Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Амурский государственный университет"

УТВЕРЖДАЮ
Проректор по учебной и научной работе
Лейфа А.В. Лейфа
24 мая 2024 г.

РАБОЧАЯ ПРОГРАММА
«МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки 10.03.01 Информационная безопасность

Направленность (профиль) образовательной программы – Безопасность автоматизированных систем (по отраслям или в сфере профессиональной деятельности)

Квалификация выпускника – Бакалавр

Год набора – 2024

Форма обучения – Очная

Курс 3 Семестр 5

Экзамен 5 сем

Общая трудоемкость дисциплины 216.0 (академ. час), 6.00 (з.е)

Составитель Л.В. Никифорова, доцент, канд. техн. наук

Институт компьютерных и инженерных наук

Кафедра информационной безопасности

2024

Рабочая программа составлена на основании Федерального государственного образовательного стандарта ВО для направления подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17.11.20 № 1427

Рабочая программа обсуждена на заседании кафедры информационной безопасности

01.02.2024 г. , протокол № 8

Заведующий кафедрой Никифорова Л.В. Никифорова

СОГЛАСОВАНО
Учебно-методическое управление
Чалкина Н.А. Чалкина
24 мая 2024 г.

СОГЛАСОВАНО
Выпускающая кафедра
Никифорова Л.В. Никифорова
24 мая 2024 г.

СОГЛАСОВАНО
Научная библиотека
Петрович О.В. Петрович
24 мая 2024 г.

СОГЛАСОВАНО
Центр цифровой трансформации и технического обеспечения
Тодосейчук А.А. Тодосейчук
24 мая 2024 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины:

Формирование у студентов общих представлений о криптографических методах защиты информации, о применении криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности и об основных принципах, лежащих в основе функционирования криптографических средств защиты информации.

Задачи дисциплины:

1. Дать представление о криптографических методах защиты информации;
2. изучить математические основы современной криптографии;
3. изучить современные стандарты симметричного шифрования;
4. изучить основные криптографические алгоритмы с открытым ключом;
5. изучить криптографические функции хеширования;
6. сформировать умение применять полученные знания для компьютерной реализации криптографических алгоритмов.

2. МЕСТО УЧЕБНОГО ПРЕДМЕТА В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина " Методы и средства криптографической защиты информации " относится к блоку обязательных дисциплин.

Для успешного освоения данной дисциплины необходимы знания, полученные при изучении дисциплины «Языки программирования», «Математический анализ», «Теория информации», «Теория вероятности и математическая статистика», «Основы информационной безопасности». После изучения дисциплины знания, будут использованы при изучении таких дисциплин, как, «Программно-аппаратные средства защиты информации», «Основы управления информационной безопасностью», «Проектирование защищенных автоматизированных систем», при прохождении производственных практик, при написании выпускной квалификационной работы.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ УЧЕБНОГО ПРЕДМЕТА И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

3.1 Профессиональные компетенции и индикаторы их достижения

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИД-1ОПК-9- знать: основные понятия и задачи криптографии, математические модели криптографических систем, основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш- функции и криптографические протоколы, национальные стандарты Российской Федерации в области криптографической защиты ин формации и сферы их применения ИД-2ОПК-9-уметь: использовать СКЗИ для решения задач профессиональной деятельности ИД-3ОПК-9- владеть навыками: применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности

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	ИД-1ОПК-4.3знать: основные меры по защите информации в автоматизированных системах, содержание эксплуатационной документации автоматизированной системы ИД-2ОПК-4.3уметь: устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей используемых в системе защиты информации программных и программно-аппаратных средств ИД-3ОПК-4.3владеть: навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы

4. СТРУКТУРА УЧЕБНОГО ПРЕДМЕТА

Общая трудоемкость учебного предмета составляет 6.00 зачетных единицы, 216.0 академических часов.

1 – № п/п

2 – Тема (раздел) учебного предмета, курсовая работа (проект), промежуточная аттестация

3 – Семестр

4 – Виды контактной работы и трудоемкость (в академических часах)

4.1 – Л (Лекции)

4.2 – Лекции в виде практической подготовки

4.3 – ПЗ (Практические занятия)

4.4 – Практические занятия в виде практической подготовки

4.5 – ЛР (Лабораторные работы)

4.6 – Лабораторные работы в виде практической подготовки

4.7 – ИКР (Иная контактная работа)

4.8 – КТО (Контроль теоретического обучения)

4.9 – КЭ (Контроль на экзамене)

5 – Контроль (в академических часах)

6 – Самостоятельная работа (в академических часах)

7 – Формы текущего контроля успеваемости

1	2	3	4									5	6	7
			4.1	4.2	4.3	4.4	4.5	4.6	4.7	4.8	4.9			
1	Основные цели и задачи криптографии	5	2		2		2						6	Опрос. Подготовка к практической работе. Выполнение и защита лабораторной работы.
2	Историческая	5	4		4		4						12	Опрос.

	криптография													Подготовка к практической работе. Выполнение и защита лабораторной работы.
3	Симметричное шифрование	5	12		12		12						28	Опрос. Подготовка к практической работе. Выполнение и защита лабораторной работы.
4	Криптография с открытым ключом	5	10		10		10						16	Опрос. Подготовка к практической работе. Выполнение и защита лабораторной работы.
5	Электронная подпись	5	4		6		6						14	Опрос. Подготовка к практической работе. Выполнение и защита лабораторной работы.
6	Протоколы	5	2										2	Опрос
7	Экзамен	5									0.3	35.7		
	Итого		34.0		34.0		34.0		0.0	0.0	0.3	35.7	78.0	

5. СОДЕРЖАНИЕ УЧЕБНОГО ПРЕДМЕТА

5.1. Лекции

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
1	Основные цели и задачи криптографии	Триада и гексада Паркера. Основные понятия криптографических методов защиты информации: шифрование, расшифрование, дешифрование, криптография, криптоанализ, хеширование, электронная подпись. Классификация криптосистем. Математическая модель шифра.
2	Историческая криптография	Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования.
3	Симметричное шифрование	DES. ГОСТ 28147-89. ГОСТ Р 34.12-2015. ГОСТ Р 34.13-2015. Режимы шифрования, иммитовставка, AES. Принципы поточного шифрования. Типы

		поточного шифрования. Синхронные и самосинхронизирующиеся шифры. Атаки на симметричные шифры. Слайдовая атака.
4	Криптография с открытым ключом	Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль- Гамаля. Криптосистема Рабина. Генерация случайных чисел. Псевдослучайные числа и их отличия от истинно случайных чисел. Подходы к получению псевдослучайных чисел. Криптографические хеш-функции. ГОСТ Р 34.11- 2012. SHA-3.
5	Электронная подпись	Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10-2012. Инфраструктура открытого ключа
6	Протоколы	Протокол раздельного вручения бита. Протоколы доказательства знания с нулевым разглашением. Протоколы простановки "слепых" подписей. Протоколы голосования. Протоколы безопасных вычислений.

5.2. Практические занятия

Наименование темы	Содержание темы
Введение в криптографию	Простые шифры замены
Шифры многоалфавитной замены	Шифр Виженера
Криптоанализ шифров замены	Криптоанализ шифра простой замены
Симметричное шифрование	Шифр DES.
Симметричное шифрование	ГОСТ 28147-89. ГОСТ Р 34.12-2015. ГОСТ Р 34.13-2015.
Симметричное шифрование	Режимы шифрования, иммитовставка.
Симметричное шифрование	AES.
Симметричное шифрование	Принципы поточного шифрования.
Симметричное шифрование	Слайдовая атака.
Криптография с открытым ключом	Протокол Диффи-Хеллмана.
Криптография с открытым ключом	Криптосистема RSA.
Криптография с открытым ключом	Криптосистема Эль-Гамаля. Криптосистема Рабина.
Криптография с открытым ключом	Генерация случайных чисел. Псевдослучайные числа и их отличия от истинно случайных чисел. Подходы к получению псевдослучайных чисел.
Криптография с открытым ключом	Криптографические хеш- функции. ГОСТ Р 34.11-2012. SHA-3.
Электронная подпись	Электронная подпись RSA и Эль-Гамаля

Электронная подпись	Электронная подпись. ГОСТ Р 34.10-2012.
Электронная подпись	Атаки на ЭЦП

5.3. Лабораторные занятия

Наименование темы	Содержание темы
Введение в криптографию	Простые шифры замены
Шифры многоалфавитной замены	Шифр Виженера
Перестановочные шифры	Шифры перестановки
Криптоанализ шифров замены	Криптоанализ шифра Виженера
Шифр DES.	Исследование процессов шифрования и расшифрования сообщений с помощью S-DES
Криптоанализ симметричных шифров	Слайдовая атака.
Системы поточного шифрования	Поточные шифры
Лабораторная работа № 1. Асимметричные шифры	Изучение криптосистемы RSA. Шифрование и расшифрование.
Лабораторная работа № 2. Асимметричные шифры	Изучение системы Эль-Гамаля
Лабораторная работа № 3. Асимметричные шифры	Проверка правильности вычисления цифровой подписи Эль-Гамаля.
Лабораторная работа № 4. Асимметричные шифры	Проверка подлинности цифровой подписи Эль-Гамаля.
Лабораторная работа № 1. ЭЦП	Изучение системы цифровой подписи Эль-Гамаля
Лабораторная работа № 2. ЭЦП	Электронная цифровая подпись RSA и ЭЦП ГОСТ Р34.10-94.

6. САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)	Трудоемкость в академических часах
1	Основные цели и задачи криптографии	Изучение учебной литературы. Подготовка к практической работе. Выполнение лабораторной работы.	6
2	Историческая криптография	Изучение учебной литературы. Подготовка к практической работе. Выполнение лабораторной работы.	12
3	Симметричное шифрование	Изучение учебной литературы. Подготовка к практической работе. Выполнение лабораторной работы.	28
4	Криптография с открытым ключом	Изучение учебной литературы. Подготовка к практической работе. Выполнение лабораторной работы.	16
5	Электронная подпись	Изучение учебной литературы. Подготовка к практической работе.	14

		Выполнение лабораторной работы.	
6	Протоколы	Изучение учебной литературы.	2

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Образовательный процесс по дисциплине строится на основе комбинации следующих образовательных технологий.

Интегральную модель образовательного процесса по дисциплине формируют технологии методологического уровня: модульно- рейтинговое обучение, технология поэтапного формирования умственных действий, технология развивающего обучения, элементы технологии развития критического мышления.

Реализация данной модели предполагает использование следующих технологий стратегического уровня (задающих организационные формы взаимодействия субъектов образовательного процесса), осуществляемых с использованием определенных тактических процедур:

– лекционные (вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция);

– лабораторные (углубление знаний, полученных на теоретических занятиях, решение задач);

– практические (формирование определенных умений и навыков, формирование алгоритмического мышления);

– активизации познавательной деятельности (приемы технологии развития критического мышления через чтение и письмо, работа с литературой, подготовка презентаций по темам домашних работ);

– самоуправления (самостоятельная работа студентов, самостоятельное изучение материала).

Информационные технологии используются при организации коммуникации со студентами для представления информации, выдачи рекомендаций и консультирования по оперативным вопросам (электронная почта), использование мультимедиа-средств при проведении лекционных и практических занятий.

В качестве образовательных технологий при изучении дисциплины используются, мультимедийные лекции, на лабораторных занятиях используются лабораторные стенды и современные пакеты программных продуктов. С целью текущего контроля знаний студентов на лабораторных работах проводится контроль выполнения работы. Студентам предлагается обсудить поученные результаты и высказать свое мнение по применению возможных приемов для улучшения показателей либо результатов работы.

8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Промежуточная аттестация по итогам освоения дисциплины: экзамен.

Вопросы для подготовки к экзамену.:

1. Способы защиты информации.
2. Триада CIA.
3. Гексада Паркера
4. Основные определения криптографии.
5. Шифр Цезаря.
6. Шифр Виженера.
7. Шифр простой одинарной перестановки.
8. Шифр блочной одинарной перестановки.
9. Шифр табличной маршрутной перестановки.
10. Шифр вертикальной перестановки.
11. Шифр множественной перестановки.
12. Одноразовый шифровальный блокнот
13. Классификация ключей.
14. Классификация криптографических алгоритмов.
15. Свойства криптосистем. Имитостойкость.
16. Свойства криптосистем. Криптографическая стойкость.

17. Основные задачи современной криптографии.
18. Управление ключами.
19. Общие требования к криптосистемам.
20. Алгебраическая модель шифра.
21. Вероятностная модель шифра.
22. Обобщенная модель шифра.
23. Результаты теории информации для криптографии
24. Режимы работы блочных шифров
25. Электронная кодовая книга
26. Сцепление блоков шифра
27. Обратная связь по шифротексту
28. Обратная связь по выходу
29. Схема алгоритма ГОСТ 28147-89
30. Режимы работы алгоритма ГОСТ 28147—89
31. Шифр «Магма» (ГОСТ Р 34.12-2015)
32. Атаки на алгоритмы шифрования
33. Метод грубой силы
34. Потеря стойкости и попытки усиления существующих шифров
35. Метод «встреча по середине»
36. Метод бумеранга
37. Линейный криптоанализ
38. Слайдовая атака
39. Структура алгоритма AES
40. Шифр «Кузнечик» (ГОСТ Р 34.12-2015)
41. Режимы простой замены (ГОСТ Р 34.13-2015)
42. Режимы гаммирования (ГОСТ Р 34.13-2015)
43. Режим выработки имитовставки
44. Генерация ключей
45. Генератор Блюм — Блюма — Шуба
46. Стандарт ANSI X9.17
47. Ключевые пространства
48. Хранение и распределение ключей
49. Система Диффи - Хеллмана
50. Вычисление числа, обратного по модулю заданному. Расширенный алгоритм Евклида.
51. Шифр Шамира
52. Шифр Эль-Гамаля.
53. Шифр RSA.
54. Выбор параметров и безопасность RSA.
55. Метод бесключевого чтения.
56. Атака на основе китайской теоремы об остатках.
57. Требования к криптографическим хэш-функциям.
58. Бесключевые хэш-функции.
59. Одноключевые хэш-функции.
60. Код аутентификации HMAC
61. Свойства цифровой подписи
62. Электронная цифровая подпись на основе RSA.
63. ЭЦП на основе схемы Эль-Гамаля
64. Стандарты на электронную цифровую подпись
65. Виды ЭЦП.
66. Цифровые сертификаты.
67. Инфраструктура открытых ключей
68. Криптографические протоколы и их участники
69. Разрешение споров по ЭЦП (протокол с судейством)
70. Обмен ключами с помощью асимметричных криптосистем

71. Атака «человек посередине»
72. Блокировочный протокол.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРЕДМЕТА

а) литература

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2024. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536902 (дата обращения: 21.03.2024).
2. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/bcode/536453 (дата обращения: 21.03.2024).
3. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2024. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536132 (дата обращения: 21.03.2024).
4. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2024. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536733 (дата обращения: 21.03.2024).
5.Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2024. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/bcode/537383 (дата обращения: 21.03.2024).

б) программное обеспечение и Интернет-ресурсы

№	Наименование	Описание
1	Операционная система Linux	GNU-лицензия (GNU General Public License)
2	LibreOffice	Бесплатное распространение по лицензии GNU LGPL https://ru.libreoffice.org/about-us/license/
3	http://www.IPRbooks.ru	Электронная библиотечная система «IPRbooks» специализируется на учебных материалах по гуманитарным, естественным и точным наукам
4	https://e.lanbook.com/	ЭБС «Лань» – это крупнейшая политематическая база данных, включающая в себя контент сотен издательств научной, учебной литературы и научной периодики.
5	https://urait.ru	Образовательная платформа Юрайт – образовательный ресурс, электронная библиотека и интернет-магазин, где читают и покупают электронные и печатные учебники авторов – преподавателей ведущих университетов для всех уровней профессионального образования, а также пользуются видео- и аудиоматериалами, тестированием и

		сервисами для преподавателей, доступными 24 часа 7 дней в неделю

в) профессиональные базы данных и информационные справочные системы

№	Наименование	Описание
1	www.elibrary.ru	Крупнейший российский информационный портал в области науки, технологии, медицины и образования.
2	https://bdu.fstec.ru/	Банк данных угроз безопасности информации

10. МАТЕРИАЛЬНО- ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРЕДМЕТА

Занятия по дисциплине проводятся в специальных помещениях, представляющих собой учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Все помещения, в которых проводятся занятия, соответствуют действующим противопожарным правилам и нормам. Каждый обучающийся обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам и к электронной информационно- образовательной среде университета. Самостоятельная работа обучающихся осуществляется в помещениях, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно- образовательную среду университета.

Для оптимальной организации процесса изучения данной дисциплины (модуля) студенту необходимо придерживаться следующих рекомендаций в организации своей деятельности.

В рамках лекций необходимо вести конспект лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.

В рамках лабораторных (практических) работ обучающимся необходимо изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д. При этом учесть рекомендации преподавателя и требования учебной программы. В ходе непосредственного выполнения лабораторных (практических) работ необходимо освоить основные понятия и методики выполнения лабораторной (практической) работы, ответить на контрольные вопросы.

При подготовке к зачету/ экзамену студент должен выполнить рекомендации по организации своей деятельности в отношении лекций и лабораторных (практических) работ. При ответе на зачете/ экзамене студент должен показать глубину понимания проблемы, знание фактического материала, первоисточников, умение логично, точно излагать свои мысли, оперировать научными понятиями и технологией.

При изучении дисциплины «Методы и средства криптографической защиты информации» используются: лекционная аудитория, оборудованная мультимедийными средствами; лаборатории, оборудованные рабочими местами пользователей ЭВМ.