Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:

Руководитель ООП

_____С.М.Дудаков

«__» _____2022 г.

Рабочая программа дисциплины (с аннотацией)

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки

09.04.03 ПРИКЛАДНАЯ ИНФОРМАТИКА

Направленность (профиль)

Интеллектуальные системы. Теория и приложения

Для студентов II курса

очная форма

Составитель: к.ф.-м.н. Кудряшов М.Ю.

Тверь, 2022

I. Аннотация

1. Цель и задачи дисциплины

Целью освоения дисциплины является:

Целью освоения дисциплины является: отражение проблематики современной криптографии, рассмотрение математических основ современных криптосистем и методов их криптоанализа, рассмотрение специфики задач, решаемых с использованием шифров с открытым ключом.

Задачами освоения дисциплины являются: изучение базовых алгоритмов симметричной и ассиметричной криптографии.

2. Место дисциплины в структуре ООП

Дисциплина относится к разделу «Профессиональный» части, формируемой участниками образовательных отношений Блока 1.

Для успешного освоения дисциплины «Математические основы защиты информации и информационной безопасности» от обучающегося требуются знания основ алгебры и навыки, необходимые для разработки, написания и отладки компьютерных программ.

Полученные знания в последующем используются при выполнении выпускной квалификационной работы, а также в дальнейшей трудовой деятельности.

3. Объем дисциплины: 6 зачетных единиц, 216 академических часов, **в том числе:**

контактная аудиторная работа: практические занятия 45 часов

самостоятельная работа: 171 час, в том числе контроль 36 часов.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
ПК-1 Способен использовать и развивать методы научных исследований и инструментарий в области искусственного интеллекта и его математических основ	ПК-1.3 Анализирует, адаптирует и совершенствует методы искусственного интеллекта для решения поставленной задачи
ПК-2 Способен выбирать, разрабатывать и проводить экспериментальную проверку работоспособности программных компонентов систем, основанных на знаниях, по обеспечению требуемых критериев эффективности и качества функционирования	ПК-2.1 Выбирает и разрабатывает программные компоненты систем, основанных на знаниях ПК-2.2 Проводит экспериментальную проверку работоспособности систем, основанных на знаниях
ПК-11 Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях	ПК-11.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях ПК-11.2 Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях

5. Форма промежуточной аттестации и семестр прохождения - экзамен, 3 семестр.

6. Язык преподавания русский**.**

II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)			Самостоятельная работа, в том числе Контроль (час.)
		Практические занятия		Контроль самостоятельной работы (в том числе курсовая работа)	
		всего	в т.ч. практическая подготовка		
Классические криптосистемы	17	3			14
Последовательности регистров сдвига	14				14
Блочные шифры	20	6			14
Элементы алгебраической геометрии. Эллиптические кривые	14				14
Вычислительные алгоритмы алгебры и теории чисел.	14				14
Система RSA и задача разложения	20	6			14
Дискретное логарифмирование в конечном поле и смежные задачи	14				14
Дискретное логарифмирование на эллиптической кривой	14				14
Шифрование с открытым ключом	29	15			14
Цифровая подпись	26	12			14
Алгебраические методы криптоанализа	17	1			16
Статистические методы криптоанализа	17	2			15
ИТОГО	216	45			171

Классические криптосистемы

1.Шифры замены.

2.Шифры перестановки.

Последовательности регистров сдвига

1.Псевдослучайные последовательности.

2.Линейные регистры сдвига с обратной связью.

3.Нелинейные алгоритмы.

4.Минимальный характеристический многочлен.

5.Алгоритм Берлекэмпа-Масси.

Блочные шифры

1.Общие принципы.

2.Режимы блочных шифров.

3.Протокол проверки идентичности.

Элементы алгебраической геометрии. Эллиптические кривые

1.Кубические кривые.

2.Касательные и точки перегиба алгебраической кривой.

3.Нормальные формы эллиптической кривой.

4.Параметризация эллиптической кривой с помощью эллиптических функций.

5.Эллиптические функции.

6.Закон сложения точек эллиптической кривой.

7.Эллиптические кривые над числовыми полями.

8.Изоморфизмы и эндоморфизмы эллиптических кривых

Вычислительные алгоритмы алгебры и теории чисел.

1.Извлечение квадратных и кубических корней в конечном поле.

2.Вычисление символа Якоби.

3.Проверка чисел и полиномов.

4.Приведение числа по модулю решетки.

5.Умножение точки эллиптической кривой на число.

6.Вычисление функции Вейля.

7.Арифметика группы классов мнимых квадратичных порядков.

Система RSA и задача разложения

1.Безопасность системы RSA и задача разложения на множители.

2.Детерминированные методы разложения.

3.Вероятностные методы разложения.

4.Атаки на систему RSA, не требующие разложения.

Дискретное логарифмирование в конечном поле и смежные задачи

1.Логарифмирование в простом поле методом решета числового поля.

2.Логарифмирование в расширенном поле.

3.Логарифмирование в группе функций Лукаша.

4.Связь между задачами Диффи-Хеллмана и дискретного логарифмирования.

Дискретное логарифмирование на эллиптической кривой

1.Универсальные методы логарифмирования.

2.Метод Гельфонда.

3.Методы встречи посередине.

4.Метол Полларда.

5.Метод встреч и на случайном дереве.

6.Сравнение сложности логарифмирования на эллиптической кривой и в конечном поле.

7.Влияние комплексного умножения на сложность логарифмирования.

8.Логарифмирование с использованием функции Вейля.

9.Время жизни параметров криптосистемы, основанной на дискретном логарифмировании.

Шифрование с открытым ключом

1.Теоретическая модель.

2.Мотивировка и общая структура.

3.Конфиденциальность.

4.Цифровая подпись.

5.Конфиденциальность и цифровая подпись.

Цифровая подпись

1.Подпись на группе трудновычислимого порядка.

2.Схема подписи RSA.

3.Схема подписи Рабина.

4.Схема подписи Фиата-Шамира.

5.Подпись на группе вычислимого порядка.

6.Схема подписи Эль-Гамаля.

7.Схема подписи Шнорра.

8.ГОСТ Р 34.10-94 и DSS.

9.Сравнительный анализ представленных схем подписи.

Алгебраические методы криптоанализа

1.Метод обобщения и редукции.

2.Метод гомоморфизмов.

3.Замкнутые и чистые шифры.

4.Вскрытие ключей замкнутых и чистых шифров.

5.Проверка шифра на замкнутость и чистоту.

6.Решеточный криптоанализ.

7.Анализ шифров с малым порядком нелинейности.

8.Криптоанализ на основе рационального продолжения полиномов Жегалкина.

9.Поиск коллизий хэш-функции.

10.Сочетание перебора и вычисления ключа.

Статистические методы криптоанализа

1.Дифференциальный криптоанализ.

2.Конечные разности.

3.Метод криптоанализа.

4.Анализ с помощью усеченных дифференциалов.

5.Анализ с помощью дифференциалов высших порядков.

6.Атака «бумеранг».

7.Криптоанализ на основе списка ключей и связанных ключей.

8.Линейный криптоанализ.

9.Анализ степенных шифров методом сдвига.

10.Генерация экстремальных подстановок для шифров.

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии
Классические криптосистемы	Практические занятия	1. Изложение теоретического материала 2. Решение задач
Последовательности регистров сдвига	Практические занятия	1. Изложение теоретического материала 2. Решение задач
Блочные шифры	Практические занятия Лабораторные занятия	1. Изложение теоретического материала 2. Решение задач
Элементы алгебраической геометрии. Эллиптические кривые	Практические занятия	3. Изложение теоретического материала 4. Решение задач
Вычислительные алгоритмы алгебры и теории чисел.	Практические занятия	1. Изложение теоретического материала 2. Решение задач
Система RSA и задача разложения	Практические занятия Лабораторные занятия	1. Изложение теоретического материала 2. Решение задач
Дискретное логарифмирование в конечном поле и смежные задачи	Практические занятия	1. Изложение теоретического материала 2. Решение задач
Дискретное логарифмирование на эллиптической кривой	Практические занятия	1. Изложение теоретического материала 2. Решение задач
Шифрование с открытым ключом	Практические занятия Лабораторные занятия	1. Изложение теоретического материала 2. Решение задач

Цифровая подпись	Практические занятия	1. Изложение теоретического материала 2. Решение задач
Алгебраические методы криптоанализа	Практические занятия	1. Изложение теоретического материала 2. Решение задач
Статистические методы криптоанализа	Практические занятия	1. Изложение теоретического материала 2. Решение задач

Преподавание учебной дисциплины строится на сочетании практических занятий, различных форм самостоятельной работы студентов. В процессе освоения дисциплины используются следующие образовательные технологии, способы и методы формирования компетенций: семинары, сопровождаемые презентациями; компьютерное тестирование; выполнение индивидуальных заданий в рамках самостоятельной работы.

Дисциплина предусматривает выполнение контрольных работ, домашних заданий на программирование, проведение и интерпретацию результатов вычислительных экспериментов.

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Для проведения текущей и промежуточной аттестации:

ПК-1 Способен использовать и развивать методы научных исследований и инструментарий в области искусственного интеллекта и его математических основ

Решение задач по основам криптоанализа

Решение задач по математическим основам обеспечения целостности информации

Имеется полное верное доказательство, включающее правильный ответ – 3 балла

Дано верное решение, но получен неправильный ответ из-за арифметической ошибки– 2 балла

Имеется верное решение части задачи из-за логической ошибки – 1 балл

Решение не дано – 0 баллов

ПК-2 Способен выбирать, разрабатывать и проводить экспериментальную проверку работоспособности программных компонентов систем, основанных

на знаниях, по обеспечению требуемых критериев эффективности и качества функционирования

Решение задач по программно-аппаратным мерам обеспечения защиты информации в компьютерных системах

Решение задач по математическим основам обеспечения целостности информации

Имеется полное верное доказательство, включающее правильный ответ – 3 балла

Дано верное решение, но получен неправильный ответ из-за арифметической ошибки– 2 балла

Имеется верное решение части задачи из-за логической ошибки – 1 балл

Решение не дано – 0 баллов

ПК-11 Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований

информационной безопасности в различных предметных областях

Решение задач по математическим основам криптографических методов защиты информации

Решение задач по применению криптографических преобразований и шифров

Имеется полное верное доказательство, включающее правильный ответ – 3 балла

Дано верное решение, но получен неправильный ответ из-за арифметической ошибки– 2 балла

Имеется верное решение части задачи из-за логической ошибки – 1 балл

Решение не дано – 0 баллов

Решение задач по математическим основам защиты информации от несанкционированного доступа

Решение задач по математическим основам обеспечения целостности информации

Имеется полное верное доказательство, включающее правильный ответ – 3 балла

Дано верное решение, но получен неправильный ответ из-за арифметической ошибки– 2 балла

Имеется верное решение части задачи из-за логической ошибки – 1 балл

Решение не дано – 0 баллов

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература

1. Информационная безопасность и защита информации: учебное пособие [Электронный рсурс]/ Е.К. Баранова, А.В. Бабаш .- 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.: 60х90 1/16. - (Высшее образование) (Переплёт) ISBN 978-5-369-01450. -Режим доступа: http://znanium.com/go.php?id=495249
2. Информационная безопасность предприятия: учебное пособие [Электронный ресурс] / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.; 60х90 1/16. - (Высшее образование: Бакалавриат). (обложка) ISBN 978-5-00091-007-8. –Режим доступа: http://znanium.com/go.php?id=491597
3. Артемов, А.В. Информационная безопасность: курс лекций / А.В. Артемов; Межрегиональная Академия безопасности и выживания. - Орел: МАБИВ, 2014. - 257 с.: табл., схем.; [Электронный ресурс]. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=428605

б) Дополнительная литература

1. Сергеева, Ю.С. Защита информации: конспект лекций: учебное пособие / Ю.С. Сергеева. - М.: А-Приор, 2011. - 128 с. - (Конспект лекций). - ISBN 978-5-384-00397-7; [Электронный ресурс]. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=72670
2. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: РИОР: ИНФРА-М, 2018. - 392 с. - (Высшее образование: Бакалавриат; Магистратура). — https://doi.org/10.12737/4868. Режим доступа: http://znanium.com/go.php?id=937469
3. Торстейнсон, П. Криптография и безопасность в технологии. NET [Электронный ресурс] / П. Торстейнсон, Г.А. Ганеш. — Электрон. дан. — Москва: Издательство "Лаборатория знаний", 2015. — 428 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=70724
4. Федин Ф.О. Информационная безопасность [Электронный ресурс]: учебное пособие/ Федин Ф.О., Офицеров В.П., Федин Ф.Ф.— Электрон. текстовые данные. — М.: Московский городской педагогический университет, 2011. — 260 с.— Режим доступа: http://www.iprbookshop.ru/26486.html
5. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс]: учебное пособие/ Спицын В.Г.— Электрон. текстовые данные. — Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011. — 148 с.— Режим доступа: http://www.iprbookshop.ru/13936.html

2) Программное обеспечение

а) Лицензионное программное обеспечение

Помещение для самостоятельной работы обучающихся: Компьютерный класс факультета ПМиК № 4б (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)	Adobe Acrobat Reader DC – Russian – бесплатное ПО; Apache Tomcat 8.0.27 – бесплатное ПО; Cadence SPB/OrCAD 16.6 - Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009; GlassFish Server Open Source Edition 4.1.1 – бесплатное ПО; Google Chrome – бесплатное ПО; Java SE Development Kit 8 Update 45 (64-bit) – бесплатное ПО; JetBrains PyCharm Community Edition 4.5.3 – бесплатное ПО; JetBrains PyCharm Edu 3.0 – бесплатное ПО; Kaspersky Endpoint Security 10 для Windows – бесплатное ПО; Lazarus 1.4.0 - бесплатное ПО; MATLAB R2012b – Акт предоставления прав № Us000311 от 25.09.2012; Mathcad 15 M010 – Акт предоставления прав ИС00000027 от 16.09.2011; Microsoft Office профессиональный плюс 2013 – Акт приема-передачи № 369 от 21 июля 2017; Microsoft SQL Server 2014 Express LocalDB - бесплатное ПО; Microsoft Visio Professional 2013 - Акт приема-передачи № 369 от 21 июля 2017; MS Visual Studio Ultimate 2013 с обновлением 4 - Акт предоставления прав № Tr035055 от 19.06.2017; MiKTeX 2.9 – бесплатное ПО; MSXML 4.0 SP2 Parser and SDK - бесплатное ПО; NetBeans IDE 8.0.2- бесплатное ПО; NetBeans IDE 8.2- бесплатное ПО; Notepad++ - бесплатное ПО; Oracle VM VirtualBox 5.0.2 - бесплатное ПО; Origin 8.1 Sr2 – договор №13918/M4 от 24.09.2009 с ЗАО «СофтЛайн Трейд»; Python 3.1 pygame-1.9.1 - бесплатное ПО; Python 3.4 numpy-1.9.2 - бесплатное ПО; Python 3.4.3 - бесплатное ПО; Python 3.5.1 (Anaconda3 2.5.0 64-bit) - бесплатное ПО; WCF RIA Services V1.0 SP2 - бесплатное ПО; WinDjView 2.1 - бесплатное ПО; MS Windows 10 Enterprise – Акт приема-передачи № 369 от 21 июля 2017.
Помещение для самостоятельной работы, учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, практики, Компьютерный класс №1 факультета ПМиК № 251 (170002, Тверская область, г.Тверь, пер. Садовый, д.35)	Adobe Acrobat Reader DC – Russian – бесплатно; Cadence SPB/OrCAD 16.6 - Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009; Google Chrome – бесплатно; Java SE Development Kit 8 Update 45 (64-bit) – бесплатно; Kaspersky Endpoint Security 10 для Windows – Акт на передачу прав №2129 от 25 октября 2016 г.; Lazarus 1.4.0 - бесплатно; Mathcad 15 M010 – Акт предоставления прав ИС00000027 от 16.09.2011; MATLAB R2012b – Акт предоставления прав № Us000311 от 25.09.2012; Microsoft Office профессиональный плюс 2013 – Акт на передачу прав № 687 от 31 июля 2018; MS Visual Studio Ultimate 2013 с обновлением 4 - Акт предоставления прав № Tr035055 от 19.06.2017;

	MiKTeX 2.9 – бесплатно; MPICH2 64-bit - бесплатно; MSXML 4.0 SP2 Parser and SDK - бесплатно; NetBeans IDE 8.0.2- бесплатно; Notepad++ - бесплатно; OpenOffice - бесплатно; Origin 8.1 Sr2 – договор №13918/M4 от 24.09.2009 с ЗАО «СофтЛайн Трейд»; Python 3.4.3 - бесплатно; Python 3.5.1 (Anaconda3 2.5.0 64-bit) - бесплатно; WCF RIA Services V1.0 SP2 - бесплатно; WinDjView 2.1 - бесплатно; Microsoft Windows 10 Enterprise – Акт на передачу прав № 687 от 31 июля 2018.

б) Свободно распространяемое программное обеспечение

Компьютерная лаборатория факультета ПМиК № 201а (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)	Перечень программного обеспечения (со свободными лицензиями): Linux OpenSuse Tumbleweed, KDE TeXLive, Mozilla Firefox TeXStudio, Qt, QtCreator Gcc, Python, Eric LibreOffice, Cervisia Kdbg, Umbrello wxMaxima, Blender digikam, GIMP Gwenview, hugin Inkscape, Okular showFoto, Kmail Konqueror, Konversation Kopete, TigerVNC viewer Amarok, K3b Kdenlive, VLC media player Kontact, Korganizer Yast, Ark Dolphin, Info Center Kget, Konsole Krusader, Midnight commander OpenJDK, pgadmin3 Xterm, Emacs Kate, Kcalc, Kgpg Kleopatra, Kompare Sweeper, Perl Apache, PostgreSQL MariaDB, SQLite, PHP

3) Современные профессиональные базы данных и информационные справочные системы

ЭБС **«ZNANIUM.COM»** www.znanium.com;

ЭБС «Университетская библиотека онлайн» https://biblioclub.ru/;

ЭБС **«Лань»** http://e.lanbook.com.

4) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-университет http://www.intuit.ru

VI. Методические материалы для обучающихся по освоению дисциплины

1. Текущий контроль успеваемости

1. Найдите ошибку в таблице

	a	b	c	d
k_1	W	X	Y	Z
k_2	Z	Y	Z	X
k_3	X	Z	W	Y
k_4	Y	W	X	Z

задающей шифрующую функцию, определенную на множестве открытых текстов $\mathbb{P} = \{a, b, c, d\}$ со значениями в шифрограммах $\mathbb{C} = \{W, X, Y, Z\}$, которая использует ключи $\mathbb{K} = \{k_1, k_2, k_3, k_4\}$.

2. Какая из величин более интересна для атакующего:

$$p(C = c|P = m) \quad \text{или} \quad p(P = m|C = c),$$

где m — открытый текст, а c — его шифрованная версия? Объясните свой ответ.

3. Какими свойствами должен обладать шифротекст, который обладает теоретико-информационной стойкостью?

4. Вспомните определение энтропии случайной величины X с распределением вероятностей $p_i = p(X = x_i)$.

5. Пусть случайная величина X принимает не более t значений. Назовите минимальное и максимальное значение энтропии $H(X)$.

6. Определите, какое из соотношений справедливы для любых шифров:

а) $H(P|K, C) = 0$,

б) $H(K, P) = H(K) + H(P)$.

Аргументируйте свой ответ.

7. Дайте определение терминов «ложный ключ» и «расстояние единственности».

8. Известно, что расстояния единственности шифров C1 и C2 равны, соответственно, n1 и n2. Какой из них предпочтительней использовать, если n1 > n2?

9. Обсудите утверждение: «ассиметричная криптография решает проблему распределения открытых ключей».

10. Покажите, что если пользователь применяет один и тот же эфемерный ключ в алгоритме DSA для подписи двух разных сообщений, то нападающий может раскрыть его долговременный секретный ключ.

11. Предположим, что $h_1 : \{0,1\}^{2n} \longrightarrow \{0,1\}^n$ — хэш-функция, защищенная от повторений. Определим

$$h_2 = \begin{cases} \{0,1\}^{4n} \longrightarrow \{0,1\}^n, \\ x_1||x_2 \mapsto h_1(h_1(x_1)||h_1(x_2)), \end{cases}$$

где $x_1, x_2 \in \{0,1\}^{2n}$. Покажите, что h_2 тоже защищена от повторений.

12. Фиксируем открытый ключ (N, E) в алгоритме RSA и определяем хэш-функцию h от сообщения M, состоящего из k блоков: $M = M_1 \dots M_k$, сопоставляющую ему элемент H_k, где $H_1 = M_1$ и

$$H_i = \left(H_{i-1}^E \pmod N\right) \oplus M_i, \quad i = 2, \dots, k.$$

Покажите, как найти повторяющиеся значения функции h.

13. Атака на функцию MAC, размер блоков и ключа в которой равен n, в идеале требует 2^n операций. Рассмотрите следующие хэш-функции, основанные на функциях MAC:

$$MAC = h(k||M), \qquad MAC = h(M||k).$$

Разработайте атаку, которая осуществляется менее чем за 2^n операций.

14. Говорят, что схема распределения ключей обладает свойством подтверждения, если каждая из сторон имеет гарантию, что ее партнер пользуется тем же ключом, что и она. Продумайте, как придать это свойство протоколу MQV.

Темы рефератов:

Применение итерированных шифров

Применение хэш-функций

Криптоанализ с помощью слайдовой атаки

Криптографические протоколы

Криптосистемы на гиперэллиптических кривых

Системы разделения секрета

Системы, основанные на задаче о рюкзаке

Системы, основанные на теории кодирования

Системы, основанные на RSA

Итоговая оценка складывается из оценки текущей работы студентов на практических и лабораторных занятиях, выполнения индивидуальных заданий и оценки за выполнение студентом учебного задания.

В первом этапе рассматриваются следующие вопросы учебной дисциплины:

Классические криптосистемы, Последовательности регистров сдвига. Блочные шифры. Элементы алгебраической геометрии. Эллиптические кривые. Вычислительные алгоритмы алгебры и теории чисел. Система RSA и задача разложения.

В втором этапе рассматриваются следующие вопросы учебной дисциплины:

Дискретное логарифмирование в конечном поле и смежные задачи. Дискретное логарифмирование на эллиптической кривой. Шифрование с открытым ключом. Цифровая подпись. Алгебраические методы криптоанализа. Статистические методы криптоанализа.

Задания:

1. Криптоанализ криптограмм методом частотного анализа
2. Криптоанализ криптограмм методом вероятных слов
3. Криптоанализ аддитивных шифров
4. Реализовать алгоритмы блочного шифрования данных ГОСТ и AES
5. Реализовать шифрование, расшифрование данных в RSA
6. Линейный криптоанализ блочных алгоритмов шифрования
7. Дифференциальный криптоанализ блочных алгоритмов шифрования

Вопросы к экзамену:

Шифрование — симметричные методы

Шифрование — асимметричные методы

Битовая стойкость основных криптографических функций с открытым ключом

Методы защиты целостности данных

Протоколы аутентификации — принципы

Протоколы аутентификации — реальный мир

Аутентификация в криптографии с открытым ключом

Определения формальной и сильной стойкости криптосистем с открытым ключом

Доказуемо стойкие и эффективные криптосистемы с открытым ключом

Сильная и доказуемая стойкость схем цифровой подписи

Формальные методы анализа протоколов аутентификации

Криптографические протоколы

VII. Материально-техническое обеспечение

Для аудиторной работы

Компьютерная лаборатория факультета ПМиК № 201а (170002, Тверская обл., г.Тверь, Садовый переулок, д.35)	Персональные ЭВМ (компьютер ПЭВМ "ХОПЕР" IS09001: 1.1/Intel Core i3-540/IntelH55-MLX/Hynix-11.4/DVD RW Sony/Монитор 21,5" AOC TFT/клавиатура/мышь – 10 штук), системный блок BASE P4 3200MHz 800 512K/1024 Mb DDR400/400Gb, концентратор сетевой DFE-916 DX HUB 16x10/100.
Помещение для самостоятельной работы, учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, практики, Компьютерный класс №1 факультета ПМиК № 251	Набор учебной мебели, персональные ЭВМ (Компьютер iRU Corp 510 I5-2400/4096/500/G210-512/DVD-RW/W7S/монитор E-Machines E220HQVB 21.5" – 10 штук).

(170002, Тверская область, г.Тверь, пер. Садовый, д.35)	

Для самостоятельной работы

Помещение для самостоятельной работы обучающихся: Компьютерный класс факультета ПМиК № 4б (170002, Тверская обл., г.Тверь, Садовый пер., д.35)	Персональные ЭВМ (компьютер RAMEC STORM C2D 4600/160Gb/DVD-RW+Монитор LG TFT 17" L1753S-SF silver – 24 шт.), мультимедийный проектор BenQ MP 724 с потолочным креплением и экран 1105, кондиционер General Climate – 2 шт., коммутатор D-Link 10/100/1000mbps 16-potr DGS-1016D, коммутатор D-Link 10/100/1000mbps 16-potr DGS-1016D- 2 шт.

VIII. Сведения об обновлении рабочей программы дисциплины

№ п.п.	Обновленный раздел рабочей программы дисциплины	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения
1.			
2.			
3.			
4.			
5.			