Автономная некоммерческая образовательная организация
высшего образования
«Воронежский экономико-правовой институт»
(АНОО ВО «ВЭПИ»)

АНОО ВО "ВОРОНЕЖСКИЙ ЭКОНОМИКО-ПРАВОВОЙ ИНСТИТУТ", АНОО ВО "ВЭПИ", ВЭПИ

Подписано цифровой подписью: АНОО ВО "ВОРОНЕЖСКИЙ ЭКОНОМИКО-ПРАВОВОЙ ИНСТИТУТ", АНОО ВО "ВЭПИ", ВЭПИ
Дата: 01.09.2026 11:18:25 +03'00'

УТВЕРЖДАЮ
Проректор
по учебно-методической работе
_____ А.Ю. Жильников
15 октября 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.15 Информационная безопасность
(наименование дисциплины (модуля)

27.03.05 Инноватика
(код и наименование направления подготовки)

Направленность (профиль) Инновационные технологии
(наименование направленности (профиля))

Квалификация выпускника Бакалавр
(наименование квалификации)

Форма обучения Очная, заочная
(очная, заочная)

Рекомендована к использованию Филиалами АНОО ВО «ВЭПИ»

Воронеж 2025

Рабочая программа дисциплины (модуля) разработана в соответствии с требованиями ФГОС ВО, утвержденного приказом Минобрнауки России от 31.07.2020 № 870 (ред. от 27.02.2023), учебным планом по направлению подготовки 27.03.05 Инноватика, направленность (профиль) «Инновационные технологии».

Рабочая программа рассмотрена и одобрена на заседании кафедры прикладной информатики.

Протокол от «08» октября 2025 г. № 2

Заведующий кафедрой  М.С. Агафонова

Разработчики:

Ст. преподаватель  Д.В. Байбеков

1. Цель освоения дисциплины (модуля)

Целью освоения дисциплины (модуля) «Информационная безопасность» является формирование у обучающихся теоретических знаний и практических навыков в области информационной безопасности, изучение основных принципов, методов и средств защиты информации в информационных системах.

2. Место дисциплины (модуля) в структуре образовательной программы высшего образования – программы бакалавриата

Дисциплина «Информационная безопасность» относится к обязательной части Блока 1 «Дисциплины (модули)».

Для освоения данной дисциплины необходимы результаты обучения, полученные в предшествующих дисциплинах (модулях) и практиках: «Теория алгоритмов», «Безопасность жизнедеятельности».

Перечень последующих дисциплин (модулей) и практик, для которых необходимы результаты обучения, полученные в данной дисциплине: «Методы оптимальных решений в инновационных процессах», «Выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с установленными в образовательной программе высшего образования – программе бакалавриата индикаторами достижения компетенций

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)
УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	**ИУК 8.1** Выявляет возможные угрозы для жизни и здоровья в повседневной и профессиональной деятельности	Знать: перечень возможных угроз для жизни и здоровья в повседневной и профессиональной деятельности, и методы защиты человека и среды жизнедеятельности от опасностей природного и техногенного характера Уметь: контролировать соблюдение требований безопасности, охраны окружающей среды в повседневной жизни, на производстве, включая действия в условиях чрезвычайных ситуаций Владеть: навыками организации оказания первой медицинской помощи
	ИУК 8.2 Контролирует соблюдение требований безопасности, окружающей среды в повседневной жизни и на производстве	
	ИУК 8.3 Выбирает методы защиты человека и среды жизнедеятельности от опасностей природного и техногенного характера, применяет навыки поддержания безопасных условий жизнедеятельности	
ПК-3**.** Способен применять современные методы исследования и моделирования проекта с	**ИПК 3.1** Применяет современные методы исследования и моделирования с использованием	Знать: стандартные методы криптографии; основные направления развития цифровых

использованием информационных технологий и соответствующих программных комплексов	информационных технологий	финансовых инструментов, а также методы их разработки Уметь: выбирать методику использования криптовалют в соответствии с областью деятельности Владеть: разработкой методов оценки динамики и рисков криптовалют
	ИПК 3.2 Находит соответствующие программные комплексы для реализации конкретного проекта	Знать: теорию исследования операций; основы информационных технологий моделирования процессов Уметь: анализировать результаты технологических исследований в рамках проекта и разрабатывать мероприятия по оптимизации процессов Владеть: навыками постановки задач на технологические исследования в рамках инновационного проекта; навыками использования информационных технологий моделирования технологических процессов
ПК-6**.** Способен осуществлять поиск, отбор и анализ научно-технической, патентной, правовой информации, проводить инвентаризацию созданных результатов интеллектуальной деятельности, средств индивидуализации и использовать комплект документов по проекту	**ИПК 6.1** Использует актуальную научно-техническую, патентную и правовую информацию по проекту	Знать: особенности обеспечения надежности функционирования систем информационного обеспечения в этой области; классификацию интеллектуальной собственности; систему правовой охраны и управления интеллектуальной собственностью; возможности наличия правовой охраны; правовые основы охраны товарных знаков, знаков обслуживания, фирменных наименований, наименований мест происхождения товара; основы правовой охраны служебной и коммерческой тайны и ноу-хау; государственный стандарт в области патентных исследований; средства и методы патентного поиска; порядок проведения патентного поиска и анализа; правила построения и анализа патентных ландшафтов Уметь: грамотно обосновывать наличие правовой охраны и ее возможности; проводить информационно-аналитический поиск с использованием научных публикаций, новостных лент институтов развития, материалов выставок-ярмарок, аналитических и прогнозных докладов, патентных справочных систем (баз данных); Владеть: терминологией в области патентно-лицензионной

		деятельности; проведение патентного поиска по актуальным направлениям развития науки, техники и технологий в Российской Федерации и за рубежом, входящим в сферу отраслевой специализации организации; построение патентных ландшафтов с целью выявления технологических направлений развития
	ИПК 6.2.Осуществляет инвентаризацию созданных результатов интеллектуальной деятельности	Знать: основные понятия, термины и определения в области управления качеством; методологические основы организации измерений и контроля качества; законодательные и нормативные правовые акты по управлению качеством; организацию и технологию подтверждения соответствия продукции процессов и услуг; физические основы измерений; правила проведения испытаний и приемки продукции Уметь: разработать систему менеджмента в организации; рассчитывать по метрологическим характеристикам средств измерений погрешности прямых и косвенных измерений; разрабатывать структуру системы качества на предприятии применительно к производству конкретного вида строительных материалов, изделий и конструкций; использовать компьютерные технологии для планирования и проведения работ; подготовить документы для сертификации системы качества по стандартам ГОСТ Р ИСО 9000; анализировать данные о качестве продукции и определять причины брака. Владеть: умением грамотно использовать измерительные средства и системы при необходимости; способами оценки по результатам эксперимента статистических оценок результатов измерений и контроля качества; навыками оформления результатов испытаний и принятия соответствующих решений; навыками оформления

		нормативно-технической документации; навыками проведения аудита

4. Структура и содержание дисциплины (модуля)

4.1. Структура дисциплины (модуля)

4.1.1. Объем дисциплины (модуля) и виды учебной работы по очной форме обучения:

Вид учебной работы		Всего часов	Семестр	
			№5	№ 6
			часов	часов
Контактная работа (всего):		140	68	72
В том числе: Лекции (Л)		70	34	36
Практические занятия (Пр)		70	34	36
Лабораторная работа (Лаб)		-	-	-
Самостоятельная работа обучающихся (СР)		103	40	63
Промежуточная аттестация	Форма промежуточной аттестации	За., Эк.	За	Эк
	Количество часов	45	-	45
Общая трудоемкость дисциплины (модуля)	Часы	288	108	180
	Зачетные единицы	8	3	5

4.1.2. Объем дисциплины (модуля) и виды учебной работы по заочной форме обучения:

Вид учебной работы		Всего часов	Курс
			№ 4
			часов
Контактная работа (всего):		36	36
В том числе: Лекции (Л)		18	18
Практические занятия (Пр)		18	18
Лабораторная работа (Лаб)		-	-
Самостоятельная работа обучающихся (СР)		239	239
Промежуточная аттестация	Форма промежуточной аттестации	За, Эк	За, Эк
	Количество часов	13	13
Общая трудоемкость дисциплины (модуля)	Часы	288	288
	Зачетные единицы	8	8

4.2. Содержание дисциплины (модуля)

4.2.1. Содержание дисциплины (модуля) по очной форме обучения

Наименование раздела, темы	Код компетенции, код индикатора достижения компетенции	Количество часов, выделяемых на контактную работу, по видам учебных занятий			Кол-во часов СР	Виды СР	Контроль
		Л	Пр	Лаб			
Тема 1. Проблема обеспечения ИБ. Основные понятия	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	7	6	-	11	Сбор, обработка и систематизация информации	сообщение
Тема 2. Угрозы ИБ	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	7	6	-	11	Анализ используемого материала. Разработка плана доклада	доклад
Тема 3. Основы теории ИБ	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	7	6	-	11	Анализ используемого материала. Разработка плана доклада	опрос

Наименование раздела, темы	Код компетенции, код индикатора достижения компетенции	Количество часов, выделяемых на контактную работу, по видам учебных занятий			Кол-во часов СР	Виды СР	Контроль
		Л	Пр	Лаб			
Тема 4. Оценка эффективности систем защиты информации	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	7	6	-	10	Сбор, обработка и систематизация информации	сообщение
Тема 5. Нормативные руководящие документы в сфере обеспечения ИБ	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	7	6	-	10	Анализ используемого материала. Разработка плана доклада	доклад
Тема 6. Программно-технические средства обеспечения ИБ	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	7	6	-	10	Анализ проведенного исследования	опрос
Тема 7. Межсетевые экраны	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	7	6	-	10	Сбор, обработка и систематизация информации	сообщение

Наименование раздела, темы	Код компетенции, код индикатора достижения компетенции	Количество часов, выделяемых на контактную работу, по видам учебных занятий			Кол-во часов СР	Виды СР	Контроль
		Л	Пр	Лаб			
Тема 8. Борьба с компьютерными вирусами	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	7	7	-	10	Сбор, обработка и систематизация информации	сообщение
Тема 9. Криптографические методы	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	7	7	-	10	Анализ используемого материала. Разработка плана доклада	доклад
Тема 10. Построение защищённых виртуальных сетей	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	7	7	-	10	Анализ используемого материала. Разработка плана доклада	опрос
Обобщающее занятие	-	-	7	-	-	-	зачет с оценкой
ВСЕГО ЧАСОВ:		70	34	-	103		

Тема 1. Проблема обеспечения ИБ. Основные понятия – 22 ч.

Лекции – 7 ч. Содержание: Основные понятия ИБ. Информация, защищаемая информация, ценность информации, уровень секретности. Объекты защиты информации. Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.

Практические занятия – 6 ч.

Вопросы:

1. Объекты защиты информации.

2. Информация, защищаемая информация, ценность информации, уровень секретности.

Темы докладов и научных сообщений:

1. Основные понятия ИБ.

2. Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.

Тема 2. Угрозы ИБ - 22 ч.

Лекции – 7 ч. Содержание: Классификация угроз безопасности: каналы утечки, воздействия. Прямые и косвенные каналы утечки данных.

Практические занятия – 6 ч.

Вопросы:

1. Каналы утечки

2. Косвенные каналы утечки данных.

Темы докладов и научных сообщений:

1. Классификация угроз безопасности.

2. Прямые и косвенные каналы утечки данных.

Тема 3. Основы теории ИБ - 22 ч.

Лекции – 7 ч. Содержание: Модель потенциального нарушителя. Способы мошенничества в информационных системах. Основные способы реализации угроз ИБ. Основные понятия теории ИБ.

Практические занятия – 6 ч.

Вопросы:

1. Модель потенциального нарушителя.

2. Способы мошенничества в информационных системах.

Тема 4. Оценка эффективности систем защиты информации - 21 ч.

Лекции – 7 ч. Содержание: Принципы организации систем обеспечения безопасности данных.

Требования, предъявляемые к системам обеспечения безопасности данных. Понятие мониторов безопасности. Физические средства защиты информации

Практические занятия – 6 ч.
Вопросы:
1. Понятие мониторов безопасности.
2. Физические средства защиты информации

Темы докладов и научных сообщений:
1. Принципы организации систем обеспечения безопасности данных.
2. Требования, предъявляемые к системам обеспечения безопасности данных.

Тема 5. Нормативные руководящие документы в сфере обеспечения ИБ - 21 ч.

Лекции – 7 ч. Содержание: Понятие политики безопасности. Дискреционные политики безопасности. Мандатные политики безопасности Модель безопасности информационных потоков. Показатели эффективности систем защиты информации. Способы оценки эффективности систем защиты информации. Руководящие документы Гостехкомиссии в сфере обеспечения ИБ.

Практические занятия – 6 ч.
Вопросы:
1. Дискреционные политики безопасности.
2. Способы оценки эффективности систем защиты информации.

Темы докладов и научных сообщений:
1. Понятие политики безопасности.
2. Гостехкомиссии в сфере обеспечения ИБ.

Тема 6. Программно-технические средства обеспечения ИБ – 21 ч.

Лекции – 7 ч. Содержание: Основные понятия теории ИБ. Принципы организации систем обеспечения безопасности данных. Требования, предъявляемые к системам обеспечения безопасности данных. Понятие мониторов безопасности. Физические средства защиты информации

Практические занятия – 6 ч.
Вопросы:
1. Принципы организации систем обеспечения безопасности данных.
2. Понятие мониторов безопасности.

Тема 7. Межсетевые экраны – 21 ч.

Лекции – 7 ч. Содержание: Руководящие документы Гостехкомиссии в

сфере обеспечения ИБ. «Общие критерии». Структура. Основные понятия. Программно-технические средства обеспечения ИБ. Межсетевые экраны.

Практические занятия – 6 ч.
Вопросы:
1. Гостехкомиссии в сфере обеспечения ИБ.
2. Программно-технические средства обеспечения ИБ.

Темы докладов и научных сообщений:
1. Руководящие документы Гостехкомиссии в сфере обеспечения ИБ.
2. Межсетевые экраны.

Тема 8. Борьба с компьютерными вирусами - 24 ч.

Лекции – 7 ч. Содержание: Типы компьютерных вирусов. Методы борьбы с компьютерными вирусами.

Практические занятия – 7 ч.
Вопросы:
1. Компьютерные вирусы
2. Борьба с вирусами

Темы докладов и научных сообщений:
1. Типы компьютерных вирусов.
2. Методы борьбы с компьютерными вирусами.

Тема 9. Криптографические методы - 24 ч.

Лекции – 7 ч. Содержание: Федеральный стандарт США на шифрование данных (стандарт DES). Отечественный стандарт на шифрование данных. Шифрование с открытым ключом, алгоритм RSA.

Практические занятия – 7 ч.
Вопросы:
1. Отечественный стандарт на шифрование данных.
2. Алгоритм RSA.

Темы докладов и научных сообщений:
1. Федеральный стандарт США на шифрование данных (стандарт DES).
2. Шифрование с открытым ключом, алгоритм RSA.

Тема 10. Построение защищённых виртуальных сетей - 24 ч.

Лекции – 7 ч. Содержание: Понятие, назначение и основные функции

защищённой виртуальной сети. Средства построения защищённой виртуальной сети. Туннелирование в протоколах различных уровней.

Практические занятия – 7 ч.

Вопросы:

1. Средства построения защищённой виртуальной сети.
2. Туннелирование в протоколах различных уровней.

4.2.2. Содержание дисциплины (модуля) по заочной форме обучения

Наименование раздела, темы	Код компетенции, код индикатора достижения компетенции	Количество часов, выделяемых на контактную работу, по видам учебных занятий			Кол-во часов СР	Виды СР	Контроль
		Л	Пр	Лаб			
Тема 1. Проблема обеспечения ИБ. Основные понятия	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	1	1	-	23	Сбор, обработка и систематизация информации	сообщение
Тема 2. Угрозы ИБ	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	1	1	-	24	Анализ используемого материала. Разработка плана доклада	доклад
Тема 3. Основы теории ИБ	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	2	2	-	24	Анализ используемого материала. Разработка плана доклада	опрос

Наименование раздела, темы	Код компетенции, код индикатора достижения компетенции	Количество часов, выделяемых на контактную работу, по видам учебных занятий			Кол-во часов СР	Виды СР	Контроль
		Л	Пр	Лаб			
Тема 4. Оценка эффективности систем защиты информации	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	2	2	-	24	Сбор, обработка и систематизация информации	сообщение
Тема 5. Нормативные руководящие документы в сфере обеспечения ИБ	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	2	2	-	24	Анализ используемого материала. Разработка плана доклада	доклад
Тема 6. Программно-технические средства обеспечения ИБ	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	2	2	-	24	Анализ проведенного исследования	опрос
Тема 7. Межсетевые экраны	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	2	2	-	24	Сбор, обработка и систематизация информации	сообщение

Наименование раздела, темы	Код компетенции, код индикатора достижения компетенции	Количество часов, выделяемых на контактную работу, по видам учебных занятий			Кол-во часов СР	Виды СР	Контроль
		Л	Пр	Лаб			
Тема 8. Борьба с компьютерными вирусами	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	2	2	-	24	Сбор, обработка и систематизация информации	сообщение
Тема 9. Криптографические методы	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	2	2	-	24	Анализ используемого материала. Разработка плана доклада	доклад
Тема 10. Построение защищённых виртуальных сетей	УК-8 (ИУК-8.1, ИУК-8.2, ИУК-8.3.) ПК-3 (ИПК-3.1, ИПК-3.2.) ПК-6 (ИПК-6.1, ИПК-6.2.)	2	2	-	24	Анализ используемого материала. Разработка плана доклада	опрос
ВСЕГО ЧАСОВ:		18	18	-	239		

Тема 1. Проблема обеспечения ИБ. Основные понятия – 25 ч.

Лекции – 1 ч. Содержание: Основные понятия ИБ. Информация, защищаемая информация, ценность информации, уровень секретности. Объекты защиты информации. Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.

Практические занятия – 1 ч.

Вопросы:

1. Объекты защиты информации.

2. Информация, защищаемая информация, ценность информации, уровень секретности.

Темы докладов и научных сообщений:

1. Основные понятия ИБ.

2. Угрозы безопасности информации, основные понятия: безопасность, конфиденциальность, целостность, доступность, утечка информации; несанкционированный доступ к информации.

Тема 2. Угрозы ИБ - 26 ч.

Лекции – 1 ч. Содержание: Классификация угроз безопасности: каналы утечки, воздействия. Прямые и косвенные каналы утечки данных.

Практические занятия – 1 ч.

Вопросы:

1. Каналы утечки

2. Косвенные каналы утечки данных.

Темы докладов и научных сообщений:

1. Классификация угроз безопасности.

2. Прямые и косвенные каналы утечки данных.

Тема 3. Основы теории ИБ – 28 ч.

Лекции – 2 ч. Содержание: Модель потенциального нарушителя. Способы мошенничества в информационных системах. Основные способы реализации угроз ИБ. Основные понятия теории ИБ.

Практические занятия – 2 ч.

Вопросы:

1. Модель потенциального нарушителя.

2. Способы мошенничества в информационных системах.

Тема 4. Оценка эффективности систем защиты информации - 28 ч.

Лекции – 2 ч. Содержание: Принципы организации систем обеспечения безопасности данных.

Требования, предъявляемые к системам обеспечения безопасности данных. Понятие мониторов безопасности. Физические средства защиты информации

Практические занятия – 2 ч.

Вопросы:

1. Понятие мониторов безопасности.

2. Физические средства защиты информации

Темы докладов и научных сообщений:

1. Принципы организации систем обеспечения безопасности данных.

2. Требования, предъявляемые к системам обеспечения безопасности данных.

Тема 5. Нормативные руководящие документы в сфере обеспечения ИБ - 28 ч.

Лекции – 2 ч. Содержание: Понятие политики безопасности. Дискреционные политики безопасности. Мандатные политики безопасности Модель безопасности информационных потоков. Показатели эффективности систем защиты информации. Способы оценки эффективности систем защиты информации. Руководящие документы Гостехкомиссии в сфере обеспечения ИБ.

Практические занятия – 2 ч.

Вопросы:

1. Дискреционные политики безопасности.

2. Способы оценки эффективности систем защиты информации.

Темы докладов и научных сообщений:

1. Понятие политики безопасности.

2. Гостехкомиссии в сфере обеспечения ИБ.

Тема 6. Программно-технические средства обеспечения ИБ - 28 ч.

Лекции – 2ч. Содержание: Основные понятия теории ИБ. Принципы организации систем обеспечения безопасности данных. Требования, предъявляемые к системам обеспечения безопасности данных. Понятие мониторов безопасности. Физические средства защиты информации

Практические занятия – 2 ч.

Вопросы:

1. Принципы организации систем обеспечения безопасности данных.

2. Понятие мониторов безопасности.

Тема 7. Межсетевые экраны - 28 ч.

Лекции – 28 ч. Содержание: Руководящие документы Гостехкомиссии в сфере обеспечения ИБ. «Общие критерии». Структура. Основные понятия. Программно-технические средства обеспечения ИБ. Межсетевые экраны.

Практические занятия – 2 ч.

Вопросы:

1. Гостехкомиссии в сфере обеспечения ИБ.
2. Программно-технические средства обеспечения ИБ.

Темы докладов и научных сообщений:
1. Руководящие документы Гостехкомиссии в сфере обеспечения ИБ.
2. Межсетевые экраны.

Тема 8. Борьба с компьютерными вирусами - 28 ч.

Лекции – 2 ч. Содержание: Типы компьютерных вирусов. Методы борьбы с компьютерными вирусами.

Практические занятия – 2 ч.
Вопросы:
1. Компьютерные вирусы
2. Борьба с вирусами

Темы докладов и научных сообщений:
1. Типы компьютерных вирусов.
2. Методы борьбы с компьютерными вирусами.

Тема 9. Криптографические методы - 28 ч.

Лекции – 2 ч. Содержание: Федеральный стандарт США на шифрование данных (стандарт DES). Отечественный стандарт на шифрование данных. Шифрование с открытым ключом, алгоритм RSA.
Практические занятия – 2 ч.
Вопросы:
1. Отечественный стандарт на шифрование данных.
2. Алгоритм RSA.

Темы докладов и научных сообщений:
1. Федеральный стандарт США на шифрование данных (стандарт DES).
2. Шифрование с открытым ключом, алгоритм RSA.

Тема 10. Построение защищённых виртуальных сетей - 28 ч.

Лекции – 2 ч. Содержание: Понятие, назначение и основные функции защищённой виртуальной сети. Средства построения защищённой виртуальной сети. Туннелирование в протоколах различных уровней.

Практические занятия – 2 ч.
Вопросы:
1. Средства построения защищённой виртуальной сети.

2. Туннелирование в протоколах различных уровней.

5. Оценочные материалы дисциплины (модуля)

Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю) представлены в виде фонда оценочных средств по дисциплине (модулю).

6. Методические материалы для освоения дисциплины (модуля)

Методические материалы для освоения дисциплины (модуля) представлены в виде учебно-методического комплекса дисциплины (модуля).

7. Перечень учебных изданий, необходимых для освоения дисциплины (модуля)

№ п/п	Библиографическое описание учебного издания	Используется при изучении разделов (тем)	Режим доступа
1.	Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2025. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт].	Тема 1-10	https://urait.ru/bcode/562070
2.	Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт].	Тема 1-10	https://urait.ru/bcode/560516
3.	Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов /	Тема 1-10	https://urait.ru/bcode/580669

	О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 352 с. — (Высшее образование). — ISBN 978-5-534-19386-2. — Текст : электронный // Образовательная платформа Юрайт [сайт].		

8. Перечень электронных образовательных ресурсов, современных профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины (модуля)

8.1. Электронные образовательные ресурсы:

№ п/п	Наименование	Гиперссылка
1.	Министерства науки и высшего образования Российской Федерации:	https://minobrnauki.gov.ru
2.	Министерство просвещения Российской Федерации:	https://edu.gov.ru
3.	Федеральная служба по надзору в сфере образования и науки:	http://obrnadzor.gov.ru/ru/
4.	Федеральный портал «Российское образование»:	http://www.edu.ru/.
5.	Электронно-библиотечная система «Знаниум»:	https://znanium.ru/
6.	Электронная библиотечная система Юрайт:	https://urait.ru/

8.2. Современные профессиональные базы данных и информационные справочные системы:

№ п/п	Наименование	Гиперссылка (при наличии)
1	Информационная система «Единое окно доступа к образовательным ресурсам». Раздел «Математика»:	http://window.edu.ru/catalog/resources?p_rubr=2.2.74.12
2	Общероссийский математический портал (информационная система)	http://www.mathnet.ru/
3	Справочно-правовая система «КонсультантПлюс»	https://www.consultant.ru/edu/

4	Справочно-правовая система «Гарант»	https://study.garant.ru/

9. Материально-техническое обеспечение дисциплины (модуля)

№ п/п	Наименование помещения	Перечень оборудования и технических средств обучения	Состав комплекта лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства
1	334 Аудитория для самостоятельной работы обучающихся	Персональные компьютеры с доступом к сети Интернет, компьютерные столы, стулья	1. 1С: Предприятие 8 - Сублицензионный договор от 02.07.2020 № ЮС-2020-00731; 2. Справочно-правовая система «КонсультантПлюс» - Договор от 17.05.2023 № 96-2023/RDD; 3. СК Гарант-Сервис - Договор от 05.12.2025 № Л6030/01/26; 4. MicrosoftOffice - Сублицензионный договор от 12.01.2017 № Вж_ПО_123015- 2017. Лицензия OfficeStd 2016 RUS OLP NL Acdmc; 5. Антивирус Dr.Web Desktop Security Suite - Лицензионный договор № 1080_S0448L о предоставлении прав на использование программ для ЭВМ от 13.07.2026 г.; 6. LibreOffice – Свободно распространяемое программное обеспечение; 7. 7-Zip – Свободно распространяемое программное обеспечение отечественного производства; 8. Электронно-библиотечная система «Юрайт»: Лицензионный договор № 7297 от 04.07.2025 (подписка 01.09.2025-31.08.2028) 9. Электронно-

№ п/п	Наименование помещения	Перечень оборудования и технических средств обучения	Состав комплекта лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства
			библиотечная система «Знаниум»: Лицензионный договор № 697эбс от 17.07.2024 (Основная коллекция ЭБС) (подписка 01.09.2024-31.08.2027)
2	243 Учебная аудитория для проведения учебных занятий	Мебель ученическая (столы, стулья), доска для письма мелом, баннеры, трибуна для выступлений, персональные компьютеры с доступом к сети Интернет, наушники, веб-камера	1. 1С: Предприятие 8 - Сублицензионный договор от 02.07.2020 № ЮС-2020-00731; 2. Справочно-правовая система «КонсультантПлюс» - Договор от 17.05.2023 № 96-2023/RDD; 3. СК Гарант-Сервис - Договор от 05.12.2025 № Л6030/01/26; 4. MicrosoftOffice - Сублицензионный договор от 12.01.2017 № Вж_ПО_123015- 2017. Лицензия OfficeStd 2016 RUS OLP NL Acdmc; 5. Антивирус Dr.Web Desktop Security Suite - Лицензионный договор № 1080_S0448L о предоставлении прав на использование программ для ЭВМ от 13.07.2026 г.; 6. LibreOffice – Свободно распространяемое программное обеспечение; 7. 7-Zip – Свободно распространяемое программное обеспечение отечественного производства; 8. Электронно-библиотечная система «Юрайт»: Лицензионный договор № 7297 от 04.07.2025 (подписка 01.09.2025-31.08.2028) 9. Электронно-

№ п/п	Наименование помещения	Перечень оборудования и технических средств обучения	Состав комплекта лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства
			библиотечная система «Знаниум»: Лицензионный договор № 697эбс от 17.07.2024 (Основная коллекция ЭБС) (подписка 01.09.2024-31.08.2027)
3	321 Учебная аудитория для проведения учебных занятий	Рабочее место преподавателя (стол, стул); мебель ученическая; доска для письма мелом; баннеры; трибуна для выступлений; персональный компьютер; колонки, веб-камера	1. 1С: Предприятие 8 - Сублицензионный договор от 02.07.2020 № ЮС-2020-00731; 2. Справочно-правовая система «КонсультантПлюс» - Договор от 17.05.2023 № 96-2023/RDD; 3. СК Гарант-Сервис - Договор от 05.12.2025 № Л6030/01/26; 4. MicrosoftOffice - Сублицензионный договор от 12.01.2017 № Вж_ПО_123015- 2017. Лицензия OfficeStd 2016 RUS OLP NL Acdmc; 5. Антивирус Dr.Web Desktop Security Suite - Лицензионный договор № 1080_S0448L о предоставлении прав на использование программ для ЭВМ от 13.07.2026 г.; 6. LibreOffice – Свободно распространяемое программное обеспечение; 7. 7-Zip – Свободно распространяемое программное обеспечение отечественного производства; 8. Электронно-библиотечная система «Юрайт»: Лицензионный договор № 7297 от 04.07.2025 (подписка 01.09.2025-31.08.2028) 9. Электронно-

№ п/п	Наименование помещения	Перечень оборудования и технических средств обучения	Состав комплекта лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства
			библиотечная система «Знаниум»: Лицензионный договор № 697эбс от 17.07.2024 (Основная коллекция ЭБС) (подписка 01.09.2024-31.08.2027)

Лист регистрации изменений к рабочей программе дисциплины (модуля)

№ п/п	Дата внесения изменений	Номера измененных листов	Документ, на основании которого внесены изменения	Содержание изменений	Подпись разработчика рабочей программы
1	01.09.2026	21-26	Федеральный государственный образовательный стандарт высшего образования-бакалавриат по направлению подготовки 27.03.05 Инноватика: приказ Минобрнауки РФ от 31.07.2020 № 870 (ред. от 27.02.2023) Пункт 4.3.2, 4.3.4 ООО "Электронное издательство ЮРАЙТ" - АНОО ВО "ВЭПИ". Договор на оказание услуг по предоставлению доступа к образовательной платформе № 7297 от 04.07.2025. ООО «ЗНАНИУМ» - АНОО ВО "ВЭПИ". Договор на оказание услуг по предоставлению доступа к ЭБС Знаниум № 697эбс от 17.07.2024.	Обновление профессиональных баз данных и информационных справочных систем, комплекта лицензионного программного обеспечения. Актуализация литературы