Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

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 2022

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 № 9 от "31" марта 2022 г.

Заведующий кафедрой
Кафедра вычислительной техники и защиты информации — Т.З. Аралбаев
наименование кафедры *подпись* *расшифровка подписи*

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

Доцент кафедры ВТиЗИ — О.Н. Яркова
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
10.03.01 Информационная безопасность — Т.З. Аралбаев
код, наименование *личная подпись* *расшифровка подписи*

Заведующий отделом комплектования научной библиотеки
Н.Н. Бигалиева
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
И.В. Крючкова
личная подпись *расшифровка подписи*

№ регистрации 1/14443

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.

Приобретение навыков применения криптографических средств 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
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1-В-1 Применяет философские основы познания и логического мышления, методы научного познания, в том числе методы системного анализа, для решения поставленных задач УК-1-В-2 Осуществляет критический анализ и синтез информации, полученной из разных источников УК-1-В-3 Понимает основные закономерности и главные особенности	**Знать:** основные положения теории информационной безопасности, нормативно-правовую документацию в области криптографических методов и средств защиты информации, криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации **Уметь:** осуществлять подбор, изучать и обобщать научно-техническую литературу в области криптографических методов и средств защиты информации; применять методы логического мышления, научного познания, системного анализа и синтеза для решения поставленных задач криптографической защиты информации; аргументировать выводы и суждения в

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	социально-исторического развития различных культур в этическом и философском контексте УК-1-В-4 Применяет методы сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий для решения поставленных задач УК-1-В-5 Формулирует и аргументирует выводы и суждения, в том числе с применением философского понятийного аппарата УК-1-В-6 Формулирует собственную гражданскую и мировоззренческую позицию с опорой на системный анализ философских взглядов и исторических закономерностей, процессов, явлений и событий	области применения криптографических методов и средств для защиты информации **Владеть:** навыками подбора и обобщения научно-технической литературы в области криптографических методов и средств защиты информации; применения методов логического мышления, научного познания, системного анализа и синтеза для решения поставленных задач криптографической защиты информации; аргументации выводов и суждений в области применения криптографических методов и средств для защиты информации
ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2-В-1 Выбирает, обосновывает и применяет современные эффективные информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе - отечественного производства, для решения задач профессиональной деятельности	**Знать:** криптографические методы, алгоритмы, протоколы; используемые для обеспечения защиты информации. Типовые средства, методы и протоколы идентификации, аутентификации и авторизации; основные 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 криптографической защиты информации **Уметь:** Выбирать, обосновывать и применять современные информационно-коммуникационные технологии и программные средства, криптографические методы и алгоритмы для решения задач криптографической защиты информации

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		Владеть: навыками выбора, обоснования и применения современных информационно-коммуникационные технологии и программных средств, криптографических методов и алгоритмов для решения задач криптографической защиты информации
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	**Знать:** криптографические методы, алгоритмы, протоколы; используемые для обеспечения защиты информации. Типовые средства, методы и протоколы идентификации, аутентификации и авторизации; основные 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
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	**Знать:** криптографические методы, алгоритмы, протоколы; используемые для обеспечения защиты информации. Типовые средства, методы и протоколы идентификации, аутентификации и авторизации; основные понятия теории криптографии; типичные слабости реализации современных криптографических систем; стандарты, модели и методы шифрования; основные алгоритмы идентификации и аутентификации, позволяющие планировать и осуществлять работы по

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		установке, настройке , обслуживанию и проверке работоспособности программных и программно-аппаратных криптографических средств защиты информации **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:	**86,5**	**86,5**
Лекции (Л)	34	34
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 материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к практическим занятиям;* *- подготовка к экзамену*	**57,5** +	**57,5**
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.	12	4	2		6
2	Стойкость криптографических систем и алгоритмов.	10	4			6
3	Симметричные криптосистемы: математический аппарат, программные средства на основе симметричных криптосистем, программирование симметричных криптосистем.	20	2		12	6
4	Асимметричных криптосистемы: математический аппарат, программные средства на основе асимметричных криптосистем, программирование асимметричных криптосистем.	14	2	2	4	6
5	Криптографические средства защиты информации: протоколы распределения ключей	18	4	4	4	6
6	Криптографические средства защиты информации: протоколы идентификации, аутентификации	12	4	2		6
7	Криптографические средства обеспечения целостности информации: электронная подпись	18	4	4	4	6
8	Практическое применение сертифицированных шифровальных (криптографических) средств.	14	4		4	6
9	Организационные мероприятия по использованию шифровальных (криптографических) средств	18	4	2	6	6
10	Надежность криптосистем	8	2			6
	Итого:	144	34	16	34	60
	Всего:	144	34	16	34	60

4.2 Содержание разделов дисциплины

1. Введение. Роль и место криптографии в обеспечении информационной безопасности компьютерных систем. Основные понятия и определения. История развития криптографии. Классификация криптографических систем. Законодательные и правовые основы защиты компьютерной информации и информационных технологий Требования к криптографическим системам.

2. **Стойкость криптографических систем и алгоритмов**. Энтропия, теоретическая и практическая стойкость, вычислительная стойкость. Теоретико-информационная стойкость. Вычислительная и временная сложность алгоритма.

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 шифровальных (криптографических) средств**. Назначение и порядок использования СКЗИ, реализующих базовый функционал по криптозащите информации ограниченного доступа на примере СКЗИ «КриптоПро CSP». Установка необходимого ПО.

9. **Организационные мероприятия по использованию шифровальных (криптографических) средств** Организация использования СКЗИ и ЭП, Регламентация использования СКЗИ и ЭП на рабочем месте.

10. Надежность криптосистем. Тесты на простоту: пробное деление, тест Ферма, тест Миллера-Рабина. Алгоритмы факторизации: пробное деление, гладкие числа, (P-1)-метод Полларда, разность квадратов, современные методы факторизации. Виды атак: Атака Винера на RSA, атаки на RSA основанные на решетках, атака Хостада, атака Франклина-Рейтера, частичное раскрытие ключа. Стойкость актуальных алгоритмов шифрования. Доказуемая стойкость.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	3	Основные криптографические преобразования	4
2	3	Блочные шифры: AES, ГОСТ	4
3	3	Поточные системы шифрования (РСЛОС, RC4)	4
4	4	Программная реализация асимметричных криптосистем (RSA, El Gamal)	4
5	5	Программная реализация протоколов идентификации и аутентификации данных	4
6	7	Программная реализация схем электронной цифровой подписи (на основе алгоритмов RSA, El Gamal)	4
	8	Назначение и порядок использования СКЗИ, реализующих базовый функционал по криптозащите информации ограниченного доступа на примере СКЗИ «КриптоПро CSP». Установка необходимого ПО.	2
	8	Назначение и порядок использования СКЗИ, реализующих базовый функционал по криптозащите информации ограниченного доступа на примере СКЗИ «КриптоАРМ» (Интерфейс и навигация), «КриптоПроPDF»	2
	9	Назначение и порядок использования СКЗИ, реализующих базовый функционал по криптозащите информации ограниченного доступа на примере СКЗИ «КриптоПро CSP». Развертывание PKI (Экспорт / импорт сертификатов)	2
	9	Инфраструктура открытых ключей (ИОК/PKI). Совместимость криптопровайдеров.	4
		Итого:	34

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Математические основы криптологии	2
2	4	Асимметричные криптосистемы (RSA, El Gamal, Рабина)	2
3	5	Схемы распределения ключей (Диффи-Хеллман, Шамир)	4
4	6	Взаимная проверка подлинности. Протокол FFS	2
5	7	Схемы электронной цифровой подписи (на основе алгоритмов RSA, El Gamal)	4
6	9	Подготовка документов по ведению СКЗИ	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.

Примерные темы:

Алгоритмы электронной цифровой подписи

Электронная цифровая подпись DSA

Хэширование MD2 MD5

Разработка ЭЦП (SHA+DSA)

Совершенно стойкие алгоритмы

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Бабаш, А. В. Криптография. – М.: Солон-Пресс, 2007. – 512 с.

2. Смарт, Н., Криптография [Текст]: пер. с англ. С.А. Кулешова, под.ред. С.К. Ландо/ Н. Смарт. – М.: Техносфера, -2006. - 528с.

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.

Методические указания

Сердюк, А. И., Яркова О. Н. Криптография. Разработка приложений для шифрования информации [Электронный ресурс] : методические указания для студентов, обучающихся по программам высшего профессионального образования по специальности 090104.65 Комплексная защита объектов информатизации, 230101.65 Вычислительные машины, комплексы, системы и сети, направлению подготовки 090900.62 Информационная безопасность, профиль "Комплексная защита объектов информатизации" / А. И. Сердюк, О. Н. Яркова; М-во образования и науки Рос. Федерации,

Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Оренбург. гос. ун-т", Каф. вычисл. техники. - Электрон. текстовые дан. (1 файл: 1.62 Мб). - Оренбург : ОГУ, 2012. - 98 с.

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. Единое окно доступа к образовательным ресурсам: информационная система. – Электрон. дан. – ФГУ ГНИИ ИТТ «Информика»; Министерство образования и науки РФ. – Режим доступа: http://window.edu.ru/. – Загл. с экрана.
2. Национальный Открытый Университет «ИНТУИТ». – Электрон. дан. - НОУ «ИНТУИТ», ИДО «ИНТУИТ», ООО «ИНТУИТ». – Режим доступа: www.intuit.ru. – Загл. с экрана.
3. https://www.coursera.org/learn/asymmetric-crypto - «Coursera», МООК: «Asymmetric Cryptography and Key Management»;
4. https://www.coursera.org/learn/crypto-info-theory - «Coursera», МООК: «Cryptography and Information Theory».
5. http://www.securitylab.ru/ информационный портал по ИТ безопасности
6. http://www.citforum.ru/ форум по информационным технологиям, методам защиты информации

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Интегрированная система решения математических, инженерно-технических и научных задач PTC MathCAD 14.0 - English
2. Средство для разработки и проектирования приложений - Microsoft Visual Studio. Доступно в рамках подписки Microsoft DreamSpark Premium.
4. Справочно-правовая система «Консультант-плюс» - http://www.consultant.ru/

5. Справочно-правовая система «Гарант» - http://www.garant.ru/

6. Рычкова А.А. Прикладная программа «Visual hash function GOST 34.11-2012»: Программное средство / А.А. Рычкова, Е.В. Зойкина. - М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. проф. образования «Оренбург. гос. ун-т». – Электрон. текстовые дан. (1 файл: 2 Мб). – Оренбург: ОГУ, 2014. – Архиватор 7-Zip Зарегистрировано в УФЭР ОГУ, Свидетельство о регистрации № 1022 от 28.10.2014 г. – Оренбург, ОГУ, 2014.

7. 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. унт". - 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.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского 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 лаборатория компьютерный класс, оснащенный компьютерами с обеспечением доступа в электронную информационно-образовательную среду ОГУ.

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