УТВЕРЖДЕНО
решением Ученого совета ФМИАТ
от «16» мая 2023 г., протокол № 4/23
Председатель _____ Волков М.А.
(подпись, расшифровка подписи)
«16» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Теоретико-числовые методы и алгоритмы, информационные технологии в автоматизированных системах
Факультет	Математики, информационных и авиационных технологий
Кафедра	Информационной безопасности и теории управления
Курс	3

Специальность: 10.05.03 "Информационная безопасность автоматизированных систем"
(код специальности (направления), полное наименование)

Специализация: "Безопасность открытых информационных систем"
полное наименование

Форма обучения: очная
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: «01» сентября 2023 г.

Программа актуализирована на заседании кафедры: протокол № 12 от 12.04.2023 г
Программа актуализирована на заседании кафедры: протокол №10 от 15.04.2024 г
Программа актуализирована на заседании кафедры: протокол №____ от _____20_____ г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Иванцов Андрей Михайлович	ИБ и ТУ	Кандидат технических наук, доцент

СОГЛАСОВАНО
Заведующий выпускающей кафедрой «Информационная безопасность и теория управления»
_____/ Андреев А.С. / *(подпись) (Ф.И.О.)* «11» 05 2023 г.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Теоретико-числовые методы и алгоритмы, информационные технологии в автоматизированных системах» является получение знаний, умений, навыков и опыта деятельности в области анализа и применения теоретико-числовых алгоритмов при решении задач информационной безопасности, характеризующих этапы формирования компетенций и обеспечивающих достижение планируемых результатов освоения образовательной программы.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Теоретико-числовые методы и алгоритмы, информационные технологии в автоматизированных системах» относится к вариативной части Блока 1 «Дисциплины (модули)» Основной Профессиональной Образовательной Программы специалитета по специальности 10.05.03 – "Информационная безопасность автоматизированных систем".

Курс учебной дисциплины тесно связан с другими учебными дисциплинами, в первую очередь с курсами «Физика», «Основы информационной безопасности», позволяющими понять физическую сущность информационных технологий.

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

знание базовых понятий в области математики и вычислительной техники;

способность использовать нормативные правовые документы;

способность анализировать проблемы и процессы;

способность использовать основные законы естественно-научных дисциплин, применять методы математического анализа и моделирования.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Сети и системы передачи информации»; «Программно-аппаратные средства обеспечения информационной безопасности»; «Модели безопасности компьютерных систем».

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины «Теоретико-числовые методы построения алгоритмов и систем защиты информации» направлен на формирование следующих компетенций.

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ПК-3 - Способен разрабатывать проектные решения по защите информации в автоматизированных системах	**Знать:** Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов Критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем Принципы формирования политики

	информационной безопасности в автоматизированных системах **Уметь:** Применять действующую нормативную базу в области обеспечения защиты информации Определять типы субъектов доступа и объектов доступа, являющихся объектами защиты Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подле-жащим реализации в автоматизированной системе **Владеть:** Навыками разработки проектов нормативных документов, регламентирующих работу по защите информации Навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах
ПК-5 - Способен участвовать в научных и исследовательских работах в сфере разработки средств защиты информации от НСД	**Знать:** Национальные, межгосударственные и международные стандарты, устанавливающие требования к организации и проведению научно-исследовательских, опытно-конструкторских работ, опытной эксплуатации средств и систем защиты информации от НСД Руководящие и методические документы упол-номоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты информации от НСД Основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты **Уметь:** Организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопас-ности, выработку предложений по вопросам комп-лексного обеспечения информационной безопасности, разработку моделей угроз НСД Проводить выбор, исследовать эффективность и разрабатывать технико-экономическое обоснование проектных решений средств и систем защиты информации от НСД с целью обеспечения требуемого уровня защищенности **Владеть:** Навыками планирования этапов выполнения

	НИОКР по созданию средств и систем защиты информации от НСД Навыками организации опытной эксплуатации средств и систем защиты информации от НСД

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 8.

4.2. Объем дисциплины по видам учебной работы (в часах):

Вид учебной работы	Количество часов (форма обучения: *очная*)			
	Всего по плану	**В т.ч. по семестрам**		
		5	**6**	
1	2	3	4	5
Контактная работа обучающихся с преподавателем в соответствии с УП	**180**	**90/90***	**90/90***	
Аудиторные занятия	**180**	**90/90***	**90/90***	
Лекции	**72**	**36/36***	**36/36***	
Практические и семинарские занятия	**36**	**18/18***	**18/18***	
Лабораторные работы (лабораторный практикум)	**72**	**36/36***	**36/36***	
Самостоятельная Работа	**36**	**18**	**18**	
Форма текущего контроля знаний и контроля самостоятельной работы.	Лабораторные работы, практические задания	Лабораторные работы, практические задания	Лабораторные работы, практические задания	
Курсовая работа				
Контроль	**72**	**36**	**36**	
Виды промежуточной аттестации	Экзамен	Экзамен	Экзамен	
Всего часов по дисциплине	**288**	**144**	**144**	

*В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий в таблице через слеш указывается количество часов работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения.

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы:

Форма обучения _____очная_____

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Раздел 1. Теоретико-числовые алгоритмы в криптологии							
1.Теория алгоритмов. Частично рекурсивные функции и их вычислимость	14	4	2	6	2	2	Защита лабораторной работы, практические задания
2. Сложность вычислений	12	4	2	4	2	2	Защита лабораторной работы, практические задания
3. Тестирование чисел на простоту и построение больших простых чисел	12	2	2	6	2	2	Защита лабораторной работы, практические задания
4. Факторизация целых чисел с экспоненциальной сложностью.	12	4	2	4	2	2	Защита лабораторной работы, практические задания
5. Факторизация целых чисел с субэкспоненциальной сложностью	8	2	2	2	2	2	Защита лабораторной работы, практические задания
6. Алгоритмы дискретного логарифмирования	12	4	4	2	2	2	Защита лабораторной работы, практические

							задания
Раздел 2. Угрозы информации							
7. Информацион-ная безопасность сетей.	8	4	2			2	Защита лабораторной работы, практические задания
8. Способы совершения компьютерных преступлений	5	4				1	
9. Уязвимость сети Интернет.	3	2				1	
Раздел 3. Виды возможных нарушений безопасности информационной системы							
10. Компьютерные преступления	13	4	2	6	2	1	Защита лабораторной работы, практические задания
11. Вредоносные программы	9	2		6	2	1	практические задания
Раздел 4. Информационная безопасность информационных систем							
12. Модели информационной безопасности информационных систем	19	6	4	6	4	3	Защита лабораторной работы, практические задания
13. Криптографические способы защиты информации	19	6	4	6	4	3	Защита лабораторной работы, практические задания
14. Организация информационной безопасности компании	19	6	4	6	4	3	Защита лабораторной работы, практические задания
15. Обеспечение информационной безопасности	19	6	4	6	2	3	Защита лабораторной работы, практические задания
Раздел 5. Методы и средства защиты компьютерной информации							
16. Контроль доступа к информации	11	4	1	4	2	2	Защита лабораторной работы,

							практические задания
17. Методы и средства защиты информации	11	4	1	4	2	2	Защита лабораторной работы, практические задания
18. Антивирусное ПО	10	4		4	2	2	Защита лабораторной работы, практические задания
Всего	288 (без экза-менов)	72	36	72	36	36	

5. СОДЕРЖАНИЕ КУРСА

Раздел 1. Теоретико-числовые алгоритмы в криптологии

Тема 1. Теория алгоритмов. Частично рекурсивныефункции и их вычислимость

Типы алгоритмических моделей. Машина произвольного доступа и вычислимые функции. Тезис Черча длямашины произвольного доступа.

Рекурсия как метод определения арифметических функций. Класс частично рекурсивных функций. Базисные функции. Операции над функциями.

Общерекурсивные и примитивно-рекурсивные функции. Тезис Черча для частично-рекурсивных функций. Способы доказательства вычислимости функций. Теорема о вычислимости суперпозиции. Теорема о вычислимости рекурсии. Теорема о вычислимости минимизации. Теорема о частичной

рекурсивности функций, вычислимых на машине произвольного доступа. Алгоритмически неразрешимые проблемы.

Тема 2. Сложность вычислений

Характеристики сложности вычислений: временная и емкостная сложность.

Классы сложности P и NP и их взаимосвязь. Понятие недетерминированной

машины Тьюринга. Полиномиальная сводимость задач. NP-полные и NP-трудные задачи. Формулировка теоремы Кука.

Тема 3. Тестирование чисел на простоту и построение больших простых чисел

Простое число. Каноническое разложение натурального числа. Методы проверки простоты чисел. Метод пробных делений. Решето Эратосфена. Тест на основе малой теоремы Ферма. Тесты на простоту для чисел специального вида. Числа Мерсенна. (N±1)-методы проверки простоты чисел и построения больших простых чисел. Алгоритм Конягина – Померанса. Вероятностные тесты на простоту. Тест Соловея – Штрассена. Тест Рабина – Миллера. Современные

методы проверки простоты чисел.

Тема 4. Факторизация целых чисел с экспоненциальной сложностью

Понятие факторизации целых чисел. Алгоритм Ферма. (P-1)-метод Полларда и оценка его сложности. ρ-метод Полларда. Метод Шермана – Лемана. Алгоритм Ленстры. Алгоритм Полларда – Штрассена.

Тема 5. Факторизация целых чисел с субэкспоненциальной сложностью

Алгоритм Диксона. Стратегия LP и использование больших простых чисел. Стратегия PS

и алгоритм Полларда – Штрассена. Стратегия EAS – стратегия раннего обрыва. Квадратичное решето. Субэкспоненциальные вероятностные алгоритмы. Методы Шнорра – Ленстры и Ленстры – Померанса. Алгоритмы решета числового поля.

Тема 6. Алгоритмы дискретного логарифмирования

Задача дискретного логарифмирования. Алгоритм согласования. Алгоритм Полига – Хеллмана. ρ-метод Полларда для дискретного логарифмирования.

Дискретное логарифмирование в простых полях. Дискретное логарифмирование в полях Галуа. Дискретное логарифмирование и решето числового поля.

Раздел 2. Угрозы информации

Тема 7. Информационная безопасность сетей.

Информационная безопасность в условиях функционирования в России глобальных сетей. Угрозы информационной безопасности для АСОИ.

Тема 8. Способы совершения компьютерных преступлений

Тема 9. Уязвимость сети Интернет

Пользователи и злоумышленники в сети Интернет. Причины уязвимости сети Интернет. Удаленные атаки на интрасети.

Раздел 3. Виды возможных нарушений безопасности информационной системы

Тема 10. Компьютерные преступления

Классификация компьютерных преступлений. Виды противников или «нарушителей».

Тема 11. Вредоносные программы

Условия существования вредоносных программ. Хакерские утилиты и прочие вредоносные программы. Спам. Понятия о видах вирусов. Классические компьютерные вирусы. Сетевые черви. Троянские программы.

Раздел 4. Информационная безопасность информационных систем

Тема 12. Модели информационной безопасности информационных систем

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Тема 13. Криптографические способы защиты информации

Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. Классификация методов криптографического закрытия информации. Шифрование. Симметричные криптосистемы. Криптосистемы с открытым ключом (асимметричные). Характеристики существующих шифров. Кодирование. Стеганография. Электронная цифровая подпись.

Тема 14. Организация информационной безопасности компании

Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны. Организация информационной безопасности компании. Выбор средств информационной безопасности.

Тема 15. Обеспечение информационной безопасности

Методы обеспечения информационной безопасности РФ. Ограничение доступа. Контроль доступа к аппаратуре.

Раздел 5. Методы и средства защитыкомпьютерной информации

Тема 16. Контроль доступа к информации

Разграничение и контроль доступа к информации. Предоставление привилегий на доступ. Идентификация и установление подлинности объекта (субъекта).

Тема 17. Методы и средства защиты информации

Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Организационные мероприятия по защите

информации. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.

Тема 18. Антивирусное ПО

Признаки заражения компьютера. Источники компьютерных вирусов. Основные правила защиты. Антивирусные программы.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

1. Частично рекурсивные функции и их вычислимость
2. Тестирование чисел на простоту и построение больших простых чисел
3. Факторизация целых чисел с экспоненциальной сложностью.
4. Факторизация целых чисел с субэкспоненциальной сложностью
5. Алгоритмы дискретного логарифмирования
6. Лицензирование и сертификация в области защиты информации. Основные нормативные руководящие документы.
7. Информационная безопасность сетей. Способы совершения компьютерных преступлений. Уязвимость сети Интернет.
8. Классификация угроз безопасности информационных объектов
9. Компьютерные преступления. Вредоносные программы. Признаки появления вирусов.
10. Выявление и фиксация следов противоправной деятельности, связанной с использованием компьютерной техники
11. Модели информационной безопасности информационных систем. Криптографические способы защиты информации.
12. Применение методов анализа многомерных данных в задачах защиты информации. Нейрокриптография.
13. Обеспечение информационной безопасности. Контроль доступа к информации. Методы и средства защиты информации.
14. Антивирусное ПО.Установка и настройка программного антивирусного комплекса
15. Анализ безопасности мобильных технологий

(форма проведения – практические занятия)

7. ЛАБОРАТОРНЫЕ РАБОТЫ (ЛАБОРАТОРНЫЙ ПРАКТИКУМ)

Темы лабораторных работ:
Лабораторная работа 1. Простые числа
Лабораторная работа 2. Факторизация целых чисел
Лабораторная работа 3. Анализ рисков информационной безопасности
Лабораторная работа 4. Построение концепции информационной безопасности предприятия
Лабораторная работа 5. Процедура аутентификации пользователя на основе пароля
Лабораторная работа 6. Программная реализация криптографических алгоритмов
Лабораторная работа 7. Механизмы контроля целостности данных
Лабораторная работа 8. Алгоритмы поведения вирусных и других вредоносных программ
Лабораторная работа 9. Алгоритмы предупреждения и обнаружения вирусных угроз
Лабораторная работа 10. Пакеты антивирусных программ
Лабораторная работа 11. Построение VPN на базе программного обеспечения

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Не предусмотрены учебным планом дисциплины.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНАМ

9.1 Вопросы к экзамену № 1

1. Понятие алгоритма, примеры алгоритмов. Понятие рекурсивной функции. Основные требования к алгоритмам. Типы алгоритмических моделей.
2. Машина произвольного доступа и вычислимые функции. Тезис Черча для машины произвольного доступа.
3. Класс частичнорекурсивных функций. Операции над функциями.
4. Общерекурсивные и примитивно-рекурсивные функции. Тезис Черча для частично-рекурсивных функций.
5. Способы доказательства вычислимости функций. Теорема о вычислимости суперпозиции. Теорема о вычислимости рекурсии.
6. Теорема о вычислимости минимизации.
7. Теорема о частичной рекурсивности функций, вычислимых на машине произвольного доступа.
8. Алгоритмически неразрешимые проблемы.
9. Характеристики сложности вычислений: временная и емкостная сложность.
10. Классы сложности P и NP и их взаимосвязь. Полиномиальная сводимость задач. NP-полные и NP-трудныезадачи. Формулировка теоремы Кука.
11. Простое число. Каноническое разложение натурального числа. Методы проверки простоты чисел. Метод пробных делений. Решето Эратосфена.
12. Тест на основе малой теоремы Ферма. Тесты на простоту для чисел специального вида. Числа Мерсенна. ($N\pm1$)-методы проверки простоты чисел и построения больших простых чисел.
13. Алгоритм Конягина – Померанса. Вероятностные тесты на простоту.
14. Тест Соловея – Штрассена. Тест Рабина – Миллера. Современные методы проверки простоты чисел.
15. Понятие факторизации целых чисел. Алгоритм Ферма.
16. (P-1)-метод Полларда и оценка его сложности. ρ-метод Полларда.
17. Метод Шермана – Лемана. АлгоритмЛенстры. Алгоритм Полларда – Штрассена.
18. Алгоритм Диксона. Стратегия LP и использование больших простых чисел.
19. Стратегия PS и алгоритм Полларда – Штрассена.
20. Стратегия EAS – стратегия раннего обрыва. Квадратичное решето.
21. Субэкспоненциальные вероятностные алгоритмы. Методы Шнорра – Ленстры и Ленстры – Померанса. Алгоритмы решета числового поля.
22. Задача дискретного логарифмирования. Алгоритм согласования. Алгоритм Полига – Хеллмана. ρ-метод Полларда для дискретного логарифмирования.
23. Основные понятия и определения информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности.
24. Классификация атак. Модели сетевой безопасности и безопасности информационной системы.
25. Классическая задача криптографии. Угрозы со стороны злоумышленника и участниковпроцесса информационного взаимодействия.
26. Шифры замены и перестановки. Моно- и многоалфавитные подстановки Шифры Цезаря, Виженера, Вернама. Методы дешифрования.
27. Классификация методов дешифрования. Модель предполагаемого противника. Правила Керкхоффа.
28. Совершенная секретность по Шеннону. Примеры совершенно секретных систем.Шифр Вернама. Понятие об управлении ключами.

29. Блочные криптосистемы с секретным ключом. Алгоритм DES. Описание DES. Основные этапы алгоритма.
30. Схема алгоритма DES. Раунд алгоритма. Преобразование ключа.
31. Алгоритм DES. Подстановка с помощью S-блоков. Расшифрование в DES.
32. Блочные криптосистемы с секретным ключом. Режимы работы. ГОСТ 28147-89 в режиме простой замены.
33. Поточные криптосистемы с секретным ключом. Синхронные и самосинхронизирующиеся поточные криптосистемы. Примеры. ГОСТ 28147-89 в режимах гаммирования.
34. Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра.
35. Теория сложности вычислений. Классификация алгоритмов.
36. Алгоритм RSA. Математическая модель алгоритма. Стойкость алгоритма.
37. Криптосистема Эль-Гамаля.
38. Электронная подпись. Варианты электронной подписи на основе алгоритмов RSA иЭль-Гамаля.
39. Хэш-функции и их применение. Хеш-функция MD2.
40. Однонаправленные (односторонние) функции с секретом и их применение.
41. Обобщенная модель электронной цифровой подписи. Схема Диффи-Хеллмана, схема Эль-Гамаля.
42. Цифровая подпись на основе алгоритма RSA.
43. Стандарт цифровой подписи DSS. Генерация цифровой подписи. Проверка цифровой подписи.
44. Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны. Протоколы аутентификации с использованием nonce и временных меток.
45. Криптографические протоколы. Понятие криптографического протокола и обоснование необходимости их использования. Протокол обмена сеансовыми ключами. Вскрытие "человек-в-середине". Протокол "держась за руки".
46. Сертификация ключей с помощью цифровых подписей. Разделение секрета. Метки времени. Пример протокола защиты базы данных.
47. Основы криптоанализа. Обзор возможных вариантов криптоанализа. Метод вскрытия «встреча посередине». Вскрытие со словарем. Вскрытие системы Вижинера, использующей простой XOR.
48. Метод бесключевого чтения RSA. Атака на подпись RSA по выбранному шифротексту. Вскрытие хэш-функций с использованием парадокса дня рождения.

9.2 Вопросы к экзамену № 2

1. Основные требования к алгоритмам. Типы алгоритмических моделей.
2. Класс частичнорекурсивных функций. Операции над функциями.
3. Общерекурсивные и примитивно-рекурсивные функции. Тезис Черча для частично-рекурсивных функций.
4. Способы доказательства вычислимости функций. Теорема о вычислимости суперпозиции. Теорема о вычислимости рекурсии.
5. Теорема о частичной рекурсивности функций, вычислимых на машине произвольного доступа.Алгоритмически неразрешимые проблемы.
6. Характеристики сложности вычислений: временная и емкостная сложность.
7. Классы сложности P и NP и их взаимосвязь. Полиномиальная сводимость задач. NP-полные и NP-трудныезадачи. Формулировка теоремы Кука.
8. Простое число. Каноническое разложение натурального числа. Методы проверки

простоты чисел. Современные методы проверки простоты чисел.
9. Понятие факторизации целых чисел. Алгоритм Ферма.
10. (P-1)-метод Полларда и оценка его сложности. ρ-метод Полларда.
11. Метод Шермана – Лемана. АлгоритмЛенстры. Алгоритм Полларда – Штрассена.
12. Алгоритм Диксона. Стратегия LP и использование больших простых чисел.
13. Стратегия PS и алгоритм Полларда – Штрассена.
14. Стратегия EAS – стратегия раннего обрыва. Квадратичное решето.
15. Субэкспоненциальные вероятностные алгоритмы. Методы Шнорра – Ленстры и Ленстры – Померанса. Алгоритмы решета числового поля.
16. Задача дискретного логарифмирования. Алгоритм согласования. Алгоритм Полига – Хеллмана. ρ-метод Полларда для дискретного логарифмирования.
17. Разграничение и контроль доступа к информации. Идентификация.
18. Законодательные и правовые основы защиты компьютерной информации информационных технологий.
19. Безопасность информационных ресурсов и документирование информации
20. Вычислительные сети и защита информации; нормативно-правовая база функционирования систем защиты информации
21. Правовая защита программного обеспечения авторским правом.
22. Проблемы защиты информации в информационных системах.
23. Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах
24. Защита локальных сетей и операционных систем;
25. Internet в структуре информационно-аналитического обеспечения информационных систем; рекомендации по защите информации в Internet.
26. Содержание системы средств защиты компьютерной информации в информационных системах.
27. Защищенная информационная система и система защиты информации;
28. законодательная, нормативно-методическая и научная база системы защиты информации.
29. Требования к содержанию нормативно-методических документов по защите информации;
30. Организационно-правовой статус службы информационной безопасности; организационно-технические и режимные меры; Политика безопасности:
31. Программно-технические методы и средства защиты информации;
32. Программно-аппаратные методы и средства ограничения доступа к компонентам компьютера;
33. Типы несанкционированного доступа и условия работы средств защиты
34. Симметричные криптосистемы: основные понятия и определения
35. Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.
36. Изучение американского стандарта шифрования данных DES;
37. Отечественный стандарт шифрования данных; режим простой замены;
38. Режим гаммирования; режим гаммирования с обратной связью;
39. Режим выработки имитовставки; блочные и поточные шифры.
40. Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах.
41. Концепция криптосистемы с открытым ключом;
42. Криптосистема шифрования данных RSA (процедуры шифрования и расшифрования в этой системе);
43. Схема шифрования Полига—Хеллмана;

44. Схема шифрования Эль-Гамаля.
45. Методы идентификации и проверки подлинности пользователей компьютерных систем. Проблема аутентификации данных и электронная цифровая подпись
46. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов
47. Отечественный стандарт хэш-функции
48. Алгоритм цифровой подписи RSA
49. Алгоритм цифровой подписи Эль-Гамаля (EGSA)
50. Алгоритм цифровой подписи DSA
51. Отечественный стандарт цифровой подписи.
52. Защита компьютерных систем от удаленных атак через сеть Internet.
53. Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН.
54. Программно-аппаратная система защиты от несанкционированного доступа (НСД) КРИПТОН-ВЕТО;
55. Защита от НСД со стороны сети; абонентское шифрование и ЭЦП
56. Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов).
57. Классификация способов защиты; защита от отладок и дизассемблирования;
58. способы встраивания защитных механизмов в программное обеспечение
59. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.
60. Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации; защита арифметических вычислений в компьютерных системах;
61. Список практических вопросов и задач на экзамене по дисциплине
62. Алгоритмы шифрования последовательности блоков методами DES, ГОСТ 28147-89 во всех режимах;
63. Алгоритмы многораундового шифрования блока методами DES, ГОСТ 28147-89 во всех режимах;
64. Операции, применяемые для шифрования блока в раунде методами DES, ГОСТ 28147 -89;
65. Алгоритмы шифрования блока в раунде методами DES, ГОСТ 28147-89;
66. Алгоритмы выработки ключа для шифрования блока в раунде методами DES, ГОСТ 28147-89;
67. Операции в конечном поле GF(28) (умножение, сложение и т.д.);
68. Алгоритм многораундового шифрования методом Rijndael;
69. Алгоритм раундового преобразования при шифровании Rijndael;
70. Операции раундового преобразования и их реализация;
71. Алгоритм выработки раундовых ключей при шифровании Rijndael;
72. Выработка открытого ключа для шифрования алгоритмом RSA. Алгоритм шифрования и подписывания методом RSA;
73. Определение секретного ключа по открытому ключу в алгоритме RSA. Алгоритмы определения взаимной простоты чисел (e и n) и поиска обратного элемента e-1 mod n;
74. Алгоритм поиска примитивных элементов в поле GF(P). Алгоритм Диффи-Хэллмана выработки общего секретного ключа.
75. Методы и средства защиты информации от случайных воздействий.
76. Методы защиты информации от аварийных ситуаций.
77. Признаки заражения компьютера. Основные правила защиты.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
Раздел 1. Теоретико-числовые алгоритмы в криптологии	Проработка учебного материала, выполнение лабораторных работ, решение задач (выполнение практических заданий)	12	Защита лабораторных работ, проверка решений задач
Раздел 2. Угрозы информации	Проработка учебного материала, выполнение лабораторных работ, решение задач (выполнение практических заданий)	4	Защита лабораторных работ, проверка решений задач
Раздел 3. Виды возможных нарушений безопасности информационной системы.	Проработка учебного материала, выполнение лабораторных работ, решение задач (выполнение практических заданий)	2	Защита лабораторных работ, проверка решений задач
Раздел 4. Информационная безопасность информационных систем	Проработка учебного материала, выполнение лабораторных работ, решение задач (выполнение практических заданий)	12	Защита лабораторных работ, проверка решений задач
Раздел 5. Методы и средства защиты компьютерной информации	Проработка учебного материала, выполнение лабораторных работ, решение задач (выполнение практических заданий)	6	Защита лабораторных работ, проверка решений задач

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Дискретная математика: прикладные задачи и сложность алгоритмов : учебник и практикум для вузов / А. Е. Андреев, А. А. Болотов, К. В. Коляда, А. Б. Фролов. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 317 с. — (Высшее образование). — ISBN 978-5-534-04246-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/514434
2. *Крупский, В. Н.* Теория алгоритмов. Введение в сложность вычислений : учебное пособие для вузов / В. Н. Крупский. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 117 с. — (Высшее образование). — ISBN 978-5-534-04817-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515096

дополнительная

1. Программно-аппаратные средства защиты информационных систем : учебное пособие / Ю.Ю. Громов [и др.].. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2017. — 193 с. — ISBN 978-5-8265-1737-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/85968.html
2. Пушкарев В.П. Защита информационных процессов в компьютерных системах : учебное пособие / Пушкарев В.П., Пушкарев В.В.. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2012. — 131 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/13929.html
3. *Журавлев, Ю. И.* Дискретный анализ. Формальные системы и алгоритмы : учебное пособие для вузов / Ю. И. Журавлев, Ю. А. Флеров, М. Н. Вялый. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 318 с. — (Высшее образование). — ISBN 978-5-534-06279-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513126

учебно-методическая

1. Пашинцев, В. П. Нестандартные методы защиты информации : лабораторный практикум / В. П. Пашинцев, А. В. Ляхов. — Ставрополь : Северо-Кавказский федеральный университет, 2016. — 196 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/63217.html
2. Иванцов А. М. Методические указания для выполнения лабораторных работ и самостоятельной работы студентов по дисциплине «Теоретико-числовые методы и алгоритмы, информационные технологии в автоматизированных системах» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / А. М. Иванцов; УлГУ, ФМИиАТ. - Ульяновск : УлГУ, 2021. - 39 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/10974 .

Согласовано:

Ведущий специалист НБ УлГУ / Терехина Л.А. / _____ / 04.05.2023 /
должность сотрудника научной библиотеки ФИО подпись дата

б) Программное обеспечение

Для образовательного процесса по данной дисциплине необходим стационарный класс ПК с установленным следующим программным обеспечением:
- операционная среда ОС Windows 10, Microsoft Windows Server, BaseAlt (Альт Рабочая станция, Альт сервер), Kali.

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2023]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство «ЮРАЙТ». – Москва, [2023]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО «Политехресурс». – Москва, [2023]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО «Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг». – Москва, [2023]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО «Букап». – Томск, [2023]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС «Лань». – Санкт-Петербург, [2023]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС Znanium.com : электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2023]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. / ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2023].

3. Базы данных периодических изданий:

3.1. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2023]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.2. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД «Гребенников». – Москва, [2023]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2023]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

Согласовано:

Инженер ведущий	/ Щуренко Ю.В.	/	/ 04.05.2023
Должность сотрудника УИТТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

- мультимедийные средства: компьютер и проектор;
- мультимедийные технологии. MS Office, Internet Explorer;

Аудитория для проведения занятий - 2/24б, 2/26.

Аудитория 2/24б укомплектована специализированной мебелью, учебной доской, имеются мульт мультимедийные средства: компьютер и проектор; используются мультимедийные технологии. MS Office, Internet Explorer, Power Point, MS Excel.

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться некоторые из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик: _____ доцент кафедры Иванцов Андрей Михайлович
подпись должность ФИО

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения или ссылка на прилагаемый текст изменения	ФИО заведующего кафедрой, реализующей дисциплину/выпускающей кафедрой	Подпись	Дата
1.	Утверждение РПД и ФОС для набора 2023 года (10.05.01 и 10.05.03). Актуализация РПД и ФОС для наборов 2022 года 10.05.01 и 10.05.03 (без изменений)	Андреев А.С.		12.04.2023 Протокол заседания кафедры № 12
2.	Утверждение РПД и ФОС для набора 2024 года (10.05.03). Актуализация РПД и ФОС для наборов 2023 года 10.05.01 и 10.05.03 (без изменений)	Андреев А.С.		15.04.2024 Протокол заседания кафедры № 10