-ES24WA - 0 шт.

Компьютерный класс
223гл
Интерактивная панель Samsung - 1 шт.

Компьютер персональный Aquarius i5/4Gb/500Gb/21,5" - 1 шт.
Компьютер персональный i3/2GB/500Gb/21,5" - 1 шт.
Сплит-система LS-H12KPA2/LU-H12KPA2 - 1 шт.
226гл
Интерактивная панель Samsung - 1 шт.
Персональный компьютер HP 6300 Pro SFF/Core i3-3220/4GB/500GB/NoODD/Win7Pro - 1 шт.
Сплит-система LS-H12KPA2/LU-H12KPA2 - 1 шт.

Лаборатория
306зр
Доска интерактивная (доска, проектор, крепления, 87 дюймов) - 0 шт.
Компьютер LENOVO - 0 шт.
Микроскоп Микромед-1 вар 2-20 - 0 шт.
Микроскоп стереоскопический Модель СМ-1 (бинокуляр) - 0 шт.
Микроскоп стереоскопический (бинокуляр) МСП-1 вариант - 2 - 0 шт.
Сплит-система LS-H24KPA2/LU-H24KPA2 - 0 шт.

9. Методические указания по освоению дисциплины (модуля)

Учебная работа по направлению подготовки осуществляется в форме контактной работы с преподавателем, самостоятельной работы обучающегося, текущей и промежуточной аттестаций, иных формах, предлагаемых университетом. Учебный материал дисциплины структурирован и его изучение производится в тематической последовательности. Содержание методических указаний должно соответствовать требованиям Федерального государственного образовательного стандарта и учебных программ по дисциплине. Самостоятельная работа студентов может быть выполнена с помощью материалов, размещенных на портале поддержки Moodl.

Методические указания по формам работы

Лекционные занятия
Передача значительного объема систематизированной информации в устной форме достаточно большой аудитории. Дает возможность экономно и систематично излагать учебный материал. Обучающиеся изучают лекционный материал, размещенный на портале поддержки обучения Moodl.

Лабораторные занятия
Практическое освоение студентами научно-теоретических положений изучаемого предмета, овладение ими техникой экспериментирования в соответствующей отрасли науки. Лабораторные занятия проводятся с использованием методических указаний, размещенных на образовательном портале университета.

Практические занятия
Форма организации обучения, проводимая под руководством преподавателя и служащая для детализации, анализа, расширения, углубления, закрепления, применения (или выполнения разнообразных практических работ, упражнений) и контроля усвоения полученной на лекциях учебной информации. Практические занятия проводятся с использованием учебно-методических изданий, размещенных на образовательном портале университета.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами
Для инвалидов и лиц с ОВЗ может изменяться объём дисциплины (модуля) в часах,

выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося (при этом не увеличивается количество зачётных единиц, выделенных на освоение дисциплины).
Фонды оценочных средств адаптируются к ограничениям здоровья и восприятия информации обучающимися.
Основные формы представления оценочных средств – в печатной форме или в форме электронного документа.
Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ с нарушением зрения:
– устная проверка: дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.;
– с использованием компьютера и специального ПО: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, дистанционные формы, если позволяет острота зрения - графические работы и др.;
– при возможности письменная проверка с использованием рельефно-точечной системы Брайля, увеличенного шрифта, использование специальных технических средств (тифлотехнических средств): контрольные, графические работы, тестирование, домашние задания, эссе, отчеты и др.
Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ с нарушением слуха:
– письменная проверка: контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.;
– с использованием компьютера: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы и др.;
– при возможности устная проверка с использованием специальных технических средств (аудиосредств, средств коммуникации, звукоусиливающей аппаратуры и др.): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.
Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ с нарушением опорно-двигательного аппарата:
– письменная проверка с использованием специальных технических средств (альтернативных средств ввода, управления компьютером и др.): контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.;
– устная проверка, с использованием специальных технических средств (средств коммуникаций): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.;
– с использованием компьютера и специального ПО (альтернативных средств ввода и управления компьютером и др.): работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы предпочтительнее обучающимся, ограниченным в передвижении и др.
Адаптация процедуры проведения промежуточной аттестации для инвалидов и лиц с ОВЗ.
В ходе проведения промежуточной аттестации предусмотрено:
– предъявление обучающимся печатных и (или) электронных материалов в формах, адаптированных к ограничениям их здоровья;
– возможность пользоваться индивидуальными устройствами и средствами, позволяющими адаптировать материалы, осуществлять приём и передачу информации с учетом их индивидуальных особенностей;
– увеличение продолжительности проведения аттестации;
– возможность присутствия ассистента и оказания им необходимой помощи (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с преподавателем).
Формы промежуточной аттестации для инвалидов и лиц с ОВЗ должны учитывать индивидуальные и психофизические особенности обучающегося/обучающихся по АОПОП ВО (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с нарушениями зрения:
– предоставление образовательного контента в текстовом электронном формате, позволяющем

переводить плоскопечатную информацию в аудиальную или тактильную форму;
– возможность использовать индивидуальные устройства и средства, позволяющие адаптировать материалы, осуществлять приём и передачу информации с учетом индивидуальных особенностей и состояния здоровья студента;
– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном образовательном портале;
– использование чёткого и увеличенного по размеру шрифта и графических объектов в мультимедийных презентациях;
– использование инструментов «лупа», «прожектор» при работе с интерактивной доской;
– озвучивание визуальной информации, представленной обучающимся в ходе занятий;
– обеспечение раздаточным материалом, дублирующим информацию, выводимую на экран;
– наличие подписей и описания у всех используемых в процессе обучения рисунков и иных графических объектов, что даёт возможность перевести письменный текст в аудиальный;
– обеспечение особого речевого режима преподавания: лекции читаются громко, разборчиво, отчётливо, с паузами между смысловыми блоками информации, обеспечивается интонирование, повторение, акцентирование, профилактика рассеивания внимания;
– минимизация внешнего шума и обеспечение спокойной аудиальной обстановки;
– возможность вести запись учебной информации студентами в удобной для них форме (аудиально, аудиовизуально, на ноутбуке, в виде пометок в заранее подготовленном тексте);
– увеличение доли методов социальной стимуляции (обращение внимания, апелляция к ограничениям по времени, контактные виды работ, групповые задания и др.) на практических и лабораторных занятиях;
– минимизирование заданий, требующих активного использования зрительной памяти и зрительного внимания;
– применение поэтапной системы контроля, более частый контроль выполнения заданий для самостоятельной работы.
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с нарушениями опорно-двигательного аппарата (маломобильные студенты, студенты, имеющие трудности передвижения и патологию верхних конечностей):
– возможность использовать специальное программное обеспечение и специальное оборудование и позволяющее компенсировать двигательное нарушение (коляски, ходунки, трости и др.);
– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном образовательном портале;
– применение дополнительных средств активизации процессов запоминания и повторения;
– опора на определенные и точные понятия;
– использование для иллюстрации конкретных примеров;
– применение вопросов для мониторинга понимания;
– разделение изучаемого материала на небольшие логические блоки;
– увеличение доли конкретного материала и соблюдение принципа от простого к сложному при объяснении материала;
– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;
– увеличение доли методов социальной стимуляции (обращение внимания, аппеляция к ограничениям по времени, контактные виды работ, групповые задания др.);
– обеспечение беспрепятственного доступа в помещения, а также пребывания них;
– наличие возможности использовать индивидуальные устройства и средства, позволяющие обеспечить реализацию эргономических принципов и комфортное пребывание на месте в течение всего периода учёбы (подставки, специальные подушки и др.).
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с нарушениями слуха (глухие, слабослышащие, позднооглохшие):
– предоставление образовательного контента в текстовом электронном формате, позволяющем переводить аудиальную форму лекции в плоскопечатную информацию;

– наличие возможности использовать индивидуальные звукоусиливающие устройства и сурдотехнические средства, позволяющие осуществлять приём и передачу информации; осуществлять взаимообратный перевод текстовых и аудиофайлов (блокнот для речевого ввода), а также запись и воспроизведение зрительной информации;
– наличие системы заданий, обеспечивающих систематизацию вербального материала, его схематизацию, перевод в таблицы, схемы, опорные тексты, глоссарий;
– наличие наглядного сопровождения изучаемого материала (структурно-логические схемы, таблицы, графики, концентрирующие и обобщающие информацию, опорные конспекты, раздаточный материал);
– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;
– обеспечение практики опережающего чтения, когда студенты заранее знакомятся с материалом и выделяют незнакомые и непонятные слова и фрагменты;
– особый речевой режим работы (отказ от длинных фраз и сложных предложений, хорошая артикуляция; четкость изложения, отсутствие лишних слов; повторение фраз без изменения слов и порядка их следования; обеспечение зрительного контакта во время говорения и чуть более медленного темпа речи, использование естественных жестов и мимики);
– чёткое соблюдение алгоритма занятия и заданий для самостоятельной работы (называние темы, постановка цели, сообщение и запись плана, выделение основных понятий и методов их изучения, указание видов деятельности студентов и способов проверки усвоения материала, словарная работа);
– соблюдение требований к предъявляемым учебным текстам (разбивка текста на час¬ти; выделение опорных смысловых пунктов; использование наглядных средств);
– минимизация внешних шумов;
– предоставление возможности соотносить вербальный и графический материал; комплексное использование письменных и устных средств коммуникации при работе в группе;
– сочетание на занятиях всех видов речевой деятельности (говорения, слушания, чтения, письма, зрительного восприятия с лица говорящего).
Специальные условия, обеспечиваемые в процессе преподавания дисциплины студентам с прочими видами нарушений (ДЦП с нарушениями речи, заболевания эндокринной, центральной нервной и сердечно-сосудистой систем, онкологические заболевания):
– наличие возможности использовать индивидуальные устройства и средства, позволяющие осуществлять приём и передачу информации;
– наличие системы заданий, обеспечивающих систематизацию вербального материала, его схематизацию, перевод в таблицы, схемы, опорные тексты, глоссарий;
– наличие наглядного сопровождения изучаемого материала;
– наличие чёткой системы и алгоритма организации самостоятельных работ и проверки заданий с обязательной корректировкой и комментариями;
– обеспечение практики опережающего чтения, когда студенты заранее знакомятся с материалом и выделяют незнакомые и непонятные слова и фрагменты;
– предоставление возможности соотносить вербальный и графический материал; комплексное использование письменных и устных средств коммуникации при работе в группе;
– сочетание на занятиях всех видов речевой деятельности (говорения, слушания, чтения, письма, зрительного восприятия с лица говорящего);
– предоставление образовательного контента в текстовом электронном формате;
– предоставление возможности предкурсового ознакомления с содержанием учебной дисциплины и материалом по курсу за счёт размещения информации на корпоративном образовательном портале;
– возможность вести запись учебной информации студентами в удобной для них форме (аудиально, аудиовизуально, в виде пометок в заранее подготовленном тексте);
– применение поэтапной системы контроля, более частый контроль выполнения заданий для самостоятельной работы;
– стимулирование выработки у студентов навыков самоорганизации и самоконтроля;
– наличие пауз для отдыха и смены видов деятельности по ходу занятия.

10. Методические рекомендации по освоению дисциплины (модуля)