Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования

Пермский национальный исследовательский политехнический университет

УТВЕРЖДАЮ
Проректор по образовательной деятельности

_____ А.Б. Петроченков

« 22 » февраля 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Криптография
(наименование)

Форма обучения: очная
(очная/очно-заочная/заочная)

Уровень высшего образования: магистратура
(бакалавриат/специалитет/магистратура)

Общая трудоёмкость: 144 (4)
(часы (ЗЕ))

Направление подготовки: 01.04.02 Прикладная математика и информатика
(код и наименование направления)

Направленность: Математическая кибернетика
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Цель дисциплины:овладение основным математическим аппаратом исследования формализованных структур, формирование логического и системного мышления студентов. Целью преподавания дисциплины является изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.
Задачи дисциплины:
- формирование знаний системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- формирование умений принципов синтеза и анализа шифров;
- приобретение навыков математических методов, используемых в криптоанализе.

1.2. Изучаемые объекты дисциплины

- алгоритмы поточного шифрования;
- алгоритмы блочного шифрования;
- алгоритмы вероятностного шифрования;
- криптографические протоколы.

1.3. Входные требования

Предварительные знания в объеме бакалаврской программы по этой или смежной тематике.

2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-1.3	ИД-1ПК-1.3	Знает основные методы получения, хранения и обработки информации. Знает алгоритмы классических криптографических шифров и методы построения бизнес-моделей.	Знает инструменты и методы моделирования бизнес-процессов	Контрольная работа
ПК-1.3	ИД-2ПК-1.3	Умеет осуществлять поиск информации и последующую обработку.	Умеет анализировать исходную документацию	Коллоквиум

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-1.3	ИД-3ПК-1.3	Владеет математическими основами криптографии. Владеет навыками построения криптостойких алгоритмов шифрования и применения их при проектировании бизнес-процессов.	Владеет навыками разработки и выбора инструментов и методов проектирования бизнес-процессов	Дифференцированный зачет

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		3
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	54	54
- лекции (Л)	18	18
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	34	34
- контроль самостоятельной работы (КСР)	2	2
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	90	90
2. Промежуточная аттестация		
Экзамен		
Дифференцированный зачет	9	9
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)	18	18
Общая трудоемкость дисциплины	144	144

4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
3-й семестр				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Раздел 1. Шифрование	6	0	10	30
Тема 1. Основные понятия, термины, определения. Предмет и задачи дисциплины. Из истории криптографии. Простейшие шифры и их свойства. Шифры замены и перестановки. Композиции шифров. Основные этапы становления криптографии как науки. Характер криптографической деятельности. Открытые сообщения и их характеристики. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений. Основные понятия криптографии. Модели шифров. Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам. Тема 2. ШИФРЫ ПЕРЕСТАНОВКИ. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки. ШИФРЫ ЗАМЕНЫ. Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы криптографической защиты данных. Современные системы шифрования (симметрические и асимметрические). ПОТОЧНЫЕ ШИФРЫ. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы. Синтез и анализ криптографических алгоритмов: классические шифры, шифры гаммирования и колонной замены. Тема 3. ТЕОРИЯ К.ШЕННОНА. Теоретико-информационный подход к оценке криптостойкости шифров. Криптографическая стойкость шифров. Надежность ключей и сообщений. Совершенные шифры. Безусловно стойкие и вычислительно стойкие шифры. Вопросы практической стойкости. Избыточность языка и расстояние единственности.				
Раздел 2. Проблемы реализации криптографических алгоритмов	4	0	8	28
Тема 4. ИМИТОСТОЙКОСТЬ ШИФРОВ. Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Коды аутентификации. Основные методы дешифрования.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
ПОМЕХОУСТОЙЧИВОСТЬ ШИФРОВ. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв. Тема 5. РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ. Основные способы реализация криптографических алгоритмов и требования, предъявляемые к ним. Различие между программными и аппаратными реализациями. Программные реализации шифров. Программно-аппаратная реализация современных криптографических схем и систем. Особенности использования вычислительной техники в криптографии. Современные криптографические интерфейсы. Криптографические стандарты. Стандарты систем шифрования (DES, ГОСТ 28147-89). Вопросы синтеза шифров.				
Раздел 3. Криптографические протоколы	8	0	16	32
Тема 6. ВОПРОСЫ СИНТЕЗА ГЕНЕРАТОРОВ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ. Методы получения случайных и псевдослучайных последовательностей. Регистры сдвига с обратной связью. Линейный конгруэнтный метод. Мультиплексорные последовательности. Проверка построенной последовательности на случайность. Методы усложнения последовательностей псевдослучайных чисел. Связь между качеством последовательностей, полученных с помощью нелинейных регистров сдвига и характеристиками функции усложнения. Применение дискретных функций для усложнений последовательности. Различные способы задания дискретных функций. Тема 7. Методы анализа криптографических алгоритмов. Понятие криптоатаки. Виды криптоатак. Классификация криптоатак. Методы анализа криптографических алгоритмов: перебор ключей, метод «встречи посередине», линеаризация уравнений шифрования, бесключевые методы. Особенности криптоанализа блочных шифров. Криптографические параметры узлов и блоков шифраторов. Основные принципы построения криптоалгоритмов (выбор группы шифра, параметров ПСП, параметров функции усложнения) СИСТЕМЫ ШИФРОВАНИЯ С ОТКРЫТЫМИ КЛЮЧАМИ. Понятие односторонней функции и односторонней функции с «лазейкой». Криптосистемы RSA и Эль-Гамаля. Проблемы факторизации целых чисел и логарифмирования в конечных полях. Секретные характеристики в системах с открытым ключом.				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Преимущества ассиметричных систем шифрования. Вероятностное шифрование. Тема 8. МОДЕЛИ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ. Сложность криптографических алгоритмов (теорема Кука, NP-полнота). Криптографические протоколы, протоколы с нулевым разглашением. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов. ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ (ЭЦП). Понятие ЭЦП. Стандарты ЭЦП. Однонаправленные функции и методы их построения. Тема 9. Протоколы установления подлинности. Парольные системы разграничения доступа и протоколы «рукопожатия». Взаимосвязь между протоколами аутентификации и ЭЦП. Протоколы управления ключами. Протоколы сертификации ключей. Протоколы распределения ключей. Открытое распределение ключей Диффи-Хэлмана и его модификация. Протоколы Oakley, ISAKMP. Проблемы и перспективы исследований в области современной криптографии. Квантовая криптография. Стеганография.				
ИТОГО по 3-му семестру	18	0	34	90
ИТОГО по дисциплине	18	0	34	90

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Простейшие шифры и их свойства. Типы атак. Атаки, в основе которых лежит парадокс задачи о днях рождения. Двусторонние атаки. Уровень безопасности. Освоение процессов зашифрования и расшифрования для простейших шифров.
2	Криптоанализ шифра однобуквенной простой замены.
3	Вскрытие шифра Вернама при повторном использовании ключа. Криптоанализ шифра Виженера.
4	Шифры, основанные на алгоритме Файстеля. Функция раунда. Реализация функции раунда. Традиционные симметричные блочные шифры.
5	Расчет метода встречных атак.
6	Канальное и сквозное шифрование. Управление секретными клю-чами. Криптоанализ рассмотренных алгоритмов симметричного шифрования. Размер ключа.
7	Цифровые подписи. Управление ключами. Взлом ключа. Согласование ключей с помощью пароля. Защищенные функции хэширования. HMAC. SHA. MD5. RIPEMD. UMAC. Криптография с открытым ключом.
8	Обмен ключами. Схема Диффи-Хеллмана. Протокол обмена ключами Oakley, ISAKMP.

№ п.п.	Наименование темы практического (семинарского) занятия
9	Стохастическое преобразование информации. R-блоки. Гаммирование. Вероятностное шифрование.

Тематика примерных курсовых проектов/работ

№ п.п.	Наименование темы курсовых проектов/работ
1	Режим электронного сцепления блоков.
2	Самосинхронизирующиеся поточные шифры.
3	Шифры гаммирования.
4	Варианты случайного распределения помех.
5	Альтернативные варианты алгоритмов шифрования, основанных на схеме Файстеля.
6	Шифрование, построенное на понятии P-полных языков.
7	ЭЦП Эль-Гамаля.

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при которой учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установления связей с ранее освоенным материалом.

Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. При проведении практических занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем и приятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.

При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.

5.2. Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

6. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Печатная учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1. Основная литература		
1	Гашков С. Б. Криптографические методы защиты информации : учебное пособие для вузов / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - Москва: Академия, 2010.	8
2	Данилов А. Н. Математические основы криптологии и криптографические методы и средства обеспечения информационной безопасности : учебное пособие / А. Н. Данилов, Е. Л. Кротова, Ю. Н. Липин. - Пермь: Изд-во ПГТУ, 2008.	64
3	Данилов А. Н. Практикум по курсам Математические основы криптологии и Криптографические методы и средства обеспечения информационной безопасности : учебное пособие / А. Н. Данилов, Е. Л. Кротова, Ю. Н. Липин. - Пермь: Изд-во ПГТУ, 2008.	59
4	Рябко Б. Я. Криптографические методы защиты информации : учебное пособие для вузов / Б. Я. Рябко, А. Н. Фионов. - Москва: Горячая линия-Телеком, 2015.	25
5	Смарт Н. Криптография : пер. с англ. / Н. Смарт. - Москва: Техносфера, 2006.	5
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Розанов Ю. А. Случайные процессы. Краткий курс : учебное пособие для вузов / Ю. А. Розанов. - Москва: Наука, 1971.	4
2	Ч. 1. - Томск: , В-Спектр, Изд-во ТУСУР, 2006. - (Специальные главы математики. (Математические основы криптографии) : учебное пособие; Ч. 1).	5
3	Ч. 2. - Томск: , Изд-во ТУСУР, 2005. - (Специальные главы математики. (Математические основы криптографии) : учебное пособие; Ч. 2).	5
2.2. Периодические издания		
	Не используется	
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
	Не используется	
4. Учебно-методическое обеспечение самостоятельной работы студента		
	Не используется	

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	С. Н. Никифоров Защита информации : Учебное пособие / С. Н. Никифоров. - Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2015.	http://www.iprbookshop.ru/74365.html	локальная сеть; свободный доступ

6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	Windows 10 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Microsoft Office Professional 2007. лиц. 42661567
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017

6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/
Электронно-библиотечеая система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Курсовая работа	Проектор, ноутбук	1
Лекция	Проектор, ноутбук	1
Практическое занятие	Проектор, ноутбук	1

8. Фонд оценочных средств дисциплины

Описан в отдельном документе

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
**«Пермский национальный исследовательский
политехнический университет»**

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся по дисциплине «Криптографические методы защиты информации»
Приложение к рабочей программе дисциплины

Направление подготовки: 01.04.02 «Прикладная математика и информатика»

Направленность (профиль) образовательной программы: «Математическая кибернетика»

Квалификация выпускника: Магистр

Выпускающая кафедра: «Высшая математика»

Форма обучения: Очная

Курс: **2** **Семестр**: **3**

Трудоёмкость:
Кредитов по рабочему учебному плану: 4 ЗЕ
Часов по рабочему учебному плану: 144 ч.

Форма промежуточной аттестации:
Дифференцированный зачет: 3 семестр

Пермь, 2023

Фонд оценочных средств для проведения промежуточной аттестации обучающихся для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

1. Объекты оценивания и виды контроля.

Согласно РПД, освоение учебного материала дисциплины запланировано в течение одного семестра (3-го семестра учебного плана) и разбито на 3 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные и практические занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируются компоненты компетенций *знать, уметь, владеть* указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, выполнении практических заданий, решении расчетно-графических, контрольных работ и экзамена. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВ)	Вид контроля				
	Текущий		Рубежный		Итоговый
	С	ТО		Т/КР	Экзамен
Усвоенные знания					
З.1. Знать основные принципы построения крипто алгоритмов.	$С_1$	$ТО_1$		$КР_1$	ТВ
З.2. Знать основные методы дешифрования; стандарты систем шифрования.	$С_1$			$КР_1$	ТВ
З.3. Знать основные методы дешифрования; стандарты систем шифрования.	$С_2$			$КР_1$	ТВ
З.4. Знать вероятностное шифрование.		$ТО_1$		$КР_1$	ТВ ПЗ
З.5. Знать основные принципы построения криптоалгоритмов, теорему Кука, NP-полноту.		$ТО_2$		$КР_1$	ТВ ПЗ
З.6. Знать классические системы шифрования.	$С_2$			$КР_1$	ТВ
З.7. Знать системы шифрования с симметричным ключом.		$ТО_2$		$КР_2$	ТВ ПЗ
З.8. Знать асимметрические системы шифрования.		$ТО_1$		$КР_2$	ТВ ПЗ
Освоенные умения					
У.1.Уметь строить современные шифрсистемы.				$КР_2$	
У.2. Уметь формулировать постановки задач криптоанализа и находить подходы к их решению.		$ТО_1$		$КР_2$	ТВ
У.3. Уметь строить современные шифрсистемы.				$КР_2$	ПЗ
У.4. Уметь формулировать постановки задач криптоанализа и находить подходы к их решению.		$ТО_2$		$КР_2$	ПЗ
У.5. Уметь использовать основные математические методы, используемые в анализе типовых криптографических алгоритмов.				$КР_2$	ПЗ
У.6. Уметь формулировать постановки задач криптоанализа и находить подходы к их решению.				$КР_2$	ПЗ
Приобретенные владения					
В.1. Владеет криптографической терминологией; методами криптоанализа простейших шифров; современной научно-технической литературой в области криптографической защиты.		$ТО_1$		$КР_2$	ТВ
В.2. Владеть криптографической терминологией; методами криптоанализа простейших шифров; современной научно-технической литературой в области криптографической защиты.		$ТО_2$		$КР_2$	ТВ ПЗ
В.3. Владеть – методами криптоанализа шифров.				$КР_2$	ТВ ПЗ

С – собеседование по теме; ТО - коллоквиум (теоретический опрос); Т/КР – рубежное тестирования (контрольная работа); ТВ - теоретический вопрос экзамена; ПЗ – практическое задание экзамена

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде экзамена, проводимая с учетом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с

Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования

– программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

– входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;

– текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;

– промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

– межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;

– контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений проводится в форме рубежных контрольных работ (после изучения каждого модуля учебной дисциплины).

2.2.1. Рубежная контрольная работа

Согласно РПД запланировано 2 рубежные контрольные работы (КР) после освоения студентами учебных модулей дисциплины. Первая КР по модулю 1 «Симметричные и асимметричные алгоритмы шифрования», вторая КР – по модулю 2 «Криптографические протоколы».

Типовые задания первой КР:

1. В центр пришло зашифрованное сообщение: **ФВМЕЖТИВФЮ.** Найдите исходное сообщение, если известно, что шифрпреобразование заключалось в следующем. Пусть x_1, x_2 – корни многочлена x^2+3x+1. К порядковому номеру каждой буквы в стандартном русском алфавите (33 буквы) прибавлялось значение многочлена $f(x)=x^6+3x^5+x^4+x^3+4x^2+4x+3$, вычисленное либо при $x=x1$ либо при $x=x2$ (в неизвестном порядке), а затем полученное число заменялось

соответствующей ему буквой.

2. Показать слабость итеративной хэш-функции, основанной на раундовой функции, где Mi –блоки данных, hi-раундовое значение хэш-функции, a и p – известные параметры.

Типовые задания второй КР:

1. Предложите свой вариант неинтерактивного протокола доказательства с нулевым разглашением конфиденциальной информации.
2. В чем состоит идея цифровой идентификации?

2.3. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная защита отчетов по всем индивидуальным заданиям, формирующая положительную интегральную оценку результатов текущего и рубежного контроля.

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний и практические задания (ПЗ) для проверки освоенных умений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций. Форма билета представлена в общей части ФОС образовательной программы.

2.3.1. Типовые вопросы и задания для экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Перечислите основные цели, которые преследует криптография.
2. Перечислите основные алгоритмы криптографических преобразований.
3. Объясните понятия «целостности», «подлинности» и «конфиденциальности» информации.
4. Дайте понятие шифра. Расскажите про известные методы симметричного шифрования.
5. Опишите построение шифра гаммирования.
6. Укажите недостатки и достоинства шифров гаммирования.
7. Перечислите основные режимы работы блочных шифров.
8. Опишите отличие архитектуры «Квадрат» от архитектуры обычных блочных шифров. В чем вы видите ее преимущества и недостатки.
9. Дайте определение криптологии.
10. Какие три основных периода криптологии вы знаете?
11. Объясните понятие «криптологический алгоритм».
12. Что такое криптография?
13. Приведите основную классификацию криптографических методов.
14. Какова суть преобразований перестановки и замены?
15. Что собой представляют шифрование и дешифрование?
16. Дайте определение аналитическому преобразованию, гаммированию и комбинированному шифрованию.
17. Что такое системы с открытыми ключами?

18.Приведите структурную схему процесса шифрования с открытым ключом.

19.Дайте определение стойкости криптосистемы.

20.Приведите основные программно-аппаратные реализации шифров.

21.В чем заключается суть DES-алгоритма? Каковы его особенности?

22.В каких режимах может работать DES-алгоритм?

23.Дайте описание отечественного алгоритма криптографического преобразования данных (ГОСТ 28147 — 89) и его отличительных особенностей.

24.Какие режимы имеет отечественный алгоритм криптографического преобразования данных (ГОСТ 28147 — 89)?

25.Чем отличаются поточные симметричные криптографические системы?

26.Какими характеристиками оценивается стойкость криптографических систем?

27.Что такое ключевая система шифра и как организуется протоколирование связи и распределения ключей?

28.В чем заключается суть электронной цифровой подписи?

29.Как проверяется целостность сообщения?

30.Дайте определение эталона ГСЧ. Можно ли говорить, что любой генератор, выдающий числа с одинаковой вероятностью, является эталоном?

31.Приведите классификацию ГСЧ.

32.В чем заключается метод серединных квадратов?

33.В чем заключается метод серединных произведений?

34.В чем заключается метод перемешивания?

35.Дайте определение линейной конгруэнтной последовательности.

36.Укажите отличие мультипликативного метода от линейного конгруэнтного метода.

37.Опишите известные вам методы проверки качества работы ГСЧ.

38.Каким методом можно получить последовательность случайных чисел с наиболее длинным периодом?

39.Дайте определение хэш-функции.

40.В чем отличие между слабой и сильной хэш-функцией?

41.Опишите «парадокс дня рождения». Какие атаки на хэш-функции основаны на этом парадоксе?

42.Опишите алгоритм MD5.

43.Что понимается под простым шифрующим преобразованием?

44.Назовите группы простых шифров.

45.Рационально ли при каскадировании комбинировать две операции, принадлежащие одной группе подряд?

46.Перечислите обратимые процедуры зашифровывания.

47.Приведите схему шифрующего преобразования с линейной структурой.

48.Перечислите требования, предъявляемые к шифрующим преобразованиям общего вида.

49.Приведите схемы стандартного шифрующего преобразования (прямого и обратного).

50.Определите инвариант стандартного шифрующего преобразования.

51.Опишите способ построения раунда шифрования в шифрующих сетях общего типа.

52.Приведите классификацию криптоатак, построенную на данных, известных криптоаналитику.

53.Перечислите возможные угрозы со стороны злоумышленника.

54.Перечислите возможные угрозы со стороны законного отправителя сообщения.

55.Перечислите возможные угрозы со стороны законного получателя сообщения.

56.Опишите классическую задачу криптографии.

57.Опишите задачу подтверждения авторства сообщения.

58.Опишите задачу вручения сообщения под расписку.

59.Перечислите основные теоретические задачи практической криптографии.

60.Укажите отличие абсолютно стойких систем от достаточно стойких систем.

61.Опишите алгоритм криптографического преобразования данных ГОСТ 28147-89.

62.В чем преимущества ГОСТ 28147-89 перед DES?

63.Какие три режима шифрования предусмотрены в ГОСТ 28147-89?

64.Для чего используется имитовставка?

65.Сформулируйте правило Кирхгофа.

66.Укажите преимущества блочных шифров перед поточными.

67.Укажите преимущества поточных шифров перед блочными.

68.Требования, предъявляемые к генераторам ПСП в криптографии.

69.Определите класс языков P.

70.Определите понятие «полиномиальный алгоритм».

71.Дайте определение класса NP.

72.Дайте понятие NP-полного языка.

73.Сформулируйте основное требование для существования односторонних функций.

74.Укажите отличие между эффективно вычислимой и односторонней функцией.

75.Опишите систему вероятностного шифрования.

76.Дайте определение эллиптической кривой над полем

77.Опишите алгоритмы подписи сообщения и проверки подписи сообщения с помощью ECDSA.

78.Что называется криптографическим протоколом?

79.Что называется протоколом доказательства с нулевым разглашением?

80.Опишите алгоритм, реализующий протокол IG.

81.Предложите свой вариант неинтерактивного протокола доказательства с нулевым разглашением конфиденциальной информации.

82.В чем состоит идея цифровой идентификации?

83.Опишите алгоритм схемы Диффи-Хэлмана и приведите пример обмена ключами на основе этого метода.

84.Опишите протокол Шнора.

85.Приведите описание протокола «электронной подписи».

86.Укажите основное отличие стеганографии от симметричного и асимметричного шифрования.

87.Возможно ли использовать стеганографические методы защиты информации совместно с блочным шифрованием?

88.В чем заключается «проблема заключенных»?

89.Что такое «контейнер»?

90.Назовите три основных приложения стеганографии.

91.Назовите основные методы современной компьютерной стеганографии.

Типовые комплексные задания для контроля приобретенных владений:

1. В центр пришло зашифрованное сообщение: **ФВМЕЖТИВФЮ.** Найдите исходное сообщение, если известно, что шифрпреобразование заключалось в следующем. Пусть x_1, x_2 – корни многочлена x^2+3x+1. К порядковому номеру каждой буквы в стандартном русском алфавите (33 буквы) прибавлялось значение многочлена $f(x)=x^6+3x^5+x^4+x^3+4x^2+4x+3$, вычисленное либо при $x=x1$ либо при $x=x2$ (в неизвестном порядке), а затем полученное число заменялось соответствующей ему буквой.

2. Сообщение, записанное в алфавите **АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ** зашифровывается при помощи последовательно букв этого же алфавита. Длина последовательности равна длине сообщения. Шифрование каждой буквы исходного сообщения состоит в сложении ее с порядковым номером соответствующей буквы шифрующей последовательности и замене такой суммы на букву алфавита, порядковый номер которой имеет тот же остаток от деления на 30, что и эта сумма. Восстановите два исходных сообщения, каждое из которых содержит слово «**КОРАБЛИ**», если результат их зашифровывания при помощи одной и той же шифрующей последовательности известен: **ЮПТЦАРГШАЛЖЖЕВЦЩЫРВУУ** и **ЮПЯТБНЩМСДТЛЖГПСГХСЦЦ**.

3. Покажите, что в схеме Файстеля дешифрование является операцией обратной шифрованию.

4. Предположим, что некто предлагает вам следующий способ подтверждения того, что вы лба владеете секретным ключом. Вы создаете строку случайных битов, длина которой равна длине ключа, объединяете эту строку случайных битов с ключом при помощи операции XOR и посылаете результат в канал связи. Ваш партнер с помощью операции XOR объединяет полученный блок с ключом (который должен совпадать с вашим) и возвращает результат. Убедившись, что полученная вами строка совпадает с оригинальной, созданной вами, строкой случайных битов, вы заключаете, что ваш партнер имеет тот же секретный ключ, что и вы, хотя ни один из вас не пересылал секретный ключ другому. Нет ли в этой схеме скрытых дефектов?

5. Показать слабость итеративной хэш-функции, основанной на раунодовой функции $h_i = a^{h_{i-1} \oplus M_i} \bmod p$, где M_i –блоки данных, h_i-раундовое значение хэш-функции, а и р – известные параметры.

6. Показать слабость итеративной хэш-функции, основанной на раундовой функции $h_i = h_{i-1} * a^{M_i} \bmod p$, где M_i –блоки данных, h_i-раундовое значение хэш-функции, a и p – известные параметры, * - операция сложения или умножения по модулю p.

7. Показать слабость итеративной хэш-функции, основанной на раундовой функции $h_i = (h_{i-1} \oplus M_i)^a \bmod p$, где M_i –блоки данных, h_i-раундовое значение хэш-функции, a и p – известные параметры.

8. Что такое коллизия? Приведите пример.

9. Можно ли по дайджесту сообщения восстановить само сообщение?

10. Какой из двух видов шифрования вы предпочтете первый: по исходному сообщению вычисляется хэш-функция, объединяется операцией конкатенации с исходным сообщением и результат шифруется по схеме Файстеля, после чего отправляется адресату; второй вариант: исходное сообщение сперва шифруется по схеме Файстеля, по зашифрованному сообщению вычисляется значение хэш-функции, которое в свою очередь операцией конкатенации присоединяется к зашифрованному сообщению и результат отсылается адресату. Обоснуйте свой ответ.

11. Опишите алгоритм DES. Если произойдет искажение одного бита символа шифрованного текста при передаче в 8-битовом режиме CFB, на сколько блоков распространится это искажение в полученном сообщении?

12. Имеет ли смысл дважды зашифровывать сообщение с помощью алгоритма DES?

13. Что означает утверждение «язык L принадлежит классу NP»?

14. Что можно утверждать, если предположить, что классы P и NP совпадают?

15. Приведите пример однонаправленной функции.

16. Определите однонаправленную функцию с потайным входом. Существенно ли ее отличие от однонаправленной функции?

17. Определите первообразный квадратный корень.

18. Извлечь квадратный корень из чисел 537; 439; 246; 238 по модулю 897.

19. Извлечь кубический корень из чисел 24; 29; 34 по модулю 41.

20. Пусть известно разложение числа p-1, где p есть простое число. Как проверить то, что число a является первообразным корнем?

21. Укажите основную область применения ассиметричного шифрования.

22. Назовите основные отличия симметричных и ассиметричных систем шифрования.

23. Определите шифрование и дешифрование в системе RSA при p=3; q=11; d=7; M=5.

24. Определите шифрование и дешифрование в системе RSA при p=5; q=11; e=3; M=9.

25. Определите шифрование и дешифрование в системе RSA при p=7; q=11; e=17; M=8.

26. Определите шифрование и дешифрование в системе RSA при p=11; q=13; e=11; M=7.

27. Определите шифрование и дешифрование в системе RSA при p=17; q=31; e=7; M=2.

28. В криптосистеме с открытым ключом, использующей RSA, вы перехватили шифрованный текст C=10, пересылаемый пользователю, открытым ключом которого является e=5, n=35. Что в данном случае является открытым текстом?

29. В использующей RSA системе открытым ключом некоторого пользователя является e=31, n=3599. Что будет личным ключом этого пользователя?

30. Предложите вариант слепой подписи с использованием системы ЭЦП Эль-Гамаля.

31. Укажите отличие между доказательством с вычислительно нулевым разглашением и доказательством с абсолютно нулевым разглашением.

32. Укажите отличия параллельного протокола с нулевым разглашением конфиденциальной информации от обычного.

2.3.2. Шкалы оценивания результатов обучения на экзамене

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 4-х балльной шкале оценивания путем выборочного контроля во время экзамена. Соответствие теоретических вопросов, практических заданий и компонентов ЗУВ приведены в табл. 1.1.

При формировании итоговой оценки промежуточной аттестации в виде экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

3.2. Оценка уровня сформированности компетенций

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в виде экзамена используются типовые критерии, приведенные в общей части ФОС

образовательной программы.

Оценка компонента ЗУВ в общем случае может быть получена как *среднее арифметическое или среднее арифметическое взвешенное* (с указанием неравнозначных весовых коэффициентов) оценок за соответствующие средства контроля (см. табл. 1.1).

Итоговая оценка освоения компетенций (как интегральных результатов обучения по дисциплине) является *сверткой* оценок результатов обучения в формате ЗУВ (см. табл. 1.1). Для этого выполняется расчет *среднее арифметического или среднего арифметического взвешенного* (с указанием неравнозначных весовых коэффициентов) оценок за составляющие компоненты ЗУВ.

Рекомендации по выбору весовых коэффициентов, типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций и их самих приведены в общей части ФОС образовательной программы. Результаты расчетов оценок за компетенции сохраняются в «бумажном» или электронном виде для последующего определения уровня освоения каждой компетенции, как это указано в общей части ФОС образовательной программы.