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

Экономический факультет
Компьютерных технологий и систем

КубГАУ
Документ подписан простой электронной подписью
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 2a00000ab42e061afa7cd1af20000200000ab4
Владелец: Тюпаков Константин Эдуардович
Действителен от 23-05-2021 до 22-05-2026

УТВЕРЖДЕНО
Декан
Тюпаков К.Э.
18.06.2026

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Уровень высшего образования: специалитет

Специальность: 38.05.01 Экономическая безопасность

Направленность (профиль)подготовки: Экономико-правовое обеспечение экономической безопасности

Квалификация (степень) выпускника: экономист

Формы обучения: очная, заочная

Год набора (приема на обучение): 2026

Срок получения образования: Очная форма обучения – 5 лет
Заочная форма обучения – 5 лет 8 месяца(-ев)

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

2026

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

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по специальности 38.05.01 Экономическая безопасность, утвержденного приказом Минобрнауки от 14.04.2021 № 293, с учетом трудовых функций профессиональных стандартов: "Специалист по управлению рисками", утвержден приказом Минтруда России от 18.04.2025 № 264н; "Бухгалтер", утвержден приказом Минтруда России от 21.02.2019 № 103н; "Специалист по финансовому мониторингу (в сфере противодействия легализации доходов, полученных преступным путем, и финансированию терроризма)", утвержден приказом Минтруда России от 24.07.2015 № 512н; "Экономист предприятия", утвержден приказом Минтруда России от 30.03.2021 № 161н; "Внутренний аудитор", утвержден приказом Минтруда России от 24.06.2015 № 398н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	Компьютерных технологий и систем	Заведующий кафедрой, руководитель подразделения, реализующего ОП	Лукьяненко Т.В.	Согласовано	18.06.2026
2	Экономический факультет	Председатель методической комиссии/совета	Толмачев А.В.	Согласовано	18.06.2026
3	Экономики и внешнеэкономической деятельности	Руководитель образовательной программы	Мельников А.Б.	Согласовано	18.06.2026

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование у обучаемых знаний в области теоретических основ информационной безопасности, приобретение ими умений и навыков практического обеспечения ее защиты, безопасного использования программных средств в вычислительных систем и сетей.

Задачи изучения дисциплины:

- изучение теоретических основ информационной безопасности;
- понимания необходимости и способов грамотного применения основ информационной безопасности;
- отработки умений и навыков эффективного практического использования аспектов обеспечения информационной безопасности при осуществлении профессиональной деятельности.

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

Компетенции, индикаторы и результаты обучения

ПК-П6 Способен осуществлять информационно-аналитическое обеспечение предупреждения, выявления, пресечения, раскрытия и расследования экономических и финансовых преступлений, применять технико-криминалистические средства и методы, формы организации и методику раскрытия и расследования преступлений в сфере экономики

ПК-П6.1 Собирает, проверяет и анализирует полученную информацию о финансовых операциях и сделках с признаками од/фт, полученную в результате мониторинга средств массовой информации, информационно-телекоммуникационной сети «интернет», а также в рамках сотрудничества участников профессиональных объединений

Знать:

ПК-П6.1/Зн1 О признаках од/фт

Уметь:

ПК-П6.1/Ум1 Собирать, проверять и анализировать полученную информацию о финансовых операциях и сделках с признаками од/фт, полученную в результате мониторинга средств массовой информации, информационно-телекоммуникационной сети «интернет», а также в рамках сотрудничества участников профессиональных объединений

Владеть:

ПК-П6.1/Нв1 Сбора, проверки и анализа полученной информации о финансовых операциях и сделках с признаками од/фт, полученную в результате мониторинга средств массовой информации, информационно-телекоммуникационной сети «интернет», а также в рамках сотрудничества участников профессиональных объединений

ПК-П6.2 Отбирает материалы финансовых расследований, выделяет характерные признаки подозрительной деятельности, систематизирует признаки и критерии подозрительной деятельности в целях под/фт

Знать:

ПК-П6.2/Зн1 О признаках подозрительной деятельности

Уметь:

ПК-П6.2/Ум1 Собрать материалы финансовых расследований, выделять характерные признаки подозрительной деятельности, систематизирует признаки и критерии подозрительной деятельности в целях под/фт

Владеть:

ПК-П6.2/Нв1 Сьора материалов финансовых расследований, выделять характерные признаки подозрительной деятельности, систематизирует признаки и критерии подозрительной деятельности в целях под/фт

ПК-П6.3 Определяет методы и процедуры судебной экономической экспертизы; исследует документацию, формулирует выводы по каждому поставленному вопросу, составляет заключение и разрабатывает по итогам экспертизы необходимые рекомендации.

Знать:

ПК-П6.3/Зн1 О методах и процедурах судебной экономической экспертизы; документацию, используемую экспертом-экономистом, о стуртуреи содержании заключения судебного эксперта

Уметь:

ПК-П6.3/Ум1 Применять методы и процедуры судебной экономической экспертизы; исследовать документацию, формулировать выводы по каждому поставленному вопросу, составлять заключение и разрабатывать по итогам экспертизы необходимые рекомендации

Владеть:

ПК-П6.3/Нв1 Определять методы и процедуры судебной экономической экспертизы; исследовать документацию, формулировать т выводы по каждому поставленному вопросу, составлять заключение и разрабатывать по итогам экспертизы необходимые рекомендации

ПК-П6.4 Осуществляет финансовый анализ информации об операциях в совокупности с внешними информационными ресурсами с целью выявления типовых схем отмывания преступных доходов, действующих в различных регионах, отраслях и секторах экономики в целях под/фт

Знать:

ПК-П6.4/Зн1 Типовые схемы отмывания преступных доходов, действующих в различных регионах, отраслях и секторах экономики в целях под/фт

Уметь:

ПК-П6.4/Ум1 Осуществлять финансовый анализ информации об операциях в совокупности с внешними информационными ресурсами с целью выявления типовых схем отмывания преступных доходов, действующих в различных регионах, отраслях и секторах экономики в целях под/фт

Владеть:

ПК-П6.4/Нв1 Осущвления финансового анализа информации об операциях в совокупности с внешними информационными ресурсами с целью выявления типовых схем отмывания преступных доходов, действующих в различных регионах, отраслях и секторах экономики в целях под/фт

ПК-П6.5 Подготавливает экспертно-оценочные материалы, содержащие информацию об участниках финансовых операций, признаках подозрительности и вопросах, подлежащих выяснению в ходе проведения проверок и финансовых расследований, формулирует выводы и рекомендации по ре-зультатам проведенного анализа

Знать:

ПК-П6.5/Зн1 Об экспертно-оценочных материалах, содержащих информацию об участниках финансовых операций, признаках подозрительности и вопросах, подлежащих выяснению в ходе проведения проверок и финансовых расследований

Уметь:

ПК-П6.5/Ум1 Подготавливать экспертно-оценочные материалы, содержащие информацию об участниках финансовых операций, признаках подозрительности и вопросах, подлежащих выяснению в ходе проведения проверок и финансовых расследований, формулировать выводы и рекомендации по результатам проведенного анализа

Владеть:

ПК-П6.5/Нв1 Подготовки экспертно-оценочных материалов, содержащих информацию об участниках финансовых операций, признаках подозрительности и вопросах, подлежащих выяснению в ходе проведения проверок и финансовых расследований, формулировать выводы и рекомендации по результатам проведенного анализа

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Информационная безопасность» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): Очная форма обучения - 7, Заочная форма обучения - 7.

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)	Зачет (часы)	Лабораторные занятия (часы)	Лекционные занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
Седьмой семестр	108	3	37	1		16	20	71	Зачет
Всего	108	3	37	1		16	20	71	

Заочная форма обучения

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Внеаудиторная контактная работа (часы)	Зачет (часы)	Лабораторные занятия (часы)	Лекционные занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
Седьмой семестр	108	3	13	1		8	4	95	Зачет
Всего	108	3	13	1		8	4	95	

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	Лабораторные занятия	Лекционные занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Основы информационной безопасности	**31**		**4**	**6**	**21**	ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Тема 1.1. Основы информационной безопасности. Основные понятия и определения.	9			2	7	
Тема 1.2. Основные стандарты в области информационнойбезопасности	11		2	2	7	
Тема 1.3. Политика государства в области информационной безопасности.	11		2	2	7	
Раздел 2. Модель угроз информационной безопасности.	**22**		**4**	**4**	**14**	ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Тема 2.1. Модель угроз информационной безопасности.	11		2	2	7	
Тема 2.2. Методы контроля и разграничения доступа.	11		2	2	7	
Раздел 3. Меры обеспечения защиты информации.	**55**	**1**	**8**	**10**	**36**	ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Тема 3.1. Меры обеспечения защиты информации.	11		2	2	7	
Тема 3.2. Криптографические методы защиты информации.	11		2	2	7	
Тема 3.3. Техническая защита информации.	11		2	2	7	
Тема 3.4. Программно-технические меры защиты информации.	11		2	2	7	
Тема 3.5. Системы обнаружения и предотвращения компьютерных атак.	11	1		2	8	
Итого	**108**	**1**	**16**	**20**	**71**	

Заочная форма обучения

Наименование раздела, темы	Всего	Внеаудиторная контактная работа	Лабораторные занятия	Лекционные занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Основы информационной безопасности	**34**	**1**	**2**	**4**	**27**	ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Тема 1.1. Основы информационной безопасности. Основные понятия и определения.	12			2	10	
Тема 1.2. Основные стандарты в области информационнойбезопасности	11	1	2		8	
Тема 1.3. Политика государства в области информационной безопасности.	11			2	9	
Раздел 2. Модель угроз информационной безопасности.	**22**		**2**		**20**	ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Тема 2.1. Модель угроз информационной безопасности.	12		2		10	
Тема 2.2. Методы контроля и разграничения доступа.	10				10	
Раздел 3. Меры обеспечения защиты информации.	**52**		**4**		**48**	ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Тема 3.1. Меры обеспечения защиты информации.	10				10	
Тема 3.2. Криптографические методы защиты информации.	11		2		9	
Тема 3.3. Техническая защита информации.	11		2		9	
Тема 3.4. Программно-технические меры защиты информации.	10				10	
Тема 3.5. Системы обнаружения и предотвращения компьютерных атак.	10				10	
Итого	**108**	**1**	**8**	**4**	**95**	

5.2. Содержание разделов, тем дисциплин

Раздел 1. Основы информационной безопасности
(Заочная: Внеаудиторная контактная работа - 1ч.; Лабораторные занятия - 2ч.; Лекционные занятия - 4ч.; Самостоятельная работа - 27ч.; Очная: Лабораторные занятия - 4ч.; Лекционные занятия - 6ч.; Самостоятельная работа - 21ч.)

Тема 1.1. Основы информационной безопасности. Основные понятия и определения.
(Заочная: Лекционные занятия - 2ч.; Самостоятельная работа - 10ч.; Очная: Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.)
1. Понятие информации.
2. Доступ, обработка и защита информации.
3. Информационные системы.
4. Информационная безопасность.

Тема 1.2. Основные стандарты в области информационнойбезопасности
(Заочная: Внеаудиторная контактная работа - 1ч.; Лабораторные занятия - 2ч.; Самостоятельная работа - 8ч.; Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.)
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.
(Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.; Заочная: Лекционные занятия - 2ч.; Самостоятельная работа - 9ч.)
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: Лабораторные занятия - 2ч.; Самостоятельная работа - 20ч.; Очная: Лабораторные занятия - 4ч.; Лекционные занятия - 4ч.; Самостоятельная работа - 14ч.)

Тема 2.1. Модель угроз информационной безопасности.
(Заочная: Лабораторные занятия - 2ч.; Самостоятельная работа - 10ч.; Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.)
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.
(Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.; Заочная: Самостоятельная работа - 10ч.)
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.; Лабораторные занятия - 8ч.; Лекционные занятия - 10ч.; Самостоятельная работа - 36ч.; Заочная: Лабораторные занятия - 4ч.; Самостоятельная работа - 48ч.)

Тема 3.1. Меры обеспечения защиты информации.
(Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.; 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.
(Заочная: Лабораторные занятия - 2ч.; Самостоятельная работа - 9ч.; Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.)

1. Криптографические методы защиты данных.
2. Шифры.
3. Компьютерные вирусы.

Тема 3.3. Техническая защита информации.
(Заочная: Лабораторные занятия - 2ч.; Самостоятельная работа - 9ч.; Очная: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.)

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: Лабораторные занятия - 2ч.; Лекционные занятия - 2ч.; Самостоятельная работа - 7ч.; 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.; Лекционные занятия - 2ч.; Самостоятельная работа - 8ч.; 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.

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.

7. Оценочные материалы промежуточной аттестации

Очная форма обучения, Седьмой семестр, Зачет

Контролируемые ИДК: ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5

Вопросы/Задания:

1. Вопросы к зачету

1. Международные стандарты информационного обмена.
2. Концепция информационной безопасности страны.
3. Место информационной безопасности в социально-экономических системах.
4. Основные нормативные руководящие документы, касающиеся государственной тайны.
5. Таксономия нарушений ИБ вычислительной системы
6. Три вида возможных нарушений информационной системы
7. Актуальность проблемы информационной безопасности.
8. Модели безопасности и их применение.

9. Классификация методов ИБ от несанкционированного доступа (НСД).
10. Классификация средств ИБ от НСД.
11. Механизмы ИБ от НСД.
12. Государственные требования к системам ИБ.
13. Концепция ИБ от НСД.
14. Требования к криптографическим средствам систем ЗИ (СЗИ).
15. Показатели защищенности средств вычислительной техники (СВТ) от НСД.
16. Классификация компьютерных систем и требования ИБ к них.
17. Использование защищенных компьютерных систем.
18. Методы контроля доступа к ресурсам компьютерных систем.
19. Способы фиксации факта доступа.
20. Структура и функции подсистемы контроля доступа программ и пользователей.
21. Средства активного аудита компьютерных систем.
22. Идентификация и аутентификация субъектов и объектов компьютерных систем.
23. Идентифицирующая информация и протоколы идентификации.
24. Основные подходы к защите данных от НСД.
25. Иерархический доступ к файлу.
26. Доступ к данным со стороны процесса.
27. Понятие скрытого доступа.
28. Модели управления доступом.
29. Дискреционная (избирательная) и мандатная (полномочная) модель управления доступом.
30. Защита алгоритма шифрования и программно-аппаратные средства шифрования.
31. Построение аппаратных компонент криптозащиты данных.
32. Сущность разрушающих программных средств.
33. Взаимодействие прикладных программ и программы злоумышленника.
34. Классификация разрушающих программных средств и их воздействий.
35. Компьютерные вирусы (КВ) как класс разрушающих программных воздействий.
36. Сущность, проявление, классификация КВ.
37. Необходимые и достаточные условия недопущения разрушающих программных воздействий.
38. Понятие изолированной программной среды.
39. Организационные средства защиты от КВ.
40. Роль морально-этических факторов в устранении угрозы разрушающих программных воздействий.

Заочная форма обучения, Седьмой семестр, Зачет
Контролируемые ИДК: ПК-П6.1 ПК-П6.2 ПК-П6.3 ПК-П6.4 ПК-П6.5
Вопросы/Задания:

1. Вопросы к зачету

1. Международные стандарты информационного обмена.
2. Концепция информационной безопасности страны.
3. Место информационной безопасности в социально-экономических системах.
4. Основные нормативные руководящие документы, касающиеся государственной тайны.
5. Таксономия нарушений ИБ вычислительной системы
6. Три вида возможных нарушений информационной системы
7. Актуальность проблемы информационной безопасности.
8. Модели безопасности и их применение.
9. Классификация методов ИБ от несанкционированного доступа (НСД).
10. Классификация средств ИБ от НСД.
11. Механизмы ИБ от НСД.
12. Государственные требования к системам ИБ.
13. Концепция ИБ от НСД.
14. Требования к криптографическим средствам систем ЗИ (СЗИ).
15. Показатели защищенности средств вычислительной техники (СВТ) от НСД.

16. Классификация компьютерных систем и требования ИБ к них.
17. Использование защищенных компьютерных систем.
18. Методы контроля доступа к ресурсам компьютерных систем.
19. Способы фиксации факта доступа.
20. Структура и функции подсистемы контроля доступа программ и пользователей.
21. Средства активного аудита компьютерных систем.
22. Идентификация и аутентификация субъектов и объектов компьютерных систем.
23. Идентифицирующая информация и протоколы идентификации.
24. Основные подходы к защите данных от НСД.
25. Иерархический доступ к файлу.
26. Доступ к данным со стороны процесса.
27. Понятие скрытого доступа.
28. Модели управления доступом.
29. Дискреционная (избирательная) и мандатная (полномочная) модель управления доступом.
30. Защита алгоритма шифрования и программно-аппаратные средства шифрования.
31. Построение аппаратных компонент криптозащиты данных.
32. Сущность разрушающих программных средств.
33. Взаимодействие прикладных программ и программы злоумышленника.
34. Классификация разрушающих программных средств и их воздействий.
35. Компьютерные вирусы (КВ) как класс разрушающих программных воздействий.
36. Сущность, проявление, классификация КВ.
37. Необходимые и достаточные условия недопущения разрушающих программных воздействий.
38. Понятие изолированной программной среды.
39. Организационные средства защиты от КВ.
40. Роль морально-этических факторов в устранении угрозы разрушающих программных воздействий.

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. ЛАПТЕВ В. Н. Информационная безопасность: метод. указания / ЛАПТЕВ В. Н., Мельников А. Б., Снимщикова С. В.. - Краснодар: КубГАУ, 2020. - 25 с. - Текст: электронный. // : [сайт]. - URL: https://edu.kubsau.ru/mod/resource/view.php?id=7965 (дата обращения: 12.05.2026). - Режим доступа: по подписке

2. ИНФОРМАЦИОННАЯ безопасность: учеб. пособие / Краснодар: КубГАУ, 2020. - 331 с. - 978-5-907346-50-5. - Текст: непосредственный.

Дополнительная литература

1. Вестник РГГУ. Серия "Информатика. Информационная безопасность. Математика", 2020, № 3: научный журнал / Москва: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Российский государственный гуманитарный университет", 2020. - 106 с. - Текст: электронный // Общество с ограниченной ответственностью «ЗНАНИУМ»: [сайт]. - URL: https://znanium.com/cover/1248/1248679.jpg (дата обращения: 08.09.2025). - Режим доступа: по подписке

2. Вестник РГГУ. Серия "Информатика. Информационная безопасность. Математика", 2020, № 1: научный журнал / Москва: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Российский государственный гуманитарный университет", 2020. - 121 с. - Текст: электронный // Общество с ограниченной ответственностью «ЗНАНИУМ»: [сайт]. - URL: https://znanium.com/cover/1224/1224798.jpg (дата обращения: 08.09.2025). - Режим доступа: по подписке

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

Профессиональные базы данных

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

Ресурсы «Интернет»

1. https://edu.kubsau.ru/ - Образовательный портал КубГАУ

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.

Компьютерный класс
101эк
- CTS-ENM101W01 - 1 шт.
- CTS-ENM101W02 - 1 шт.
- CTS-ENM101W03 - 1 шт.
- CTS-ENM101W04 - 1 шт.
- CTS-ENM101W05 - 1 шт.
- CTS-ENM101W06 - 1 шт.
- CTS-ENM101W07 - 1 шт.
- CTS-ENM101W08 - 1 шт.
- CTS-ENM101W09 - 1 шт.
- CTS-ENM101W10 - 1 шт.
- CTS-ENM101W11 - 1 шт.
- CTS-ENM101W12 - 1 шт.
- CTS-ENM101W13 - 1 шт.
- CTS-ENM101W14 - 1 шт.
- CTS-ENM101W15 - 1 шт.
- CTS-ENM101W16 - 1 шт.
- CTS-ENM101W17 - 1 шт.
- CTS-ENM101W18 - 1 шт.
- CTS-ENM101W19 - 1 шт.
- CTS-ENM101W20 - 1 шт.
- CTS-ENM101W21 - 1 шт.
- CTS-ENM101W22 - 1 шт.
- CTS-ENM101W23 - 1 шт.
- CTS-ENM101W24 - 1 шт.
- электронная доска 101 - 1 шт.

103эк
- CTS-ENM103W01 - 1 шт.
- CTS-ENM103W02 - 1 шт.
- CTS-ENM103W03 - 1 шт.
- CTS-ENM103W04 - 1 шт.
- CTS-ENM103W05 - 1 шт.
- CTS-ENM103W06 - 1 шт.
- CTS-ENM103W07 - 1 шт.
- CTS-ENM103W08 - 1 шт.
- CTS-ENM103W09 - 1 шт.
- CTS-ENM103W10 - 1 шт.
- CTS-ENM103W11 - 1 шт.
- CTS-ENM103W12 - 1 шт.
- CTS-ENM103W13 - 1 шт.
- CTS-ENM103W14 - 1 шт.
- CTS-ENM103W15 - 1 шт.

CTS-ENM103W16 - 1 шт.
CTS-ENM103W17 - 1 шт.
CTS-ENM103W18 - 1 шт.
CTS-ENM103W19 - 1 шт.
CTS-ENM103W20 - 1 шт.
CTS-ENM103W21 - 1 шт.
CTS-ENM103W22 - 1 шт.
CTS-ENM103W23 - 1 шт.
CTS-ENM103W24 - 1 шт.
Маркерная доска 103 - 1 шт.

108эк

CTS-ENM108W01 - 1 шт.
CTS-ENM108W02 - 1 шт.
CTS-ENM108W03 - 1 шт.
CTS-ENM108W04 - 1 шт.
CTS-ENM108W05 - 1 шт.
CTS-ENM108W06 - 1 шт.
CTS-ENM108W07 - 1 шт.
CTS-ENM108W08 - 1 шт.
CTS-ENM108W09 - 1 шт.
CTS-ENM108W10 - 1 шт.
CTS-ENM108W11 - 1 шт.
CTS-ENM108W12 - 1 шт.
CTS-ENM108W13 - 1 шт.
CTS-ENM108W14 - 1 шт.
CTS-ENM108W15 - 1 шт.
CTS-ENM108W16 - 1 шт.
CTS-ENM108W17 - 1 шт.
CTS-ENM108W18 - 1 шт.
CTS-ENM108W19 - 1 шт.
CTS-ENM108W20 - 1 шт.
CTS-ENM108W21 - 1 шт.
CTS-ENM108W22 - 1 шт.
CTS-ENM108W23 - 1 шт.
CTS-ENM108W24 - 1 шт.
CTS-ENM108W25 - 1 шт.
CTS-ENM108W26 - 1 шт.
Маркерная доска 108 - 1 шт.

Лекционный зал

403эк

CTS-ENM403W01 - 1 шт.
Маркерная доска 403 - 1 шт.
Электронная доска 403 - 1 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.

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)