МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ:
Директор института
Энергетики и автоматизированных систем
_____ С.И. Лукьянов
«20» сентября 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем
шифр наименование направления подготовки (специальности)

Направленность (профиль/ специализация) программы
Обеспечение информационной безопасности распределенных информационных систем
наименование направленности (профиля) подготовки (специализации)

Уровень высшего образования
специалитет

Форма обучения
очная

Институт	Энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	7,8

Магнитогорск
2017 г.

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры
Информатики и информационной безопасности
(наименование кафедры - разработчика)

«03» марта 2017 г., протокол № 10.

Зав. кафедрой _____ / И.И. Баранкова/
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией
института Энергетики и автоматизированных систем
(наименование факультета (института) - исполнителя)

«14» марта 2017 г., протокол № 6.

Председатель _____ / С.И. Лукьянов/
(подпись) (И.О. Фамилия)

Рабочая программа составлена: зав.кафедрой ИиИБ, д.т.н., профессор
(должность, ученая степень, ученое звание)

_____ / И.И. Баранкова /
(подпись) (И.О. Фамилия)

Рецензент: зав. кафедрой Бизнес-информатики
и информационных технологий, к.п.н. профессор
(должность, ученая степень, ученое звание)

_____ / Г.Н. Чусавитина/
(подпись) (И.О. Фамилия)

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата, № протокола заседания кафедры	Подпись зав. кафедрой
1.	7	Переработка фонда оценочных средств	№1 от 07.09.2018	
2.	8	Обновление списка основной и дополнительной литературы	№1 от 07.09.2018	
3.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
4.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
5.	7	Переработка фонда оценочных средств	№1 от 04.09.2020	
6.	8	Обновление списка основной и дополнительной литературы	№1 от 04.09.2020	

1. Цели освоения дисциплины

Целью дисциплины «Криптографические методы защиты информации» является ознакомление обучающихся с основным понятиям криптографии; моделям шифров и математическим методам их исследования; требованиям, предъявляемым к шифрам и основным характеристикам шифров; основополагающими принципами защиты информации на основе криптографических методов; криптографическими стандартами и их использовании в информационных системах; с реализацией криптографических методов на практике; в соответствии с требованиями ФГОС ВО для специальности 10.05.03 «Информационная безопасность автоматизированных систем».

2. Место дисциплины в структуре ООП подготовки специалиста

Дисциплина «Криптографические методы защиты информации» входит в базовую часть блока 1 образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин «Основы информационной безопасности», «Математическая логика и теория алгоритмов», «Информатика», «Математический анализ», «Программно-аппаратные средства обеспечения информационной безопасности», «Технологии и методы программирования», «Языки программирования».

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплины «Алгоритмы шифрования информации», учебной и производственной практик.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Криптографические методы защиты информации» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-14 - способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	
Знать:	• Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Классификацию криптографических средств защиты информации. • методы шифрования, использующие классические симметричные алгоритмы, • методы шифрования, использующие классические алгоритмы моноалфавитной и многоалфавитной подстановки и перестановки для защиты текстовой информации, • методы шифрования (расшифрования) перестановкой символов, подстановкой, гаммированием, использованием таблицы Виженера. • общие принципы действия шифровальной машины Энигма • общие принципы шифрования, используемые в алгоритме симметричного шифрования AES • принципы шифрования информации с помощью биграммного шифра Плейфера

Структурный элемент компетенции	Планируемые результаты обучения
	• Способы контрольных проверок работоспособности применяемых криптографических средств защиты информации.
Уметь:	• исследовать различные методы защиты текстовой информации и их стойкости на основе подбора ключей • Участвовать в настройке криптографических средств обеспечения информационной безопасности. • Самостоятельно настраивать криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств ЗИ. • Применять криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств обеспечения ИБ.
Владеть:	• Техникой настройки криптографических средств обеспечения информационной безопасности. • Навыками использования криптографических средств обеспечения информационной безопасности автоматизированных систем. • Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.
ОПК-2 – способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники	
Знать:	• математический аппарат теории информации, теории алгоритмов • процессы генерации простых чисел для систем ассиметричного шифрования • процессы постановки и верификации ЭЦП • математический аппарат шифра скользящей перестановки • принцип работы сети Фейстеля как базовым преобразованием симметричных блочных криптосистем
Уметь:	• корректно применять при решении профессиональных задач математический аппарат теории алгоритмов, теории информации, в том числе с использованием вычислительной техники • реализовывать методы генерации простых чисел средствами вычислительной техники • проводить дешифрование шифра простой перестановки при помощи метода биграмм
Владеть:	• навыками использованием вычислительной техники для реализации криптографических алгоритмов

4 Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 7 зачетных единицы 252акад. часов, в том числе:

– контактная работа – 142,8 акад. часов:
– аудиторная – 136 акад. часов;
– внеаудиторная – 6,8 акад. часов
– самостоятельная работа – 73,5 акад. часов;
– промежуточная аттестация – зачет и экзамен, защита курсовой работы

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лабораторные занятия	практич. занятия				
Раздел 1. Введение в криптографию. Основные классы шифров и их свойства 1.1 История криптографии. Основные понятия криптографии. Модели шифров. Основные этапы становления криптографии как науки. Открытые сообщения и их характеристики. Виды информации, подлежащие закрытию, их модели и свойства. Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Основные требования к шифрам.	7	4		4/2И	7	Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы	**ОПК-2** з **ПК-14 з**
1.2. Шифры перестановки. Шифры замены. Поточные шифры Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановок. Одноалфавитные и многоалфавитные замены.	7	10		10/4И	7	Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками,	– устный опрос (собеседование); – контрольные работы	**ОПК-2** зув **ПК-14**

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лабораторные	практич. занятия				
						каталогами, словарями, энциклопедиями Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками		**зув**
1.3 Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы криптографической защиты данных.	7	10		10/4И	7	Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы	**ОПК-2** зув **ПК-14 зув**
1.4. Надежность шифров. Имитостойкость шифров. Помехоустойчивость шифров. Криптографическая стойкость шифров. Имитация и подмена сообщения. Характеристика имитостойкости шифров. Коды аутентификации. Характеристики помехоустойчивости. Характеризация	7	10		10/4И	7	Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями,	– устный опрос (собеседование); – контрольные работы	**ОПК-2** зув **ПК-14 зув**

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лабораторные	практич. занятия				
шифров, не размножающих искажений типа замены и пропуска букв.						энциклопедиями Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками		
Итого по разделу		**34**		**34/14 И**	**38,2**		**Промежуточная аттестация (зачет)**	**ОПК-2 зув** **ПК-14 зув**
Раздел 2. Принципы построения криптографических алгоритмов Реализация криптографических алгоритмов 2.1 Основные способы реализации криптографических алгоритмов и требования, предъявляемые к ним. Методы получения случайных и псевдослучайных последовательностей. Методы усложнения последовательностей псевдослучайных чисел. Методы криптоанализа. Понятие криптоатаки. Классификация криптоатак. Классификация методов анализа криптографических алгоритмов	8	6		4/2И	6	Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы	**ОПК-2** з **ПК-14 з**
2.2 Шифры с открытыми ключами Криптосистемы RSA и Эль-Гамаля. Преимущества асимметричных систем	8	6		4/2И	6	Подготовка к семинарским, практическим занятиям Поиск дополнительной	– устный опрос (собеседование); – контрольные работы	**ОПК-2 зув**

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	тиялаборат.	практич. занятия				
шифрования. Криптографические хэш-функции. Характеристики и алгоритмы выработки хэш-функций.						информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками		**ПК-14 зув**
2.3 Модели криптографических протоколов Понятие криптографического протокола. Основные примеры, классификация криптографических протоколов. Понятие электронной цифровой подписи. Стандарты ЭЦП.	8	6		4/2И	6	Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы	**ПК-14 зув**
2.4 Разграничение и контроль доступа пользователей к техническим средствам вычислительной сети АПМДЗ «КРИПТОН-ЗАМОК». Идентификация и аутентификация пользователей до запуска BIOS. Блокировка компьютера при НСД, накопление и ведение электронного	8	10		16/4И	8	Самостоятельное изучение учебной литературы, конспектов лекций. Подготовка практическим занятиям.	- Практическая работа	**ПК-14 зув**

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лабораторные	практич. занятия				
журнала событий. Контроль целостности.								
2.5 Протоколы установления подлинности. Протоколы управления ключами. Взаимосвязь между протоколами аутентификации и цифровой подписи. Протоколы сертификации ключей. Протоколы распределения ключей.	8	6		6/4И	6	Самостоятельное изучение учебной литературы, конспектов лекций. Подготовка презентации для представления доклада.	– устный опрос (собеседование); – контрольные работы	**ПК-14 зув**
Итого по разделу		**34**		**34/14 И**	**35.3**	Самостоятельное изучение учебной литературы, конспектов лекций		
Подготовка к экзамену					**35.7**	Самостоятельное изучение учебной литературы, конспектов лекций	**Промежуточная аттестация (экзамен)**	**ОПК-2 зув** **ПК-14 зув**
Итого по дисциплине		**68**		**68/28 И**	**73,5**			

И – в том числе, часы, отведенные на работу в интерактивной форме.

5 Образовательные и информационные технологии

1. Традиционные образовательные технологии ориентируются на организацию образовательного процесса, предполагающую прямую трансляцию знаний от преподавателя к обучающемуся (преимущественно на основе объяснительно-иллюстративных методов обучения). Учебная деятельность обучающегося носит в таких условиях, как правило, репродуктивный характер.

Формы учебных занятий с использованием традиционных технологий:

Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

Практическая работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2. Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности обучающихся.

Формы учебных занятий с использованием технологий проблемного обучения:

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала.

Лекция «вдвоем» (бинарная лекция) – изложение материала в форме диалогического общения двух преподавателей (например, реконструкция диалога представителей различных научных школ, «ученого» и «практика» и т.п.).

Практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от обучающегося применения как научно-теоретических знаний, так и практических навыков.

Практическое занятие на основе кейс-метода – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации.

3. Игровые технологии – организация образовательного процесса, основанная на реконструкции моделей поведения в рамках предложенных сценарных условий.

Формы учебных занятий с использованием игровых технологий:

Учебная игра – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого.

Деловая игра – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и т.п.

Ролевая игра – имитация или реконструкция моделей ролевого поведения в предложенных сценарных условиях.

4. Технологии проектного обучения – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения учебного задания. Проект предполагает совместную учебно-познавательную деятельность группы обучающихся, направленную на выработку концепции, установление целей и задач, формулировку ожидаемых результатов, определение принципов и методик решения поставленных задач, планирование хода работы, поиск доступных и оптимальных ресурсов, поэтапную реализацию плана работы, презентацию результатов работы, их осмысление и рефлксию.

Основные типы проектов:

Исследовательский проект – структура приближена к формату научного исследования (доказательство актуальности темы, определение научной проблемы, предмета и объекта

исследования, целей и задач, методов, источников, выдвижение гипотезы, обобщение результатов, выводы, обозначение новых проблем).

Творческий проект, как правило, не имеет детально проработанной структуры; учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия и т.п.).

Информационный проект – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

5. Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды.

Формы учебных занятий с использованием специализированных интерактивных технологий:

Лекция «обратной связи» – лекция–провокация (изложение материала с заранее запланированными ошибками), лекция-беседа, лекция-дискуссия, лекция-прессконференция.

Семинар-дискуссия – коллективное обсуждение какого-либо спорного вопроса, проблемы, выявление мнений в группе (межгрупповой диалог, дискуссия как спор-диалог).

6. Информационно-коммуникационные образовательные технологии – организация образовательного процесса, основанная на применении специализированных программных сред и технических средств работы с информацией.

Формы учебных занятий с использованием информационно-коммуникационных технологий:

Лекция-визуализация – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).

Практическое занятие в форме презентации – представление результатов проектной или исследовательской деятельности с использованием специализированных программных сред.

6.Учебно-методическое обеспечение самостоятельной работы обучающихся

Перечень тем домашних заданий

1. Подготовка текста к шифрованию. Элементы шифрования
2. Криптоанализ классических шифров
3. Шифр двойной перестановки. Шифр простой замены. Шифр Виженера
4. Шифрование и дешифрование по алгоритму RSA
5. Генерация и проверка цифровой подписи на основе криптосистемы Эль-Гамаля.
6. Генерация ЭЦП
7. Проверка подлинности ЭЦП

Перечень1 тем контрольных работ

1) Основные типы информации требующей сокрытия.
2) Определить основные понятия криптографии (шифрование, дешифрование, расшифрование, открытый текст, закрытый текст, ключ, конфиденциальность, целостность, аутентификация, криптографические протоколы, хэш-функции).

3) Определить шифр замены. Определить шифр перестановки. Привести примеры шифров замены и перестановки. Привести примеры шифров являющихся композициями шифров замены и перестановки. Описать алгебраическую модель шифра. Описать вероятностную модель шифра
4) Сформулировать основные требования к шифрам. Дать понятие теоретической стойкости. Дать понятие практической стойкости. Дать определение совершенных шифров по Шеннону
5) Описать общую схему криптосистем с открытым ключом. Сформулировать основные математические задачи обеспечивающие безопасность асимметричных криптосистем. Описать принцип RSA. Перечислить и охарактеризовать параметры RSA
6) Перечислить основные типы криптографических протоколов. Привести примеры протоколов генерации и распределения ключей. Дать определение хеш-функции. Дать определение ЭЦП.

Перечень2 тем контрольных работ

1) Что такое «квадрат Полибия»? Объясните его устройство.
2) Опишите метод шифрования инверсными символами.
3) Чем отличается псевдооткрытый текст от настоящего открытого текста?
4) Перечислите компоненты шифровальной машины «Энигма».
5) Дайте определение термину «алгоритм симметричного шифрования». Приведите пример алгоритма.
6) Объясните суть метода шифрования кодом Цезаря.
7) В чем заключается суть метода шифрования путем перестановки символов?
8) Как зависит время вскрытия шифра путем подбора ключей от длины вероятного слова?
9) За что отвечает рефлектор шифровальной машины «Энигма»?
10) В чем заключается преобразование замешивания столбцов в алгоритме шифрования AES Rijndael?
11) Что такое «решетка Кардано»? К какому классу методов шифрования относится данный метод?
12) Частью какого метода шифрования является метод гаммирования?
13) Зависит ли время вскрытия шифра гаммирования от мощности алфавита протяжки вероятного слова?
14) Опишите процедуру использования шифровальной машины «Энигма».
15) Дайте определение методу шифрования Rijndael.
16) Опишите метод шифрования с помощью таблицы Виженера.
17) Чем определяется стойкость шифрования методом гаммирования?
18) Что такое «псевдооткрытый текст»?
19) Какие функции имело входное колесо шифровальной машины «Энигма»?
20) Опишите преобразование путем замены байт в алгоритме AES Rijndael.
21) Опишите устройство сциталы.
22) К какому классу методов шифрования относится код Цезаря?
23) Чем служит «вероятное слово» в раскрытии шифров перестановки?
24) Какие функции включала в себя коммутационная панель шифровальной машины «Энигма»?
25) Что из себя представляет ключ шифрования алгоритма AES Rijndael?
26) Опишите устройство диска Альберти.
27) Назовите один из самых известных методов криптоанализа.
28) Перечислите недостатки метода дешифрования с использованием протяжки вероятного слова.
29) Сколько букв использовала военная модель шифровальной машины «Энигма»?
30) Какие преобразования включает в себя шифр Rijndael?
31) В чем суть многоалфавитного метода шифрования?
32) Что такое «одноразовый шифровальный блокнот»?
33) В чем заключается метод протяжки вероятного слова?

34) Что представляет собой ротор шифровальной машины «Энигма»?
35) Назовите варианты длины ключа и длины блока алгоритма AES Rijndael.
36) С помощью чего можно вычислить смещение в криптоалгоритмах подстановки и перестановки?
37) Что можно определить по гистограмме шифрованного текста?
38) Как оценивается стойкость алгоритмов шифрования?
39) За счет чего шифрование машиной «Энигма» имело высокую стойкость?
40) В чем заключается преобразование путем сдвига строк в алгоритме AES Rijndael?

Перечень3 тем контрольных работ

1) Какие числа называются «числами Кармайкла»?
2) Перечислите стандарты ЭЦП, действующие в РФ.
3) Для выполнения каких требований к защищенности компьютерных систем могут применяться криптографические методы защиты?
4) Вычислить 127 (mod 7).
5) Дайте определение однонаправленной хэш-функции.
6) Опишите алгоритм RSA.
7) Назовите виды проверок числа на простоту.
8) Дайте определение ЭЦП.
9) Какие общие требования предоставляются к гамме шифра?
10) В чем заключается малая теорема Ферма?
11) Почему в качестве первого основания в тестах типа теста Ферма для проверки на простоту очень больших чисел целесообразно использовать число 2?
12) Вычислить 1812 (mod 13).
13) Опишите процедуру постановки ЭЦП.
14) В чем состоит назначение хэш-функций?
15) Опишите алгоритм Диффи-Хеллмана.
16) Перечислите условия, которым должна удовлетворять хэш-функция.
17) Опишите процедуру проверки ЭЦП.
18) Дайте определение ассиметричным системам шифрования.
19) Вычислите 343 (mod 5).
20) Опишите алгоритм DSA.
21) Перечислите стандарты хэш-функций, действующие в РФ.
22) Кратко опишите работу схемы реализации шифра скользящей перестановки.
23) В чем заключаются основные требования к защищённости компьютерных систем?
24) Сформулируйте суть теста на простоту с использованием пробных делений.
25) Перечислите достоинства ЭЦП.
26) На каких принципах основана криптостойкость современных алгоритмов ЭЦП?
27) Почему шифрование методом гаммирования является наиболее подходящим для высокоскоростных линий телекоммуникационной связи?
28) Как происходит дешифрование шифра перестановки?
29) Какая информация содержится в ЭЦП?
30) Опишите суть метода проверки на простоту тестом Ферма.

Перечень практических работ

Практическая работа 1

Использование классических алгоритмов подстановки и перестановки для защиты текстовой информации

Цель работы: изучение классических криптографических алгоритмов моноалфавитной подстановки, многоалфавитной подстановки и перестановки для защиты текстовой

информации. Использование гистограмм, отображающих частоту встречаемости символов в тексте для криптоанализа классических шифров.

Контрольные вопросы:

1. Перечислить методы криптографической защиты файлов
2. Преимущества и недостатки одноалфавитных методов
3. Обоснование выбора метода шифрования
4. Обоснование целесообразности повторного применения метода многоалфавитного шифрования и метода Цезаря

Практическая работа 2

Исследование методов защиты текстовой информации и их стойкости на основе подбора ключей

Цель работы: изучение методов шифрования (расшифрования) перестановкой символов, гаммированием, использованием таблицы Виженера. Исследование и сравнение стойкости на основе атак путем перебора возможных ключей.

Контрольные вопросы:

1. Чем отличается псевдооткрытый текст от настоящего открытого текста?
2. Как зависит время вскрытия шифра по ложному ключу от длины вероятного слова?
3. Зависит ли время вскрытия шифра гаммирования (или таблицы Виженера) от мощности алфавита гаммы?
4. В чем недостатки метода дешифрования с использованием протяжки вероятного слова?

Практическая работа 3

Изучение устройства и принципа работы шифровальной машины «Энигма»

Практическая работа 4

Ознакомление с принципами шифрования, используемыми в алгоритме симметричного шифрования AES RIJNDAEL.

Контрольные вопросы:

1. Сравнение основных характеристик алгоритмов RIJNDAEL и ГОСТ 28147-89
2. Описание структуры сети Фейстеля

Практическая работа 5

Генерация простых чисел для использования в асимметричных системах шифрования.

Контрольные вопросы:

1. Тест Ферма для проверки на простоту больших чисел
2. Тест на простоту с использованием пробных делений
3. Вычислить 1812 (mod 13); 127(mod 7).

Практическая работа 6

Ознакомление с принципами защищенного документооброиа и алгоритмами постановки ЭЦП.

Контрольные вопросы:

1. Назначение хэш-функции, требования к хэш-функциям, используемым для постановки ЭЦП
2. Стандарты Российской Федерации для хэш-функций
3. Процедуры постановки и использования ЭЦП.
4. Стандарты ЭЦП в Российской Федерации
5. Криптостойкость современных алгоритмов ЭЦП
6. Примеры реализации алгоритма ЭЦП (RSA, Эль-Гамаль, DSA)

Практическая работа 7

Шифрование методом скользящей перестановки.

Контрольные вопросы:

1. Общие требования, применяемые к гамме шифра
2. Описание работы схемы реализации шифра скользящей перестановки.

Практическая работа 8

Изучение принципа шифрования информации с помощью биграммного шифра Плейфера.

Контрольные вопросы:

1. К какому классу шифров относится шифр Плейфера?
2. Описать процедуры шифрования и расшифрования по методу Плейфера
3. Оценить криптостойкость метода шифрования с помощью биграммного шифра Плейфера и возможности применения метода в современных криптосистемах.

Практическая работа 9

Дешифрование шифра простой перестановки с помощью метода биграмм.

Контрольные вопросы:

1. Суть основной теоремы Шеннона для канала без помех.
2. В чем заключается метод шифрования (расшифрования) с использованием перестановок?
3. Применение алгоритма перестановки в современных симметричных крипосистемах
4. Какие требования к исходным текстам и длинам ключей шифрования обеспечат максимальных эффект для использования изученного метода шифрования?

Практическая работа 10

Изучение принципа работы сети Фейстеля. Симметричные криптоалгоритмы, использующие сеть Фейстеля (DES и ГОСТ-28147-89).

Контрольные вопросы:

1. В каких современный симметричных системах шифрования используется сеть Фейстеля.
2. В каких блочных криптосистемах используется сбалансированная сеть?
3. Какой длины используются блоки для шифрования и цикловые ключи в блочных криптосистемах DES и ГОСТ-28147-89?

Практическая работа 11

Изучение принципа работы генератора псевдослучайных последовательностей, основанного на регистре сдвига с линейной обратной связью .

Контрольные вопросы:

1. Что такое М—последовательность?
2. Описать процесс работы четырехбитового регистра сдвига с линейной обратной связью.
3. О чего зависит период регистра сдвига с линейной обратной связью?
4. Что входит в понятие линейная сложность бинарной последовательности?

Курсовая работа должна быть оформлена в соответствии с СМК-О-СМГТУ-42-09 «Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления».

Примерный перечень тем курсовых работ и пример задания представлены в разделе 7 «Оценочные средства для проведения промежуточной аттестации».

7 Оценочные средства для проведения промежуточной аттестации

Промежуточная аттестация имеет целью определить степень достижения запланированных результатов обучения по каждой дисциплине (модулю) за определенный период обучения (семестр) и может проводиться в форме зачета, экзамена, защиты курсовой работы.

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-14 - способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации		
Знать:	• Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах Классификацию криптографических средств защиты информации. • методы шифрования, использующие классические симметричные алгоритмы, • методы шифрования, использующие классические алгоритмы моноалфавитной и многоалфавитной подстановки и перестановки для защиты текстовой информации, • методы шифрования (расшифрования) перестановкой символов, подстановкой, гаммированием, использованием таблицы Виженера. • общие принципы действия шифровальной машины Энигма • общие принципы шифрования, используемые в алгоритме симметричного шифрования AES	**Вопросы для зачета** 1. Основные понятия криптографии. 2. Модели шифров. 3. Открытые сообщения и их характеристики. 4. Виды информации, подлежащие закрытию, их модели и свойства. 5. Блочные и поточные шифры. 6. Понятие криптосистемы. 7. Ручные и машинные шифры. 8. Основные требования к шифрам. 9. Шифры перестановки. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановок 10. Поточные шифры. Шифры замены. Одноалфавитные и многоалфавитные замены. 11. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. 12. Вопросы криптоанализа простейших шифров замены. 13. Стандартные алгоритмы криптографической защиты данных. **Перечень вопросов для экзамена** 1. Основные способы реализации криптографических алгоритмов и требования, предъявляемые к ним. 2. Методы получения случайных и псевдослучайных последовательностей. 3. Методы усложнения последовательностей псевдослучайных чисел. 4. Методы криптоанализа. 5. Понятие криптоатаки.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	• принципы шифрования информации с помощью биграммного шифра Плейфера • Способы контрольных проверок работоспособности применяемых криптографических средств защиты информации.	6. Классификация криптоатак. 7. Классификация методов анализа криптографических алгоритмов 8. Шифры с открытыми ключами 9. Криптосистемы RSA и Эль-Гамаля. 10. Преимущества асимметричных систем шифрования. 11. Криптографические хэш-функции. 12. Характеристики и алгоритмы выработки хэш-функций. 13. Модели криптографических протоколов 14. Понятие криптографического протокола. 15. Основные примеры, классификация криптографических протоколов. понятие электронной цифровой подписи. 16. Стандарты ЭЦП. 17. Протоколы установления подлинности. 18. Протоколы управления ключами. 19. Взаимосвязь между протоколами аутентификации и цифровой подписи. 20. Протоколы сертификации ключей. 21. Протоколы распределения ключей. 22. Аппаратные возможности АПМДЗ «Криптон-Замок»
Уметь:	• исследовать различные методы защиты текстовой информации и их стойкости на основе подбора ключей • Участвовать в настройке криптографических средств обеспечения информационной безопасности. • Самостоятельно настраивать криптографические средства обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств ЗИ. • Применять криптографические средства	Провести оценку шифрования по критериям: • Надежность шифров. • Имитостойкость шифров. • Помехоустойчивость шифров. • Криптографическая стойкость шифров. • Имитация и подмена сообщения. Характеристика имитостойкости шифров. • Коды аутентификации. • Характеристики помехоустойчивости.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	обеспечения ИБ. Исследовать эффективность контрольных проверок работоспособности применяемых криптографических средств обеспечения ИБ.	
Владеть:	• Техникой настройки криптографических средств обеспечения информационной безопасности. • Навыками использования криптографических средств обеспечения информационной безопасности автоматизированных систем. • Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.	1. Оценить криптостойкость метода шифрования с помощью биграммного шифра Плейфера и возможности применения метода в современных криптосистемах. 2. Разграничить доступа к аппаратным ресурсам ПЭВМ с АПМДЗ «Криптон-Замок». Создать несколько пользователей с различными правами доступа. Обеспечить контроль целостности установленной программной среды. Настроить блокировку компьютера при НСД. Проверить журнал событий. 3. Спроектировать конфигурацию СКЗИ для многофункционального АРМ.
ОПК-2 – способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники		
Знать:	• математический аппарат теории информации, теории алгоритмов • процессы генерации простых чисел для систем ассиметричного шифрования • процессы постановки и верификации ЭЦП • математический аппарат шифра скользящей перестановки	**Вопросы для зачета** 1. Виды информации, подлежащие закрытию, их модели и свойства. 2. Блочные и поточные шифры. 3. Понятие криптосистемы. 4. Ручные и машинные шифры. 5. Основные требования к шифрам. 6. Шифры перестановки. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	• принцип работы сети Фейстеля как базовым преобразованием симметричных блочных криптосистем	перестановок 7. Поточные шифры. Шифры замены. Одноалфавитные и многоалфавитные замены. 8. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. 9. Вопросы криптоанализа простейших шифров замены. 10. Описать процесс работы четырехбитового регистра сдвига с линейной обратной связью.
Уметь:	• корректно применять при решении профессиональных задач математический аппарат теории алгоритмов, теории информации, в том числе с использованием вычислительной техники • реализовывать методы генерации простых чисел средствами вычислительной техники • проводить дешифрование шифра простой перестановки при помощи метода биграмм	• Провести тест Ферма для проверки на простоту больших чисел • Провести тест на простоту с использованием пробных делений • Вычислить 1812 (mod 13); 127(mod 7). • Описать процесс работы четырехбитового регистра сдвига с линейной обратной связью.
Владеть:	• навыками использованием вычислительной техники для реализации криптографических алгоритмов	**Подготовить курсовую работу на тему:** 1. Разработать программное обеспечение для шифрования и дешифрования текста на основе шифра маршрутной перестановки. 2. Разработать программное обеспечение для шифрования и дешифрования текста на основе шифра двойной перестановки. 3. Разработать программное обеспечение для шифрования и дешифрования текста на основе алгоритма Диффи-Хэлмана. 4. Разработать программное обеспечение для шифрования и дешифрования текста на основе шифра Цезаря.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		5. Разработать программное обеспечение для шифрования и дешифрования текста на основе шифра табличной маршрутной перестановки. 6. Разработать программное обеспечение для шифрования и дешифрования текста на основе шифра вертикальной перестановки. 7. Разработать программное обеспечение для шифрования и дешифрования текста на основе одноалфавитного шифра подстановки с использованием кодового слова. 8. Разработать программное обеспечение для шифрования и дешифрования текста на основе шифра Виженера. 9. Разработать программное обеспечение для шифрования и дешифрования текста на основе алгоритма RSA.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Показатели и критерии оценивания зачета:

– на оценку **«зачтено»** – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации;

– на оценку **«не зачтено»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации.

Показатели и критерии оценивания экзамена:

– – на оценку «**отлично**» (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку «**хорошо**» (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку «**удовлетворительно**» (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку «**неудовлетворительно**» (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала или не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

Курсовая работа выполняется под руководством преподавателя, в процессе ее написания обучающийся развивает навыки к научной работе, закрепляя и одновременно расширяя знания, полученные при изучении дисциплины. При выполнении курсовой работы обучающийся должен показать свое умение работать с нормативным материалом и другими литературными источниками, а также возможность систематизировать и анализировать фактический материал и самостоятельно творчески его осмысливать.

В процессе написания курсовой работы обучающийся должен разобраться в теоретических вопросах избранной темы, самостоятельно проанализировать практический материал, разобрать и обосновать практические предложения.

Показатели и критерии оценивания курсовой работы:

– на оценку «**отлично**» (5 баллов) – работа выполнена в соответствии с заданием, обучающийся показывает высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку «**хорошо**» (4 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам;

– на оценку «**удовлетворительно**» (3 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания на уровне воспроизведения и объяснения информации, интеллектуальные навыки решения простых задач;

– на оценку «**неудовлетворительно**» (2 балла) – задание преподавателя выполнено частично, в процессе защиты работы обучающийся допускает существенные ошибки, не может показать интеллектуальные навыки решения поставленной задачи, обучающийся не может воспроизвести и объяснить содержание, не может показать интеллектуальные навыки решения поставленной задачи.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1) Бутакова Н.Г., Федоров Н.В. Криптографические методы и средства защиты информации: учебное пособие / Н.Г. Бу-таков, Н.В. Федоров–СПб.: ИЦ«Интермедия», 2017. – 384 с. https://ibooks.ru/reading.php?productid=356918

2) Введение в теоретико-числовые методы криптографии [Текст] : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2018. - 394 с. : ил., табл., схемы. - Для: КУР. - ISBN 978-5-8114-1116-0 : 893 р. 86 к.

б) Дополнительная литература:

1) Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 236 с.: http://znanium.com/bookread2.php?book=987215

2) Введение в теоретико-числовые методы криптографии [Текст] : учебное пособие для вузов / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. - СПБ. ; М. ; Краснодар : Лань, 2011. - 394 с. : табл. - ISBN 978-5-8114-1116-0 : 676 р. 94 к.

3) Гашков, С. Б. Криптографические методы защиты информации [Текст] : учебное пособие. - М. : Академия, 2010. - 298 с. : ил. - ISBN 978-5-7695-4962-5 : 499 р. 40 к.

с) Программное обеспечение и Интернет-ресурсы:

1. Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.
2. Журнал «Безопасность информационных технологий»: периодич. интернет-изд. URL: http://www.pvti.ru/articles_14.htm – Загл. с экрана. Яз. рус.
3. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.
4. «Журнал сетевых решений LAN»: периодич. интернет-изд. URL: http://www.osp.ru/lan/ Издательство "Открытые системы. СУБД". URL: http://www.osp.ru/os/– Загл. с экрана. Яз. рус.
5. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru, свободный.– Загл. с экрана. Яз. рус.
6. Российская национальная библиотека. [Электронный ресурс] / –URL: http://www.nlr.ru. – Загл. с экрана. Яз. рус.
7. Компьютерра: все новости про компьютеры, железо, новые технологии, информационные : периодич. интернет-изд. URL: http://www.computerra.ru/ – Загл. с экрана. Яз. рус.
8. http://www.безопасник.рф– Загл. с экрана. Яз. рус.

9 Материально-техническое обеспечение дисциплины

Тип и название аудитории	Оснащение аудитории
Лекционная аудитория (ауд. 2124, ауд. 226, 309а, ауд. 365, ауд. 388 и т.д.)	Мультимедийные средства хранения, передачи и представления информации
Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.)	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office (Microsoft Open License 42649837,

Тип и название аудитории	Оснащение аудитории
	бессрочная); Выход в Интернет и доступ в электронную информационно-образовательную среду университета.
Лаборатория радиомониторинга и контроля утечек информации, ауд. 226	Комплект учебного оборудования «Криптографические системы»
Лаборатория программно-аппаратных средств защиты информации, ауд. 2124	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); АПМДЗ «Криптон-Замок».
Аудитория для самостоятельной работы читальные залы библиотеки, ауд 132а	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office (Microsoft Open License 42649837, бессрочная); Выход в Интернет и доступ в электронную информационно-образовательную среду университета.