МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАДЖИКИСТАН
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ»

«Утверждаю»
Декан ЕНФ Махмадбегов Р. С.
«___» _____ 2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ «Криптографические методы защити информации»

Направление подготовки - 09.03.03 «Прикладная информатика»

Профиль – Инженерия программного обеспечения

Форма подготовки - очная

Уровень подготовки - бакалавриат

ДУШАНБЕ – 2023

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ

о т 12 марта 2015г. № 207

При разработке рабочей программы учитываются:

требования работодателей, профессиональных стандартов по направлению / специальности (при наличии);

содержание программ дисциплин, изучаемых на предыдущих и последующих этапах обучения;

новейшие достижения в данной предметной области.

Рабочая программа обсуждена на заседании кафедры Информатики и ИТ, протокол № 1 от 29 августа 2023 г.

Рабочая программа утверждена УМС естественнонаучного факультета, протокол №1 от 30 08 2023 г.

Рабочая программа утверждена Ученым советом естественнонаучного факультета, протокол № 1 от 31 08 2023г.

Заведующий кафедрой, к.э.н., доцент _____ Лещукович А.И.

Зам. председателя УМС факультета, к.э.н., доцент _____ Абдулхаева Ш.Р.

Разработчик, к.ф.-м.н., доцент: _____ Зимонов М.З.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Криптографические методы защиты информации (КМЗИ)» изучается студентами 4-го курса направления 09.03.03 «Прикладная информатика (уровень бакалавриата)».

1.1. Цели изучения дисциплины

Заложить методически правильные основы знаний по КМЗИ, необходимые специалистам, занимающимся вопросами проектирования, внедрения и эксплуатации корпоративных вычислительных и информационных систем (ВС/ИС). Дисциплина является важной составной частью теоретической подготовки специалиста по прикладной информатике и занимает существенное место в его будущей практической деятельности. Она обеспечивает возможность эффективной работы специалиста в ИТ-службах предприятий и государственных учреждений.

Преподавание дисциплины «Криптографические методы защити информации» имеет следующие базовые задачи:

- дать будущим специалистам необходимые для их работы теоретические знания о современных средствах, методах и технологиях обеспечения информационной безопасности ВС/ИС;
- сформировать у студентов практические навыки организации работ по обеспечению информационной безопасности на предприятиях.

1.2. Задачи изучения дисциплины

Задачи дисциплины формулируются в соответствии с требованиями ФГОС, предъявляемые к компетенциям обучающегося. В результате освоения дисциплины КМЗИ формируются определенный набор компетенции обучающегося:

1) Универсальные компетенции выпускников и индикаторы их достижения

Код	Формируемая компетенция	Содержание этапа формирования компетенции	Форма контроля
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	**Знать:** принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач.	устный опрос
		Уметь: принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач.	устный опрос
		Владеет: навыками научного поиска и практической работы с информационными источниками; методами принятия решений	устный опрос

2) Общепрофессиональные компетенции выпускников и индикаторы их достижения

Код	Формируемая компетенция	Содержание этапа формирования компетенции	Форма контроля
ОПК-1	Способен применять естественнонаучные и общеинженерные знания,	**Знать:** основы математики, физики, вычислительной техники и программирования.	устный опрос
		Умеет: решать стандартные профессиональные задачи с применением	Эссе

	методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования	
		Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности	устный опрос
ОПК-6	Способен анализировать и разрабатывать организационно- технические и экономические процессы с применением методов системного анализа и математического моделирования	**Знать:** - основы теории систем и системного анализа, дискретной математики, теории вероятностей и математической статистики, методов оптимизации и исследования операций, нечетких вычислений, математического и имитационного моделирования.	устный опрос
		Умеет: - применять методы теории систем и системного анализа, математического, статистического и имитационного моделирования для автоматизации задач принятия решений, анализа информационных потоков, расчета экономической эффективности и надежности информационных систем и технологий.	к/работа
		Владеть: - навыками проведения инженерных расчетов основных показателей результативности создания и применения информационных систем и технологий.	устный опрос

3) Профессиональные компетенции: проектная деятельность:

Код	Формируемая компетенция	Содержание этапа формирования компетенции	Форма контроля
ПК-5	Способность моделировать прикладные (бизнес) процессы и предметную область.	**Знать:** - способы организации розничной торговли в Интернет; модели организации закупок через Интернет; основные группы услуг, оказываемых через Интернет и особенности их оказания; способы оплаты товаров и услуг в электронной коммерции; методологические основы планирования бизнеса; основные методы и технологию бизнес-планирования; место и роль бизнес-плана при управлении компаниями; методические особенности составления различных типов бизнес-планов используемых при управлении бизнесом; основные классы систем электронной коммерции; способы организации розничной торговли в Интернет; основные методы стиму-	эссе

		лирования продаж в Интернет-магазине; модели организации закупок через Интернет; основные группы услуг, оказываемых через Интернет и особенности их оказания; способы оплаты товаров и услуг в электронной коммерции; Российское, таджикское и международное законодательство в области электронной коммерции.	
		Уметь:- использовать навыки менеджера в процессе управления проектной группой с использованием ИКТ; использовать методы современного бизнес-планирования как базовой технологии управления бизнесом; составлять различные разделы бизнес-планов; проводить анализ деятельности предприятия и выявлять участки производства, нуждающиеся в реинжиниринге; осуществлять сбор и подготовку аналитических данных для оценки эффективности рекламы в Интернет; изучать и анализировать методы предоставления различных услуг в Интернет; создавать веб-страницы и сайты, в том числе с активным содержимым, создавать графический материал для наполнения страниц, готовить текстовый материал для размещения на странице, настраивать программное обеспечение веб-серверов.	устный опрос
		Владеть: - методикой составления управленческого бизнес-плана; инструментами создания бизнес-моделей и моделирования новых бизнес-процессов; средствами для разработки веб-приложений	к/работа

2.МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Курс дает базовую основу для понимания, анализа и оценки основных проблем, связанных с обеспечением КМЗИ предприятия и защитой информации, а также разработкой, внедрением и сопровождением средств информационной защиты.

Курс подготавливает выпускника к работе в современной компании, внедряющей, использующей или разрабатывающей программные средства для обеспечения информационной безопасности. Она является дисциплиной по выбору студента общенаучного цикла, изучается в 7 семестре. Логически и содержательно-методически взаимосвязана с дисциплинами ООП, указанных в табл. 1:

Таблица 1

№	Название дисциплины	Семестр	Место дисци-

			плины в структуре ООП
1.	Математика	1-2	Б1.Б.5
2.	Дискретная математика	1	Б1.Б.6
3.	Теория алгоритмов	2	Б1.В.ОД.10
4.	Теория вероятности и математическая статистика	2	Б1.Б.9
5.	Операционные системы	2	Б1.Б.13
6.	Информатика и программирование	1-3	Б1.Б.8
7.	Практикум по программированию	2-4	Б1.В.ОД.9
8.	Базы данных	3-4	Б1.Б.18
9.	Вычислительные системы сети и телекоммуникации	3-4	Б1.Б.12
10.	Разработка программных приложений/ Системное и прикладное программное обеспечение	4	Б1.В.ДВ.9
11.	Программная инженерия	4-5	Б1.Б.14
12.	Интеллектуальные информационные системы	5	Б1.В.ОД.14
13.	Программирование в среде C++/ Программирование в среде QBasic /Pascal/Delphi	7	Б1.В.ДВ.2
14.	Интернет-программирование/ Java-технологии	7	Б1.В.ДВ.4
15.	Проектирование ИТ структуры предприятия	7	Б1.В.ОД.13
16.	Управление программными проектами	7-8	Б1.В.ОД.12
17.	Информационное безопасности	7	Б1.Б.19

При освоении данной дисциплины необходимы умения и готовность («входные» знания) обучающегося по дисциплинам 1-5, указанных в Таблице 1. Дисциплины 6 и 7 относятся к группе «входных» знаний, вместе с тем определенная их часть изучается параллельно с данной дисциплиной («входные-параллельные» знания).

Дисциплины 11-12 взаимосвязаны с данной дисциплиной, они изучаются параллельно.

Теоретическими дисциплинами и практиками, для которых освоение данной дисциплины необходимо как предшествующее являются:13-16.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных единиц, всего 108 часов, из которых: лекции 16 часов, практические занятия 16 часов, КСР – 8 часов, всего часов аудиторной нагрузки - 90 часов, в том числе в интерактивной форме 32 часа (16 ч.- лекции, 16 ч. - практические занятия), самостоятельная работа – 68 часов.

Экзамен – 7-й семестр

№ п/п	Раздел Дисциплины	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Литература
		Лек.	Пр.	Лаб.	КСР	
	7 семестр					
1.	**Тема 1. Виды криптографических преобразований информации.** Основные понятия и определения криптографии. Принципы криптографической защиты информации. История развития криптографии. Шифрующие криптографические преобразования. Односторонние функции. Хэш - функции.	2				1,3,5,7

	Электронная цифровая подпись. Генераторы псевдослучайных последовательностей. Шифры перестановки. Шифры замены (подстановки). Шифры гаммирования. Композиционные блочные шифры и принципы их построения. Криптоанализ и виды криптоаналитических атак. **Практическая работа** Выполнение и подготовка к защите работы 1 Групповые консультации по теме 1		2		2	
	Тема 2. Алгоритмы симметричного шифрования. Основные понятия, относящиеся к алгоритмам симметричного шифрования: ключ шифрования, plaintext, ciphertext. Определение стойкости алгоритма, типы операций, используемые в алгоритмах симметричного шифрования. Сеть Фейштеля. Основные понятия криптоанализа, линейный и дифференциальный криптоанализ. Схема шифрования алгоритма DES. Режимы использования DES. Криптостойкость алгоритма DES. Увеличение криптостойкости DES **Практическая работа** Выполнение и подготовка к защите работы 1-2 Групповые консультации по теме 1	4	4		2	1,5,
	Тема 3. Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра. Описание AES. Алгоритм обработки ключа. Варианты алгоритма. Криптостойкость. **Практическая работа** Выполнение и подготовка к защите работы 3-5 **Практическое занятие**	2	4		1	2,6
	Тема 4. Хэш-функции и аутентификация сообщений. Основные понятия, относящиеся к обеспечению целостности сообщений с помощью MAC и хэш-функций; представлены простые хэш-функции и сильная хэш-функция MD5. Сильные хэш-функции SHA-1, SHA-2 и ГОСТ 3411. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC **Практическая работа**	2	2		1	1,3,7

	Выполнение и подготовка к защите работы 6-7					
2.	**Тема 5. Цифровая подпись**. Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS. **Практическая работа** Выполнение и подготовка к защите работы 8 Групповые консультации по темам 4-5	2	2		2	2,4,8
3.	**Тема 6. Криптография с использованием эллиптических кривых**. Математические понятия, связанные с эллиптическими кривыми, в частности задача дискретного логарифмирования на эллиптической кривой. Аналог алгоритма Диффи - Хеллмана на эллиптических кривых, алгоритма шифрования с открытым ключом получателя на эллиптических кривых. **Практическая работа** Выполнение и подготовка к защите работы 9 Групповые консультации по темам 5	4	4		2	1,3,5
	Итого по семестру	**16**	**16**		**8**	

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

4.1. План-график выполнения самостоятельной работы по дисциплине КМЗИ (вопросы приведены в приложении 1)

№ п/п	Объем СРС в ч.	Тема самостоятельной работы	Форма и вид результатов самостоятельной работы	Форма контроля
1	7	Общие вопросы информационной безопасности. Основные понятия и определения. Законодательство РФ и РТ в области информационной безопасности.	Конспект, реферат	Опрос
2	7	Разработка алгоритма и пакета программы шифрования и расшифрования шифра замены.	Презентация, программа	Опрос
3	7	Разработка алгоритма и пакета программы шифрования и расшифрования шифра перестановки.	Презентация, доклад	Выступление
4	7	Разработка алгоритма и пакета программы шифрования и расшифрования системы с открытым ключом.	Презентация, программа	Выступление
5	7	Разработка алгоритма и пакета программы для элементов теории чисел.	Конспект, программа	Опрос

6	7	Разработка алгоритма и пакета программы шифрования и расшифрования шифра метода DES	Конспект, программа	Опрос
7	6	Разработка алгоритма и пакета программы шифрования и расшифрования метода AES	Презентация, программа	Опрос
8	4	Разработка алгоритма и пакета программы шифрования и расшифрования аналога алгоритма Диффи - Хеллмана на эллиптических кривых.	Презентация, программа	Выступление
9	4	Разработка алгоритма и пакета программы шифрования и расшифрования метода эль-Гамаля на эллиптических кривых.	Презентация, программа	Опрос

4.2. Характеристика заданий для самостоятельной работы и методические рекомендации по их выполнению

Для выполнения задания, прежде всего, необходимо ознакомиться и изучить основные положения теоретических материалов соответствующей темы из литературных источников. Они указаны в разделе 3 «Содержание и структура дисциплины».

Текущая самостоятельная работа включает следующие виды работ:

- работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданному вопросу;
- изучение тем, вынесенных на самостоятельную проработку;
- подготовка к практическим занятиям и КСР;
- подготовка к промежуточному контролю, зачету, экзамену.

Творческая проблемно-ориентированная самостоятельная работа студентов ориентирована на развитие интеллектуальных умений, комплекса общекультурных и профессиональных компетенций, повышения творческого потенциала студентов и включает в себя следующие виды работ по основным проблемам курса:

- поиск научных источников, анализ деятельности современных предприятий и организаций с целью разработки их стратегии развития;
- решение соответствующих тестов по изучаемым темам;
- исследовательская работа и участие в научных студенческих конференциях, семинарах и олимпиадах.

4.3. Требования к представлению и оформлению результатов самостоятельной работы

Для этого студентам данного направления как очной, так и заочной форм обучения необходимо посещать лекционные, практические (семинарские) занятия и КСР. Внимательно прослушивая лекции, самостоятельно готовясь к обсуждению тем, необходимо активно участвовать в дискуссиях на занятиях и сдать своевременно самостоятельные работы. Студентам рекомендуется уделить особое внимание выполнению самостоятельной работы в виде решения задач, тестов и примеров на практических занятиях и защите своих позиций по рассмотрению конкретных ситуаций при сдаче самостоятельных работ. Кроме того, студентам заочного отделения необходимо при выполнении контрольной работы по самостоятельно выбранной теме, изучить перечень рекомендуемой литературы и на примере деятельности современных предприятий и организаций рассмотреть конкретную ситуацию. При этом основой для изучения дисциплины являются изучение необходимой литературы, конспекты лекций и результаты практических занятий, КСР. В частности, выполнение самостоятельной

работы студентов заключается в решении тестов, рассмотрении конкретных ситуаций из практической деятельности современных организаций и предприятий. Выполненную самостоятельную работу студенты на практическом занятии и в процессе КСР будут обсуждать вместе с группой и преподавателям. Практические занятия и КСР должны следовать после окончания изучения лекционного материала, где проводится опрос студентов по составленным контрольным вопросам темы (приведены ниже) с целью оценки уровня освоенных тем при изучении данной дисциплины.

4.4. Критерии оценки выполнения самостоятельной работы

В основу разработки балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется постоянно в процессе его обучения в университете. Настоящая система оценки успеваемости студентов основана на использовании совокупности контрольных точек, равномерно расположенных на всем временном интервале изучения дисциплины. При этом предполагается разделение всего курса на ряд более или менее самостоятельных, логически завершенных блоков и модулей и проведение по ним промежуточного контроля.

Студентам выставляются следующие баллы за выполнение задания к ПК:

- **оценка «отлично» (10 баллов)** выставляется студенту, если реферат выполнен в соответствии с требованиями, затронуты все вопросы касающиеся темы, а также студент отвечает уверенно;
- **оценка «хорошо» (8-9 баллов)** выставляется студенту, если реферат выполнен в соответствии с требованиями, затронуты все вопросы касающиеся темы, но студент отвечает не уверенно;
- **оценка «удовлетворительно» (6-7 баллов)** выставляется студенту, если реферат выполнен в соответствии с требованиями, не затронуты все вопросы касающиеся темы и студент отвечает не уверенно;
- **оценка «неудовлетворительно» (5 и ниже)** выставляется студенту, если реферат не выполнен в соответствии с требованиями, не затронуты все вопросы касающиеся темы, студент не может отвечает вообще, не проявлена самостоятельность при выполнении реферата, реферат скачан из интернета.

Текущий контроль осуществляется в ходе учебного процесса по результатам выполнения самостоятельной работы и контрольной работы.

Основными формами текущего контроля знаний являются:

- обсуждение вынесенных в планах практических занятий лекционного материала и контрольных вопросов;
- решение тестов и их обсуждение с точки зрения умения сформулировать выводы, вносить рекомендации и принимать адекватные управленческие решения;
- выполнение контрольной работы и обсуждение результатов;
- участие в дискуссиях в качестве участника и модератора групповой дискуссии по темам дисциплины;
- написание и презентация доклада;
- написание самостоятельной (контрольной) работы.

Для контроля усвоения данной дисциплины учебным планом предусмотрен экзамен. Общее количество баллов по дисциплине – 100 баллов. Распределение баллов на текущий и промежуточный контроль освоения дисциплины, а также итоговой оценки представлено ниже.

	Недели		РК 1	Недели		РК 2	Адм.	ИК	ВСЕГО
	1-4	5-8		9-13	14-17		баллы		
Баллы	9	12	10	12	12	10	5	30	100

5. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

1. Кардашова, И. Б. Основы теории национальной безопасности [Текст]: учебник для вузов / И. Б. Кардашова. — Москва: Издательство Юрайт, 2019. — 303 с. — URL: https://biblio-online.ru/bcode/438881
2. Бартош, А. А. Основы международной безопасности. Организации обеспечения международной безопасности [Текст]: учебное пособие для бакалавриата и специалитета / А. А. Бартош. — Москва : Издательство Юрайт, 2019. — 247 с. — (Высшее образование). — ISBN 978-5-534-05426-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/441405
3. *Лось, А. Б.* Криптографические методы защиты информации[Электронный ресурс]: учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва: Издательство Юрайт, 2019. — 473 с. — URL: https://biblio-online.ru/bcode/431164.
4. *Нестеров, С. А.* Информационная безопасность[Электронный ресурс]: учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва: Издательство Юрайт, 2019. — 321 с. — URL: https://biblio-online.ru/bcode/442312.
5. *Нестеров, С. А.* Информационная безопасность[Электронный ресурс]: учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва: Издательство Юрайт, 2019. — 321 с.— URL: https://biblio-online.ru/bcode/434171

5.2. Дополнительная литература

6. *Трофимов, В. В.* Алгоритмизация и программирование [Электронный ресурс]: учебник для академического бакалавриата / В. В. Трофимов, Т. А. Павловская ; под редакцией В. В. Трофимова. — Москва: Издательство Юрайт, 2019. — 137 с. —URL: https://biblio-online.ru/bcode/423824
7. *Фомичёв, В. М.* Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты[Электронный ресурс]: учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва: Издательство Юрайт, 2019. — 209 с.— URL: https://biblio-online.ru/bcode/433420.
8. *Фомичёв, В. М.* Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты[Электронный ресурс]: учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва: Издательство Юрайт, 2019. — 245 с.— URL:

5.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://www.iprbookshop.ru
2. http://www.metod-kopilka.ru/page-2-2-6-10.html
3. www.algolist.manual.ru
4. www.cryptography.ru
5. www.intuit.ru
6. www.securitylab.ru
7. www.5-tv.ru/
8. https://xakep.ru
9. www.pikabu.ru
10. www.cryptocom.ru

5.4. Перечень информационных технологий и программного обеспечения

Используются лицензионное программное обеспечение ОС Windows -7 и программное обеспечение открытого доступа (Open source), среды программирования (Microsoft C++/C#, Java и др.)

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Студенты, изучающие курс «Криптографические методы защити информации», должны в первую обратить внимание на общие подходы к реализации информационной безопасности современного предприятия. Здесь следует обратить особое внимание на то, что в переходный период к построению информационного общества информационные ресурсы становятся востребуемым продуктом, имеющим высокую потребительскую ценность. Отсюда следует объективная необходимость развития мер защиты информации и данных. Для свободной ориентации в информационном пространстве современного общества специалист любого профиля должен уметь получать, грамотно обрабатывать и использовать информацию с помощью средств вычислительной техники и телекоммуникаций.

Студенты должны знать общие подходы к построению защищенной информационной или вычислительной системы. Основным моментом этого раздела следует считать системный подход формированию моделей угроз, общей модели информационной защиты, модели политики ИБ и структуре документов в сфере ИБ современного предприятия. Для каждого вида угроз необходимо выстраивать цепочку: <вид угрозы> - <оценка риска реализации> - <оценка достаточности средств защиты> - <компенсация возможного ущерба>.

Студенты должны знать стандарты информационной безопасности. Развитие семейства стандартов следует рассматривать в контексте развития информационных технологий в целом. При этом особое внимание следует обратить на построение системы оценки рисков, которая является одной из основных составляющих общей системы безопасности. Здесь необходимо достаточно подробно рассматривать содержание современных стандартов обеспечения ИБ и информационных рисков.

Студенты должны уметь использовать современные технологии и инструменты информационной безопасности. Важным аспектом является то, что вследствие быстрого развития ИТ постоянно изменяются методы и технологии работы с информацией, появляются способы проникновения в информационные системы предприятия, а также всё новые и новые семейства вирусов. Всё это приводит к необходимости постоянного совершенствования защиты информационной инфраструктуры предприятия и необходимости построения комплексной информационной защиты ПО.

Основа для изучения дисциплины «Криптографические методы защити информации» - конспекты лекций, результаты лабораторных занятий и выполненные самостоятельные работы самыми студентами.

На лабораторных занятиях с использованием средств вычислительной техники студенты выполняют задания, предусмотренные для приобретения пользовательских навыков, решают задачи вычислительного характера, устанавливают и настраивают программные продукты, разрабатывают алгоритмы и программы для решения прикладных задач, выполняют типовые расчеты. Во время самостоятельной работы студента с преподавателем обсуждаются проблемные лекции, решаются сложные алгоритмы.

Все это может дать положительный результат, если студент активно занимается самостоятельной работой в соответствии с планом-графиком п.4.1. Процесс выполнения СРС с описанием этапов решения примерной задачи описан в п.4.2

Вместе с тем основой обучения являются аудиторные занятия - лекции, практические занятия и лабораторные работы по рассмотрению проблем информационной технологии и решению конкретных задач защиты информации. Поэтому рассмотрим каждую тему отдельно, чтобы указать на какие моменты обратить внимания, чтобы лучше освоить материал темы.

Тема 1. Виды криптографических преобразований информации. Основные понятия

и определения криптографии. Принципы криптографической защиты информации. История развития криптографии. Шифрующие криптографические преобразования. Односторонние функции. Хэш - функции. Электронная цифровая подпись. Генераторы псевдослучайных последовательностей. Шифры перестановки. Шифры замены (подстановки). Шифры гаммирования. Композиционные блочные шифры и принципы их построения. Криптоанализ и виды криптоаналитических атак.

Тема 2. Алгоритмы симметричного шифрования. Основные понятия, относящиеся к алгоритмам симметричного шифрования: ключ шифрования, plaintext, ciphertext. Определение стойкости алгоритма, типы операций, используемые в алгоритмах симметричного шифрования. Сеть Фейштеля. Основные понятия криптоанализа, линейный и дифференциальный криптоанализ. Схема шифрования алгоритма DES. Режимы использования DES. Криптостойкость алгоритма DES. Увеличение криптостойкости DES

Тема 3. Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра. Описание AES. Алгоритм обработки ключа. Варианты алгоритма. Криптостойкость.

Тема 4. Хэш-функции и аутентификация сообщений. Основные понятия, относящиеся к обеспечению целостности сообщений с помощью MAC и хэш-функций; представлены простые хэш-функции и сильная хэш-функция MD5. Сильные хэш-функции SHA-1, SHA-2 и ГОСТ 3411. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC.

Тема 5. Цифровая подпись. Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS.

Тема 6. Криптография с использованием эллиптических кривых. Математические понятия, связанные с эллиптическими кривыми, в частности задача дискретного логарифмирования на эллиптической кривой. Аналог алгоритма Диффи - Хеллмана на эллиптических кривых, алгоритма шифрования с открытым ключом получателя на эллиптических кривых.

Необходимо подкрепить все теоретические материалы решением конкретных задач как во время практических занятий и лабораторных работ, так и в процессе самостоятельной подготовки.

7. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Промежуточная аттестации осуществляется: для зачета – контрольная работа и опрос. Экзамен проводится в форме тестирования.

Текущий контроль студентов осуществляется путем защиты лабораторных работ, выполнения задания, обсуждения теоретических вопросов

Контролирующие материалы по дисциплине содержат:

Контрольные вопросы и задания для текущего контроля знаний по дисциплине (Приложение 1);

Тестовые задания для промежуточного контроля знаний по дисциплине (Приложение 2);

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины при кафедре информатики и ИС РТСУ имеются 5 компьютерных классов, 2 из которых обеспеченны электронными досками. В трех компьютерных классах реализованы облачные технологии на базе блейд-серверной системы.

9 **Контрольные вопросы к экзамену по дисциплине «Криптографические методы защиты информации».**

1. Основные понятия и определения информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности. Классификация атак. Модели сетевой безопасности и безопасности информационной системы.
2. Классическая задача криптографии. Угрозы со стороны злоумышленника и участников процесса информационного взаимодействия.
3. Шифры замены и перестановки. Моно- и многоалфавитные подстановки. Шифры Цезаря, Виженера, Вернама. Методы дешифрования.
4. Классификация методов дешифрования. Модель предполагаемого противника. Правила Керкхоффа.
5. Совершенная секретность по Шеннону. Примеры совершенно секретных систем. Шифр Вернама. Понятие об управлении ключами.
6. Блочные криптосистемы с секретным ключом. Алгоритм DES. Описание DES. Основные этапы алгоритма.
7. Схема алгоритма DES. Раунд алгоритма. Преобразование ключа.
8. Алгоритм DES. Подстановка с помощью S-блоков. Расшифрование в DES.
9. Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра.
10. Алгоритм RSA. Математическая модель алгоритма. Стойкость алгоритма.
11. Криптосистема Эль-Гамаля.
12. Однонаправленные (односторонние) функции с секретом и их применение.
13. Основы криптоанализа. Обзор возможных вариантов криптоанализа. Метод вскрытия «встреча посередине». Вскрытие со словарем. Вскрытие системы Вижинера, использующей простой XOR. Метод бесключевого чтения RSA. Атака на подпись RSA по выбранному шифротексту. Вскрытие хэш-функций с использованием парадокса дня рождения.
14. Криптосистемы на эллиптических кривых.

Приложение 1

КОНТРОЛЬНЫЕ ЗАДАНИЯ И ВОПРОСЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ЗНАНИЙ ПО ДИСЦИПЛИНЕ (ДЛЯ ТЕКУЩЕЙ АТТЕСТАЦИИ И КОНТРОЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ)

Вопросы

1. Определение безопасности. Объекты, изучаемые информационной безопасности.
2. Информация. Единицы измерения информации. Виды информации.
3. Способы представление и защиты информации.
4. Аппаратная архитектура компьютеров. Основные устройства и их назначение.

5. Угрозы информации.
6. Метод Диффи- Хеллмана.
7. Математические методы защиты информации.
8. Защита информации от случайных угроз.
9. Представление информации на ЭВМ.
10. Понятие о системах счисления.
11. Атрибутивные способы идентификации. Виды пластиковых карт.
12. Классификация чисел.
13. Метод Эйлера. Теорема Ферма (малая)
14. Правовая защита информации.
15. Характеристики защитных действий информации.
16. Программные средства защиты информации.
17. Защитные действия по масштабу.
18. Компьютерные вирусы: классификация.
19. Управление доступом.
20. Компьютерные вирусы: классификация.
21. Шифрование и дешифрование информаций.
22. Криптографические методы защиты информации, ее составляющие и классификации.
23. Основные виды защищаемой информации.
24. Проблемы информационной безопасности в мировом сообществе.
25. Методы защиты информации. Защита информации в локальных компьютерных сетях.
26. Шифрование и дешифрование информаций на ЭК.
27. Международные и отечественные стандарты безопасности информации.