Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет имени В.А. Бондаренко»

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.19 Методы и средства криптографической защиты информации»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
10.03.01 Информационная безопасность
(код и наименование направления подготовки)

Безопасность автоматизированных систем (информационные технологии и электронная промышленность)
(наименование направленности (профиля) образовательной программы)

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2026

2240873

Рабочая программа дисциплины «*Б1.Д.Б.19 Методы и средства криптографической защиты информации*» рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 10 от "06" 03 2026 г.

Заведующий кафедрой
Кафедра вычислительной техники и защиты информации _____ В.В. Тугов
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
Доцент кафедры ВТиЗИ _____ А.А. Рычкова
должность *подпись* *расшифровка подписи*

_____
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
10.03.01 Информационная безопасность _____ В.В. Тугов
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
главный библиограф ФОГ Т.С. Гасайтис
личная подпись *расшифровка подписи*

Уполномоченный по качеству института
_____ С.Н. Морозова
личная подпись *расшифровка подписи*

№ регистрации _____

© Рычкова А.А., 2026
© ОГУ, 2026

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

формирование теоретических знаний основных криптографических алгоритмов и практических навыков их применения для защиты информации, изучить основные положения криптографии, познакомиться с наиболее распространенными типами шифров и методами их криптоанализа, понятиями целостности информации, криптографическими протоколами, электронной подписью.

Задачи:

1. Освоение основных понятий и алгоритмов криптографии.
2. Ознакомление с наиболее распространенными типами шифров и методами их криптоанализа.
3. Освоение основных криптографических протоколов идентификации и аутентификации.
4. Изучение алгоритмов электронной цифровой подписи.
5. Приобретение навыков шифрования, расшифровки информации.
6. Приобретение навыков реализации алгоритмов идентификации и аутентификации.
7. Приобретение навыков применения криптографических средств защиты информации и разработки собственного программного обеспечения для решения задач защиты информации.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.6 Основы информационной безопасности, Б1.Д.Б.10 Программно-аппаратные средства защиты информации, Б1.Д.Б.17 Дискретная математика, Б1.Д.Б.24 Языки программирования, Б1.Д.В.3 Математические основы криптологии, Б1.Д.В.5 Основы стеганографии*

Постреквизиты дисциплины: *Б1.Д.Б.33 Комплексные системы защиты информации на предприятии, Б1.Д.Б.35 Безопасность информационных систем и баз данных, Б1.Д.Б.36 Операционные системы и администрирование средств защиты информации, Б1.Д.В.Э.6.1 Информационная безопасность в сетях и телекоммуникациях*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9-В-1 Производит выбор и обоснование средства криптографической и технической защиты информации для решения задач для решения задач проектно-технологического и организационно-управленческого типа ОПК-9-В-2 Знает современные криптографические системы шифрования, инфраструктуру открытых ключей, основные криптографические протоколы ОПК-9-В-3 Умеет применять средства	**Знать:** криптографические методы, алгоритмы, протоколы; используемые для обеспечения защиты информации. Типовые средства, методы и протоколы идентификации, аутентификации и авторизации; основные

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	криптографической защиты информации для шифрования данных	понятия теории криптографии; типичные слабости реализации современных криптографических систем; стандарты, модели и методы шифрования; основные алгоритмы идентификации и аутентификации, позволяющие выбирать, обосновывать и применять современные информационно-коммуникационные технологии и программные средства для решения задач проектно-технологического и организационно-управленческого типа **Уметь:** Выбирать, обосновывать и применять современные информационно-коммуникационные технологии и программные средства, реализующие криптографические методы и алгоритмы для решения задач проектно-технологического и организационно-управленческого типа **Владеть:** навыками выбора, обоснования и применения современных информационно-коммуникационные технологии и программных средств, реализующих криптографические методы и алгоритмы для решения задач проектно-технологического и организационно-управленческого типа

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ОПК-4.3 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3-В-1 Планирует порядок и осуществляет необходимые работы по установке, настройке , обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ОПК-4.3-В-2 Умеет настраивать, конфигурировать и использовать отдельные программные, программно-аппаратные (в том числе криптографические) и технические средств защиты информации	**Знать:** Знать криптографические компоненты автоматизированных систем, возможности современных криптографических средств защиты **Уметь:** планировать и осуществлять работы по установке, настройке , обслуживанию и проверке работоспособности программных и программно-аппаратных криптографических средств защиты информации **Владеть:** навыками планирования и осуществления работ по установке, настройке , обслуживанию и проверке работоспособности программных и программно-аппаратных криптографических средств защиты информации

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 академических часа).

Вид работы	Трудоемкость, академических часов	
	7 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**70,5**	**70,5**
Лекции (Л)	18	18
Практические занятия (ПЗ)	16	16
Лабораторные работы (ЛР)	34	34
Консультации	1	1
Индивидуальная работа и инновационные формы учебных занятий	1	1
Промежуточная аттестация (зачет, экзамен)	0,5	0,5
Самостоятельная работа: *- выполнение курсовой работы (КР);* *- самоподготовка (проработка и повторение лекционного материала и*	**73,5** +	**73,5**

Вид работы	Трудоемкость, академических часов	
	7 семестр	всего
материала учебников и учебных пособий; *- изучение разделов курса в системе электронного обучения;* *- изучение разделов массового открытого онлайн-курса «Методы криптографической защиты информации»;* *- подготовка к лабораторным занятиям;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю)*		
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение. Роль и место криптографии в обеспечении информационной безопасности компьютерных систем.	5	1	-	-	4
2	Законодательная и нормативно-методическая база использования шифровальных (криптографических) средств	10	2	-	-	8
3	Симметричные криптосистемы: математический аппарат, программные средства на основе симметричных криптосистем, программирование симметричных криптосистем.	22	4	2	12	10
4	Асимметричных криптосистемы: математический аппарат, программные средства на основе асимметричных криптосистем, программирование асимметричных криптосистем.	22	2	4	4	10
5	Криптографические средства защиты информации: протоколы распределения ключей	20	2	4		10
6	Криптографические средства защиты информации: протоколы идентификации, аутентификации	16	2	2	4	10
7	Криптографические средства обеспечения целостности информации: электронная подпись	22	2	2		10
8	Практическое применение сертифицированных шифровальных (криптографических) средств	22	4	-	14	10
9	Надежность криптосистем. Стойкость криптосистем	5	1	-	-	4
	Итого:	144	18	16	34	76
	Всего:	144	18	16	34	76

4.2 Содержание разделов дисциплины

1. Роль и место криптографии в обеспечении информационной безопасности компьютерных систем. Основные понятия и определения. История развития криптографии. Классификация криптографических систем. Требования к криптографическим системам.

2. Законодательная и нормативно-методическая база использования шифровальных (криптографических) средств Требования регуляторов. Приказ ФАПСИ 152, Приказ ФСБ РФ от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», Постановление Правительства РФ №313. Р 1323565.1.012-2017 Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. ГОСТы

3. **Симметричные криптосистемы: математический аппарат, программные средства на основе симметричных криптосистем, программирование симметричных криптосистем**. Общий принцип функционирования.Традиционные шифры. Современные блочные и поточные шифры: DES, ГОСТ, AES, РСЛОС, RC4.

4. **Асимметричных криптосистемы: математический аппарат, программные средства на основе асимметричных криптосистем, программирование асимметричных криптосистем**. Общий принцип функционирования. Математическая основа. Криптографическая система RSA, El Gamal, Rabina.

5. **Криптографические средства защиты информации: протоколы распределения ключей**. Иерархия ключей. Генерация ключей. Жизненный цикл ключей. Протоколы с центром распределения ключей. Протокол Kerberos. Прямой обмен ключами. Протокол Диффи-Хеллмана

6**. Криптографические средства защиты информации: протоколы идентификации, аутентификации**. Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля. Взаимная проверка подлинности пользователей. Идентификация с нулевой передачей знаний. Схемы обязательств. Системы электронного голосования. Цифровые сертификаты: системы перераспределения доверия, неявные сертификаты.

7**. Криптографические средства обеспечения целостности информации: электронная подпись.** Целостность данных и аутентификация сообщений. Хэш-функции (MD, SHA). Алгоритмы ЭЦП: RSA, Эль Гамаля, Шнорра, Нибберга-Руппеля.

8. **Практическое применение сертифицированных криптографических средств**. Разработка локальных нормативных актов по требованиям регуляторов. Организационные мероприятия по использованию шифровальных (криптографических) средств

9**. Надежность криптосистем**. **Стойкость криптографических систем и алгоритмов**. Энтропия, теоретическая и практическая стойкость, вычислительная стойкость. Теоретико-информационная стойкость. Вычислительная и временная сложность алгоритма. Виды атак: Стойкость актуальных алгоритмов шифрования. Доказуемая стойкость. на простоту: пробное деление, тест Ферма, тест Миллера-Рабина

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	3	Традиционные криптосистемы	1
2	3	Блочные шифры: AES, ГОСТ	2
3	3	Поточные систем шифрования (РСЛОС, RC4)	3
4	4	Программная реализация асимметричных криптосистем (RSA, El Gamal)	4
5	5	Программная реализация протоколов идентификации и аутентификации данных	5
6	8	Практическое применение сертифицированных шифровальных (криптографических) средств	6
		Итого:	34

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	3	Традиционные симметричные криптосистемы	2
2	3	Изучения математических основ преобразований AES	2
3	4	Асимметричные криптосистемы (RSA, El Gamal, Рабина)	4
4	5	Схемы распределения ключей (Диффи-Хеллман, Шамир)	4
5	6	Взаимная проверка подлинности. Протокол FFS	2
6	7	Схемы электронной цифровой подписи (на основе алгоритмов RSA, El Gamal)	2
		Итого:	16

4.5 Курсовая работа (7 семестр)

Задание к КР включает изучение криптографических методов и средств защиты информации, исследование и/или разработку метода криптографической защиты информации.

Примерная тема: Анализ методов и средств криптографической защиты информации

Примеры индивидуальных задании:

1 Алгоритмы электронной цифровой подписи ГОСТ 34.10.

2 Хэширование ГОСТ 34.11

3 Протокол TLS

4 Блочный шифр ГОСТ 34.12.

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Бабаш, А. В. Криптография [Текст] / А. В. Бабаш, Г. П. Шанкин; под ред. В. П. Шерстюка, Э. А. Применко. - М. : Солон-Пресс, 2007. - 512 с. - (Аспекты защиты). - Библиогр.: с. 439-461. - Прил.: с. 462-509. - ISBN 5-93445-135-3.

2. Смарт, Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова ; под ред. С. К. Ландо. - Москва : Техносфера, 2006. - 528 с. : табл. - (Мир программирования). - Предм. указ.: с. 524-525. - ISBN 15-94836-043-1. - ISBN 0077099877. - ISBN 15-94836-043-1.

5.2 Дополнительная литература

1. Хорев, П.Б., Методы и средства защиты информации в компьютерных системах [Текст] : учеб. пособие / П. Б. Хорев .- 4-е изд., стер. - М. : Академия, 2008. - 256 с.

2. Биркгоф, Г. Современная прикладная алгебра = Modern Applied Algebra [Текст] : пер. с англ. / Г. Биркгоф, Т.К. Барти.- 2-е изд., стер. - СПб. : Лань, 2005. - 400 с.

3. Судоплатов С.В., Овчинникова Е.В. Элементы дискретной математики: учеб. для вузов / С.В. Судоплатов. – Новосибирск: НГТУ, 2002.

4. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии [Текст]: [монография] / О. Н. Василенко. - М. : МЦНМО, 2003. - 328 с.

5. Криптография: шаг за шагом: Учебник. - М. : Навигатор, 2002 + CD-ROM.

6. Рычкова А.А. Интерактивный учебно-исследовательский комплекс для построения и анализа алгоритмов шифрования информации (VisualCrypt): (комплекс прикладных программ для лабораторного практикума) / А.А. Рычкова, Р.И. Усманов. - М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т". - Электрон. текстовые дан. (1 файл: 8.7 Mb). - Оренбург : ОГУ, 2015. -Архиватор 7-Zip Зарегистрировано в УФЭР ОГУ. Свидетельство о регистрации № 1116 от 26.05.2015 г. – Оренбург, ОГУ, 2014.

5.3 Периодические издания

1. Информационные технологии : журнал. - М. : Агентство "Роспечать", 2021, 2022.
2. Мехатроника, автоматизация, управление : журнал. - М. : Агентство "Роспечать", 2021, 2022.

5.4 Интернет-ресурсы

1. Национальный Открытый Университет «ИНТУИТ». – Электрон. дан. - НОУ «ИНТУИТ», ИДО «ИНТУИТ», ООО «ИНТУИТ». – Режим доступа: www.intuit.ru. – Загл. с экрана.
2. https://www.coursera.org/learn/asymmetric-crypto - «Coursera», МООК: «Asymmetric Cryptography and Key Management»;
3. https://www.coursera.org/learn/crypto-info-theory - «Coursera», МООК: «Cryptography and Information Theory».
4. http://www.securitylab.ru/ информационный портал по ИТ безопасности
5. http://www.citforum.ru/ форум по информационным технологиям, методам защиты информации

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.

2. Пакет офисных приложений «МойОфис Образование»

3. Для работы с ресурсами Интернет - веб-браузер Яндекс https://yandex.ru/..

4. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2026]. – Режим доступа в сети ОГУ http://garant.net.osu.ru

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется компьютерный класс, оснащенный плакатами.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.