

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Косенок Сергей Михайлович
Должность: ректор
Дата подписания: 22.06.2026 12:40:23
Уникальный программный ключ:
e3a68f3eaa1e62674b54f4998099d3d6bfdcf836

Балтийский университет высшего образования
Ханты-Мансийского автономного округа-Югры
"Сургутский государственный университет"

УТВЕРЖДАЮ
Проректор по УМР

_____ Е.В. Коновалова

11 июня 2026 г., протокол УМС №5

Методы защиты

рабочая программа дисциплины (модуля)

Закреплена за кафедрой	Информатики и вычислительной техники		
Учебный план	b090302-ИнфСист-26-4.plx 09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ Направленность (профиль): Информационные системы и технологии		
Квалификация	Бакалавр		
Форма обучения	очная		
Общая трудоемкость	3 ЗЕТ		
Часов по учебному плану	108	Виды контроля в семестрах:	
в том числе:		зачет 7	
аудиторные занятия	32	контрольная работа 7	
самостоятельная работа	76		

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	7 (4.1)		Итого	
	Неделя 17 2/6			
Вид занятий	уп	рп	уп	рп
Лекции	16	16	16	16
Лабораторные	16	16	16	16
Итого ауд.	32	32	32	32
Контактная работа	32	32	32	32
Сам. работа	76	76	76	76
Итого	108	108	108	108

Программу составил(и):

Старший преподаватель, Еловой Сергей Григорьевич

Рабочая программа дисциплины

Методы защиты

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.02 Информационные системы и технологии (приказ Минобрнауки России от 19.09.2017 г. № 926)

составлена на основании учебного плана:

09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

Направленность (профиль): Информационные системы и технологии

утвержденного учебно-методическим советом вуза от 11.06.2026 протокол № 5.

Рабочая программа одобрена на заседании кафедры

Информатики и вычислительной техники

Зав. кафедрой Лысенкова С.А.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Образовательные цели курса: формирование знаний об основных положениях теории и практики информационной безопасности; умений применять современные методы и средства защиты информации в вычислительных системах и сетях; компетенций в области разработки и использования средств защиты компьютерной информации в процессе ее обработки, передачи и хранения в информационных системах у студентов профиля подготовки – Вычислительные машины, комплексы, системы и сети.
-----	---

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:	Б1.В.ДВ.02
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Базы данных
2.1.2	Информатика
2.1.3	Основы информационной безопасности
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Подготовка к сдаче и сдача государственного экзамена
2.2.2	Производственная практика, преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-4.1: Демонстрирует знания методов и технологий обеспечения функционирования баз данных

ПК-4.2: Разрабатывает алгоритмы предотвращения потерь и повреждений данных

ПК-4.3: Обеспечивает информационную безопасность

ПК-7.1: Демонстрирует знания методов управления программно-аппаратными средствами инфокоммуникационной системы организации

ПК-7.2: Управляет программно-аппаратными средствами инфокоммуникационной системы организации

ПК-7.3: Выполняет администрирование сетей

В результате освоения дисциплины обучающийся должен

3.1	Знать:
3.1.1	базовый перечень методов и средств защиты компьютерной информации;
3.1.2	принципы классификации и примеры угроз безопасности компьютерным системам;
3.1.3	современные отечественные и международные стандарты информационной безопасности информационных систем.
3.2	Уметь:
3.2.1	реализовывать методы криптографической защиты информации в вычислительных системах;
3.2.2	конфигурировать встроенные и дополнительные средства безопасности в операционной системе, локальных и глобальных сетях;
3.2.3	устанавливать и настраивать программное обеспечение для защиты компьютерной информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Примечание
	Раздел 1. Раздел 1					
1.1	Актуальность проблемы защиты информации. Основные факторы повышения уязвимости информации /Лек/	7	0,5	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	
1.2	Актуальность проблемы защиты информации. Основные факторы повышения уязвимости информации /Лаб/	7	0,5	ПК-4.3	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	

1.3	Актуальность проблемы защиты информации. Основные факторы повышения уязвимости информации /Ср/	7	4	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.4	Основные понятия информационной безопасности. /Лек/	7	0,5	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.5	Основные понятия информационной безопасности. /Лаб/	7	0,5	ПК-4.3	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.6	Основные понятия информационной безопасности. /Ср/	7	4	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.7	Законодательные и правовые основы защиты компьютерной информации информационных технологий. /Лек/	7	1	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.8	Законодательные и правовые основы защиты компьютерной информации информационных технологий. /Лаб/	7	1	ПК-4.3	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.9	Законодательные и правовые основы защиты компьютерной информации информационных технологий. /Ср/	7	4	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.10	Проблемы защиты информации в Базах данных. /Лек/	7	1	ПК-4.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.11	Проблемы защиты информации в Базах данных. /Лаб/	7	1	ПК-4.2 ПК-7.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.12	Проблемы защиты информации в Базах данных. /Ср/	7	4	ПК-4.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.13	Содержание системы средств защиты компьютерной информации в сети. /Лек/	7	1	ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4

1.14	Содержание системы средств защиты компьютерной информации в сети. /Лаб/	7	1	ПК-4.3 ПК-7.3	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.15	Содержание системы средств защиты компьютерной информации в сети. /Ср/	7	4	ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.16	Изучение традиционных симметричных криптосистем. /Лек/	7	1	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3 Э4
1.17	Изучение традиционных симметричных криптосистем. /Лаб/	7	1	ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.18	Изучение традиционных симметричных криптосистем. /Ср/	7	4	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.19	Применение симметричных криптосистем для защиты компьютерной информации в инфокоммуникационной системе организации. /Лек/	7	1	ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.20	Применение симметричных криптосистем для защиты компьютерной информации в инфокоммуникационной системе организации. /Лаб/	7	1	ПК-7.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.21	Применение симметричных криптосистем для защиты компьютерной информации в инфокоммуникационной системе организации. /Ср/	7	4	ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э4
1.22	Применение ассиметричных криптосистем для защиты компьютерной информации в инфокоммуникационной системе организации. /Лек/	7	1	ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.23	Применение ассиметричных криптосистем для защиты компьютерной информации в инфокоммуникационной системе организации. /Лаб/	7	1	ПК-7.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.24	Применение ассиметричных криптосистем для защиты компьютерной информации в инфокоммуникационной системе организации. /Ср/	7	4	ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4

1.25	Функции хэширования. /Лек/	7	1	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.26	Функции хэширования. /Лаб/	7	1	ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.27	Функции хэширования. /Ср/	7	4	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.28	Методы идентификации и проверки подлинности пользователей компьютерных систем. /Лек/	7	1	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.29	Методы идентификации и проверки подлинности пользователей компьютерных систем. /Лаб/	7	1	ПК-4.3 ПК-7.3	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.30	Методы идентификации и проверки подлинности пользователей компьютерных систем. /Ср/	7	4	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.31	Защита компьютерных систем от удаленных атак через сеть Internet /Лек/	7	1	ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.32	Защита компьютерных систем от удаленных атак через сеть Internet /Лаб/	7	1	ПК-4.2 ПК-4.3 ПК-7.3	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.33	Защита компьютерных систем от удаленных атак через сеть Internet /Ср/	7	3	ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.34	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). /Лек/	7	1	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.35	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). /Лаб/	7	1	ПК-4.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4

1.36	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). /Ср/	7	3	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.37	Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии. /Лек/	7	1	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.38	Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии. /Лаб/	7	1	ПК-4.2 ПК-4.3	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.39	Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии. /Ср/	7	3	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.40	Методы и средства защиты носителей информации /Лек/	7	1	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.41	Методы и средства защиты носителей информации /Лаб/	7	1	ПК-7.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.42	Методы и средства защиты носителей информации /Ср/	7	3	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.43	Защита информационных ресурсов от несанкционированного доступа. Внутримашинные средства. /Лек/	7	1	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3
1.44	Защита информационных ресурсов от несанкционированного доступа. Внутримашинные средства. /Лаб/	7	1	ПК-4.2 ПК-7.3	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.45	Защита информационных ресурсов от несанкционированного доступа. Внутримашинные средства. /Ср/	7	10	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.46	Методы и средства защиты носителей информации. /Лек/	7	1	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4

1.47	Методы и средства защиты носителей информации. /Лаб/	7	1	ПК-4.3 ПК-7.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.48	Методы и средства защиты носителей информации. /Ср/	7	4	ПК-4.1 ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.49	Основные виды атак на протоколы аутентификации. Основные приемы предотвращения атак. /Лек/	7	1	ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.50	Основные виды атак на протоколы аутентификации. Основные приемы предотвращения атак. /Лаб/	7	1	ПК-4.2 ПК-4.3	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.51	Основные виды атак на протоколы аутентификации. Основные приемы предотвращения атак. /Ср/	7	10	ПК-7.1	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4
1.52	/Зачёт/	7	0	ПК-4.1 ПК-4.2 ПК-4.3 ПК-7.1 ПК-7.2 ПК-7.3	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Оценочные материалы для текущего контроля и промежуточной аттестации

Представлены отдельным документом

5.2. Оценочные материалы для диагностического тестирования

Представлены отдельным документом

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО❖, 2017, электронный ресурс	1
Л1.2	Шаньгин В. Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2017, электронный ресурс	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Братановский С. Н., Лапин С. Ю.	Обеспечение доступа граждан к информации о деятельности органов государственной власти и местного самоуправления в Российской Федерации. Информационно-правовой аспект: Монография	Саратов: Электронно-библиотечная система IPRbooks, 2012, электронный ресурс	1

Л2.2	Гулятьева Т. А.	Основы теории информации и криптографии: Конспект лекций	Новосибирск: Новосибирский государственный технический университет, 2010, электронный ресурс	1
Л2.3	Бухтояров В. В., Золотарев В. В., Жуков В. Г.	Поддержка принятия решений при проектировании систем защиты информации: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2014, электронный ресурс	1

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Жук А. П., Жук Е. П., Лепешкин О. М., Тимошкин А. И.	Защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2015, электронный ресурс	1
Л3.2	Хорев П. Б.	Программно-аппаратная защита информации: Учебное пособие	Москва: Издательство "ФОРУМ", 2015, электронный ресурс	1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	электронный журнал Открытые системы http://www.osp.ru
Э2	сайт Информационных технологий http://inftech.webservis.ru/
Э3	интернет-издание, посвященное новостям компьютерной индустрии, науки и техники. http://www. computeIta.ru
Э4	журнал для ИТ-профессионалов http://www.bytemag.iTi/

6.3.1 Перечень программного обеспечения

6.3.1.1	Пакет прикладных программ Microsoft Office
6.3.1.2	Операционная система Windows

6.3.2 Перечень информационных справочных систем

6.3.2.1	http://www.garant.ru Информационно-правовой портал Гарант.ру
6.3.2.2	http://www.consultant.ru/ Справочно-правовая система Консультант Плюс

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	аудитория, оборудованная техническими средствами для демонстрации лекций-визуализаций;
7.2	лабораторные работы должны выполняться в специализированных классах, оснащенных современными персональными компьютерами, включенными в сеть и программным обеспечением, в соответствии с тематикой изучаемого материала;
7.3	число рабочих мест в классах должно быть таким, чтобы обеспечивалась индивидуальная работа студента на отдельном персональном компьютере;