МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ В.Р. Храмшин

10.02.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	7, 8

Магнитогорск
2023 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
09.02.2023, протокол № 5

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
10.02.2023 г. протокол № 7

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
доцент кафедры ИиИБ, канд. техн. наук _____ У.В. Кузьмина

Рецензент:
начальник отдела информационной безопасности «КУБ» (АО) ,
_____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2029 - 2030 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целью дисциплины «Методы и средства криптографической 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 (модуля) в структуре образовательной программы

Дисциплина Методы и средства криптографической защиты информации входит в обязательную часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Организация ЭВМ и вычислительных систем

Теория информации

Информатика

Языки программирования

Теория вероятностей, математическая статистика

Математический анализ

Основы информационной безопасности

Технологии и методы программирования

Программно-аппаратные средства обеспечения информационной безопасности

Основы теории оптимизации

Основы безопасности цифрового общества

Учебная - ознакомительная практика

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Защита электронного документооборота

Управление информационной безопасностью

Защита программного обеспечения

Методы проектирования систем защиты распределенных информационных систем

Обеспечение информационной безопасности критической информационной инфраструктурой

Защита информационно-технологических ресурсов автоматизированных систем

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Форензика

Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

Производственная - научно-исследовательская работа

Производственная - преддипломная практика

Методы и стандарты оценки защищенности компьютерных систем

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

В результате освоения дисциплины (модуля) «Методы и средства криптографической защиты информации» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	
ОПК-10.1	Применяет при решении профессиональных задач математический аппарат теории алгоритмов, теории информации
ОПК-10.2	Использует современные средства криптографической защиты информации
ОПК-10.3	Использует вычислительную технику для реализации криптографических алгоритмов

4. Структура, объём и содержание дисциплины (модуля)

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

– контактная работа – 141,8 акад. часов:

– аудиторная – 136 акад. часов;

– внеаудиторная – 5,8 акад. часов;

– самостоятельная работа – 74,5 акад. часов;

– в форме практической подготовки – 0 акад. час;

– подготовка к экзамену – 35,7 акад. час

Форма аттестации - зачет, экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
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	7	Подготовка к семинарским, практическим занятиям Самостоятельное изучение учебной и научно литературы, работа с материалами образовательног о портала и ЭБС. Подготовка к тестированию	Тестирование	ОПК-10.1, ОПК-10.2, ОПК-10.3
1.2 Шифры перестановки. Шифры замены. Поточные шифры Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановок. Одноалфавитные и многоалфавитные замены.		10		10	7	Подготовка к семинарским, практическим занятиям Самостоятельное изучение учебной и научно литературы, работа с материалами образовательног о портала и ЭБС. Подготовка к тестированию и АКР.	Тестирование и аудиторная контрольная работа	ОПК-10.1, ОПК-10.2, ОПК-10.3

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.		10		10	7	Подготовка к семинарским, практическим занятиям Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к аудиторным работам.	Аудиторная контрольная работа	ОПК-10.1, ОПК-10.2, ОПК-10.3
1.4 Надежность шифров. Имитостойкость шифров. Помехоустойчивость шифров. Криптографическая стойкость шифров. Имитация и подмена сообщения. Характеристика имитостойкости шифров. Коды аутентификации. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв.		10		10	7	Подготовка к семинарским, практическим занятиям Подготовка к контрольной работе Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС.	Аудиторная контрольная работа	ОПК-10.1, ОПК-10.2, ОПК-10.3
1.5 Подготовка к зачету					10,2	Подготовка к зачету. Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС.	Зачет	ОПК-10.1, ОПК-10.2, ОПК-10.3
Итого по разделу		34		34	38,2			
Итого за семестр		34		34	38,2		зачёт	
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	6	Подготовка к семинарским, практическим занятиям Подготовка к контрольной работе. Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС.	Аудиторная контрольная работа, устный опрос	ОПК-10.1, ОПК-10.2, ОПК-10.3
2.2 Шифры с открытыми ключами Криптосистемы RSA и Эль-Гамаля. Преимущества асимметричных систем шифрования. Криптографические хэш-функции. Характеристики и алгоритмы выработки хэш-функций.		6		4	6	Подготовка к семинарским, практическим занятиям Подготовка к контрольной работе Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС.	Аудиторная контрольная работа, устный опрос	ОПК-10.1, ОПК-10.2, ОПК-10.3
2.3 Модели криптографических протоколов Понятие криптографического протокола. Основные примеры, классификация криптографических протоколов. Понятие электронной цифровой подписи. Стандарты ЭЦП.		6		4	6	Подготовка к семинарским, практическим занятиям Подготовка к контрольной работе Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС.	Аудиторная контрорьная работа, устный опрос	ОПК-10.1, ОПК-10.2, ОПК-10.3

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 журнала событий. Контроль целостности.		10		16	12,3	Самостоятельное изучение учебной литературы, конспектов лекций. Подготовка практическим занятиям.	Практическая работа	ОПК-10.1, ОПК-10.2, ОПК-10.3
2.5 Протоколы установления подлинности. Протоколы управления ключами. Взаимосвязь между протоколами аутентификации и цифровой подписи. Протоколы сертификации ключей. Протоколы распределения ключей.		6		6	6	Самостоятельное изучение учебной литературы, конспектов лекций. Подготовка презентации для представления доклада.	Доклад по практической работе.	ОПК-10.1, ОПК-10.2, ОПК-10.3
2.6 Подготовка к экзамену						Самостоятельное изучение учебной литературы, конспектов лекций	Экзамен	ОПК-10.1, ОПК-10.2, ОПК-10.3
Итого по разделу		34		34	36,3			
Итого за семестр		34		34	36,3		экзамен	
Итого по дисциплине		68		68	74,5		зачет, экзамен	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. 2) Раздельно-компетентностная технология, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. 3) 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. 4) Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности обучающихся. 5) Игровые технологии – организация образовательного процесса, основанная на реконструкции моделей поведения Формы учебных занятий с использованием предложенных сценарных условий. 6) 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 рефлексию. 7) Информационно-коммуникационные образовательные технологии – организация образовательного процесса, основанная на применении специализированных программных сред и технических средств работы с информацией.

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 документооборота 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?

7 Оценочные средства для проведения промежуточной аттестации

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

Компетенция / Индикатор достижения компетенции	Оценочные средства
ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	
ОПК-10.1 Применяет при решении профессиональных задач математический аппарат теории алгоритмов, теории информации	**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. 14. Виды информации, подлежащие закрытию, их модели и свойства. 15. Блочные и поточные шифры. 16. Понятие криптосистемы. 17. Ручные и машинные шифры. 18. Основные требования к шифрам. 19. Шифры перестановки. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановок 20. Поточные шифры. Шифры замены. Одноалфавитные и многоалфавитные замены. 21. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа.

	22. Вопросы криптоанализа простейших шифров замены. 23. 10. Описать процесс работы четырехбитового регистра сдвига с линейной обратной связью. **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. 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»
ОПК-10.2 Использует современные средства криптографической защиты информации	1. Провести оценку шифрования по критериям: • Надежность шифров. • Имитостойкость шифров. • Помехоустойчивость шифров. • Криптографическая стойкость шифров. • Имитация и подмена сообщения. Характеристика имитостойкости шифров. • Коды аутентификации. 2. Характеристики помехоустойчивости. 3. Оценить криптостойкость метода шифрования с помощью биграммного шифра Плейфера и возможности применения метода в современных криптосистемах. 4. 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. 5. Спроектировать конфигурацию СКЗИ для многофункционального АРМ.
ОПК-10.3 Использует	1. Разработать программное обеспечение для шифрования

вычислительную технику для реализации криптографических алгоритмов	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. 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.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714 (дата обращения: 27.04.2023). – Режим доступа: по подписке.

2. Маршаков, Д. В. Методы и средства криптографической защиты информации. Практический курс : учебное пособие / Д.В. Маршаков, Д.В. Фахти. — Москва : ИНФРА-М, 2022. — 76 с. — (Высшее образование). - ISBN 978-5-16-110842-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1891129 (дата обращения: 27.04.2023). – Режим доступа: по подписке.

3. Романьков, В. А. Введение в криптографию : курс лекций / В.А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2023. — 240 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-00091-493-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1937958 (дата обращения: 27.04.2023). – Режим доступа: по подписке.

б) Дополнительная литература:

1. Баранова, Е. К. Актуальные вопросы защиты информации : монография / А.В. Бабаш, Е.К. Баранова. — Москва : РИОР : ИНФРА-М, 2023. — 111 с. — (Научная мысль). — https://doi.org/10.12737/monography_58dbc380aa3a4. - ISBN 978-5-369-01680-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1915704 (дата обращения: 27.04.2023). – Режим доступа: по подписке.

2. Жданов, О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования : монография / О.Н. Жданов. — Москва : ИНФРА-М, 2021. — 88 с. — (Научная мысль). - ISBN 978-5-16-006890-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1514896 (дата обращения: 27.04.2023). – Режим доступа: по подписке.

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронного каталога https://magtu.informsystema.ru .
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта*.

*При открытии макрообъектов учитывайте настройки антивирусной защиты

в) Методические указания:

1. Методические указания по выполнению практических работ (Приложение 1)
2. Методические указания по выполнению внеаудиторных самостоятельных работ (Приложение 2)

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
7Zip	свободно	бессрочно
eTokenSecurLogon for Oracle	К-271-12 от 16.10.2012	бессрочно
СКЗИ КриптоПро CSP	К-271-12 от 16.10.2012	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно

Браузер Yandex	свободно	бессрочно
Linux Calculate	свободно	бессрочно
FAR Manager	свободно	бессрочно
LibreOffice	свободно	бессрочно
MS Visual Studio Code	свободно распространяемое ПО	бессрочно
MS Visual Studio 2017 Community Edition	свободно распространяемое ПО	бессрочно
VIP Net Client	Д-946-14 от 22.07.2014	бессрочно
VIP Net CryptoService	Д-946-14 от 22.07.2014	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации ФСТЭК России	https://fstec.ru

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

1) Лаборатория программно-аппаратных средств обеспечения информационной безопасности (2124):

Программно-аппаратное средство ограничения доступа к компьютеру «КРИПТОН-ЗАМОК/У»

Программно-аппаратное средство ограничения доступа к компьютеру «КРИПТОН-ЗАМОК/Е»(2 шт)

СКЗИ Крипто БД (лицензия: договор К-271-12 от 16.10.12)

Электронный ключ Guardant (12 шт)

Электронный ключ Etoken (12 шт)

Устройство идентификации (Электронный ключ Guardant ID сертифицированный)

ПЭВМ на базе Windows 10 – 12 шт

Программно-аппаратное средство ограничения доступа к компьютеру «КРИПТОН-ЗАМОК/Е»(1шт)

2) Лаборатория защищенных автоматизированных систем (2113):

Комплект учебного оборудования «Криптографические системы (3 шт)

3) Аудитория для самостоятельной работы: читальные залы библиотеки, ауд 132а

4) Лекционные аудитории (ауд. 2124, ауд. 2113, ауд. 2122):

Мультимедийные средства хранения, передачи и представления информации

ПРИЛОЖЕНИЕ 1

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

Рекомендации направлены на оказание методической помощи обучающимся при выполнении практических занятий.

Практическое занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории (компьютерном классе университета или учебной специализированной лаборатории университета), направленное на углубление научно-теоретических знаний и получение практических навыков решения типовых и прикладных задач.

Целью практических занятий является формирование и отработка практических умений и навыков, необходимых в последующей деятельности обучающихся.

Основными задачами практических занятий являются:

- углубление уровня освоения общекультурных и профессиональных компетенций;
- обобщение, систематизация, углубление, закрепление полученных практических знаний по конкретным темам дисциплин различных циклов;
- приобретение обучающимися умений и навыков использования современных теоретических знаний в решении конкретных практических задач;
- развитие профессионального мышления, профессиональной и познавательной мотивации.

Перечень тем практических занятий определяется рабочей программой дисциплины. План практических занятий отвечает общей направленности лекционного курса и соотнесен с ним в последовательности тем.

Структура практического занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущего практического занятия, ставится его цели и задачи, проверяется исходный уровень готовности обучающихся к практическому занятию (выполнение тестов, контрольные вопросы и т.п.)

На практическом занятии преподаватель может использовать разнообразные образовательные технологии (методы IT, работа в команде, case-study, проблемное обучение, учебные дискуссии и т.п.) по своему выбору для достижения качественного уровня обучения.

Правила по технике безопасности для обучающихся при проведении практических работ

Общие правила:

1. Практические работы проводятся под наблюдением преподавателя. К выполнению практических работ обучающиеся допускаются только после прослушивания инструктажа по технике безопасности, правилам поведения, противопожарным мерам в компьютерном классе и специализированных лабораториях.

2. Обучаемый должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах и специализированных лабораториях университета.

Порядок выполнения практических работ

При подготовке к выполнению практических работ обучающийся должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

Практическая работа выполняется каждым обучающимся самостоятельно, согласно индивидуальному заданию.

Обучающиеся, пропустившие занятия, выполняют практические работы во внеурочное время.

После выполнения каждой практической работы обучающийся демонстрирует результат выполнения преподавателю, отвечает на вопросы. Преподаватель оценивает

работу в соответствии с заданными критериями оценки практических работ.

Правила оформления результатов и оценивания практической работы

Результаты выполненной практической работы оформляются в соответствии с требованиями к выполнению конкретной работы.

Практическая работа считается выполненной, если обучающийся набрал балл, который составляет половину максимального количества баллов.

Для оценивания работы прилагается следующие критерии.

Оценка «отлично» – работа выполнена в полном объеме и без замечаний.

Оценка «хорошо» – работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

Оценка «неудовлетворительно» – допущены две (и более) существенные ошибки в ходе работы, которые обучающийся не может исправить даже по требованию преподавателя, или работа не выполнена.

ПРИЛОЖЕНИЕ 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы обучающихся и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
   a) предоставляемыми преподавателем на лекционных занятиях;
   b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
   c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.
2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.
3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.
4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы с обучающимися группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: индивидуальные задания, аудиторные контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.