МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

РАБОЧАЯ ПРОГРАММА

Шифр	Наименование дисциплины (модуля)
Б1.В.01.ДВ.08	**Основы криптографии**

Код направления подготовки	44.03.05
Направление подготовки	Педагогическое образование (с двумя профилями подготовки)
Наименование (я) ОПОП (направленность / профиль)	Математика. Информатика
Уровень образования	бакалавр
Форма обучения	очная

Разработчики:

Должность	Учёная степень, звание	Подпись	ФИО
Доцент	кандидат педагогических наук		Паршукова Наталья Борисовна

Рабочая программа рассмотрена и одобрена (обновлена) на заседании кафедры (структурного подразделения)

Кафедра	Заведующий кафедрой	Номер протокола	Дата протокола	Подпись
Кафедра информатики, информационных технологий и методики обучения информатике	Рузаков Андрей Александрович	10	13.06.2019	
Кафедра информатики, информационных технологий и методики обучения информатике	Рузаков Андрей Александрович	1	10.09.2020	

ОГЛАВЛЕНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Дисциплина «Основы криптографии» относится к модулю части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины/модули» основной профессиональной образовательной программы по направлению подготовки 44.03.05 «Педагогическое образование (с двумя профилями подготовки)» (уровень образования бакалавр). Дисциплина является дисциплиной по выбору.

1.2 Общая трудоемкость дисциплины составляет 3 з.е., 108 час.

1.3 Изучение дисциплины «Основы криптографии» основано на знаниях, умениях и навыках, полученных при изучении обучающимися следующих дисциплин: «Информационные технологии», «Методы статистической обработки информации».

1.4 Дисциплина «Основы криптографии» формирует знания, умения и компетенции, необходимые для освоения следующих дисциплин: «Актуальные проблемы защиты информации», «Актуальные проблемы обучения информатике».

1.5 Цель изучения дисциплины:

Формирование у студентов систематизированных знаний в области современной криптографии. Рассмотреть основные широко используемые блочные и поточные шифры, криптографические хеш-функции, шифры с открытым ключом и методы цифровой (электронной) подписи. Познакомить с отечественными государственными стандартами в области криптографической защиты информации.

1.6 Задачи дисциплины:

1) Знать основные понятия шифрования данных для защиты информации в компьютерных сетях
2) Уметь применять методы шифрования данных для защиты информации в компьютерных сетях
3) Владеть технологией шифрования данных для защиты информации в компьютерных сетях
4) Знать основные понятия в области защиты информации
5) Уметь применять методы защиты информации
6) Владеть технологией защиты информации

1.7 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы:

№ п/п	Код и наименование компетенции по ФГОС
	Код и наименование индикатора достижения компетенции
1	ПК-1 способен осваивать и использовать базовые научно-теоретические знания и практические умения по преподаваемому предмету в профессиональной деятельности
	ПК.1.1 Знает содержание, особенности и современное состояние, понятия и категории, тенденции развития соответствующей профилю научной (предметной) области; закономерности, определяющие место соответствующей науки в общей картине мира; принципы проектирования и реализации общего и (или) дополнительного образования по предмету в соответствии с профилем обучения
	ПК.1.2 Умеет применять базовые научно-теоретические знания по предмету и методы исследования в предметной области; осуществляет отбор содержания, методов и технологий обучения предмету (предметной области) в различных формах организации образовательного процесса
	ПК.1.3 Владеет практическими навыками в предметной области, методами базовых научно-теоретических представлений для решения профессиональных задач

№ п/п	Код и наименование индикатора достижения компетенции	Образовательные результаты по дисциплине
1	ПК.1.1 Знает содержание, особенности и современное состояние, понятия и категории, тенденции развития соответствующей профилю научной (предметной) области; закономерности, определяющие место соответствующей науки в общей картине мира; принципы проектирования и реализации общего и (или) дополнительного образования по предмету в соответствии с профилем обучения	З.1 Знать основные понятия шифрования данных для защиты информации в компьютерных сетях З.2 Знать основные понятия в области защиты информации

2	ПК.1.2 Умеет применять базовые научно-теоретические знания по предмету и методы исследования в предметной области; осуществляет отбор содержания, методов и технологий обучения предмету (предметной области) в различных формах организации образовательного процесса	У.1 Уметь применять методы шифрования данных для защиты информации в компьютерных сетях У.2 Уметь применять методы защиты информации
3	ПК.1.3 Владеет практическими навыками в предметной области, методами базовых научно-теоретических представлений для решения профессиональных задач	В.1 Владеть технологией шифрования данных для защиты информации в компьютерных сетях В.2 Владеть технологией защиты информации

2. ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ (МОДУЛЯ) И ВИДОВ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Наименование раздела дисциплины (темы)	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Итого часов
	Л	ЛЗ	СРС	
Итого по дисциплине	**24**	**24**	**60**	**108**
Первый период контроля				
Шифрование с закрытым ключом	***12***	***14***	***30***	***56***
Основные понятия криптографии.	2	2	5	9
Простейшие методы шифрования с закрытым ключом	2	2	5	9
Принципы построения блочных шифров с закрытым ключом	2	2	5	9
Симметричные блочные шифры	2	2	5	9
Многократное блочное шифрование	2	4	5	11
Криптографические хеш-функции	2	2	5	9
Шифрование с открытым ключом	***12***	***10***	***30***	***52***
Введение в криптографию с открытым ключом	2	2	5	9
Алгоритмы шифрования с открытым ключом	2	2	5	9
Электронная цифровая подпись	2	2	5	9
Криптографические способы защиты данных в компьютерных сетях	2	2	5	9
Средства защиты от несанкционированного доступа	2	2	5	9
Коды с исправлением ошибок в криптографии	2		5	7
Итого по видам учебной работы	24	24	60	108
Форма промежуточной аттестации				
Зачет				
Итого за Первый период контроля				**108**

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

3.1 Лекции

Наименование раздела дисциплины (модуля)/ Тема и содержание	**Трудоемкость (кол-во часов)**
1. Шифрование с закрытым ключом	***12***
Формируемые компетенции, образовательные результаты: ПК-1: З.1 (ПК.1.1), З.2 (ПК.1.1), У.1 (ПК.1.2), В.1 (ПК.1.3)	
1.1. Основные понятия криптографии. 1. Предмет и задачи криптографии 2. Основные определения 3. Реализация криптографических методов 4. Криптографические атаки 5. Пример шифра 6. Криптографический протокол 7. Общая схема симметричного шифрования Учебно-методическая литература: 1, 2, 3	2
1.2. Простейшие методы шифрования с закрытым ключом 1. Методы замены: одноалфавитная замена, пропорциональные шифры, многоалфавитные подстановки, методы гаммирования 2. Методы перестановки: - перестановка с фиксированным периодом, - перестановка по таблице Учебно-методическая литература: 1, 2, 3	2
1.3. Принципы построения блочных шифров с закрытым ключом 1. Понятие композиционного шифра 2. Операции, используемые в блочных алгоритмах симметричного шифрования 3. Структура блочного алгоритма симметричного шифрования Учебно-методическая литература: 1, 2, 3	2
1.4. Симметричные блочные шифры 1. Сеть Фейштеля 2. Требования к блочному алгоритму шифрования Учебно-методическая литература: 1	2
1.5. Многократное блочное шифрование 1. Методы криптоанализа блочных шифров 2. Многократное блочное шифрование 3. Параметры современных блоковых шифров Учебно-методическая литература: 1, 2, 3, 4	2
1.6. Криптографические хеш-функции 1. Понятие хеш-функции 2. Использование блочных алгоритмов шифрования для формирования хеш-функции 3. Обзор алгоритмов формирования хеш-функций Учебно-методическая литература: 1, 2, 3	2
2. Шифрование с открытым ключом	***12***
Формируемые компетенции, образовательные результаты: ПК-1: В.2 (ПК.1.3), У.2 (ПК.1.2), З.2 (ПК.1.1)	
2.1. Введение в криптографию с открытым ключом 1. Ассиметричные криптосистемы 2. Криптосистема с открытым ключом 3. Реализация криптосистемы с открытым ключом. Учебно-методическая литература: 1, 2, 3, 4	2

2.2. Алгоритмы шифрования с открытым ключом 1. Алгоритм Эль-Гамаля 2. Основные сведения 3. Шифрование 4. Пример шифрования Учебно-методическая литература: 1, 2, 3	2
2.3. Электронная цифровая подпись 1. Цифровая подпись на основе алгоритмов с открытым ключом 2. Цифровая подпись на основе алгоритма Эль-Гамаля 3. Стандарты на алгоритмы цифровой подписи 4. Новый отечественный стандарт электронной цифровой подписи Учебно-методическая литература: 1, 2, 3	2
2.4. Криптографические способы защиты данных в компьютерных сетях 1. Криптографические протоколы. 2. Сертификаты открытых ключей 3. Безопасность сетевого доступа Учебно-методическая литература: 3, 4	2
2.5. Средства защиты от несанкционированного доступа 1. Способы предотвращения удаленных атак на информационные системы 2. Устройства для защиты от несанкционированного доступа Учебно-методическая литература: 1, 2, 4	2
2.6. Коды с исправлением ошибок в криптографии 1. Введение в коды с исправлением ошибок. 2. Исправление ошибок при передаче данных. 3. Коды Хэмминга для исправления ошибок в криптографических системах Учебно-методическая литература: 1, 2, 4	2

3.2 Лабораторные

Наименование раздела дисциплины (модуля)/ Тема и содержание	**Трудоемкость (кол-во часов)**
1. Шифрование с закрытым ключом	***14***
Формируемые компетенции, образовательные результаты: ПК-1: З.1 (ПК.1.1), З.2 (ПК.1.1), У.1 (ПК.1.2), В.1 (ПК.1.3)	
1.1. Основные понятия криптографии. 1. Методы замены: одноалфавитная замена, пропорциональные шифры, многоалфавитные подстановки, методы гаммирования 2. Методы перестановки: - перестановка с фиксированным периодом, - перестановка по таблице Учебно-методическая литература: 1, 3	2
1.2. Простейшие методы шифрования с закрытым ключом 1. Общая схема симметричного шифрования 2. Методы замены: одноалфавитная замена, пропорциональные шифры, многоалфавитные подстановки, методы гаммирования 3. Методы перестановки: перестановка с фиксированным периодом, перестановка по таблице Учебно-методическая литература: 1, 3	2
1.3. Принципы построения блочных шифров с закрытым ключом 1. Операции, используемые в блочных алгоритмах симметричного шифрования 2. Структура блочного алгоритма симметричного шифрования 3. Сеть Фейштеля 4. Требования к блочному алгоритму шифрования Учебно-методическая литература: 1, 2, 3	2

1.4. Симметричные блочные шифры 1. Изучение алгоритма симметричного блочного шифра. 2. Реализация алгоритма симметричного блочного шифра. Учебно-методическая литература: 1, 2, 3	2
1.5. Многократное блочное шифрование 1. Применение нескольких блочных алгоритмов. 2. Реализация многократного блочного шифрования. Учебно-методическая литература: 1, 2, 3	4
1.6. Криптографические хеш-функции 1. Понятие хеш-функции 2. Использование блочных алгоритмов шифрования для формирования хеш-функции 3. Обзор алгоритмов формирования хеш-функций Учебно-методическая литература: 1, 2, 3	2
2. Шифрование с открытым ключом	***10***
Формируемые компетенции, образовательные результаты: ПК-1: В.2 (ПК.1.3), У.2 (ПК.1.2), З.2 (ПК.1.1)	
2.1. Введение в криптографию с открытым ключом 1. Изучение алгоритмов шифрования с открытым ключом. 2. Дискуссия об эффективности шифрования с открытыми ключами. Учебно-методическая литература: 1, 2	2
2.2. Алгоритмы шифрования с открытым ключом 1. Изучение теории создания алгоритма Эль-Гамаля 2. Разбор алгоритма шифрования Эль-Гамаля 3. Решение задач Учебно-методическая литература: 1, 2, 3	2
2.3. Электронная цифровая подпись 1. Цифровая подпись на основе алгоритмов с открытым ключом 2. Цифровая подпись на основе алгоритма Эль-Гамаля 3. Стандарты на алгоритмы цифровой подписи 4. Новый отечественный стандарт электронной цифровой подписи Учебно-методическая литература: 1, 4	2
2.4. Криптографические способы защиты данных в компьютерных сетях 1. Выступления с докладами по криптографическим способам защиты данных в компьютерных сетях. 2. Дискуссия об уязвимости и защищенности в криптографических системах. Учебно-методическая литература: 2, 3, 4	2
2.5. Средства защиты от несанкционированного доступа 1. Разбор кейсов по обнаружению несанкционированного доступа. 2. Дискуссия о методах защиты данных от несанкционированного доступа. Учебно-методическая литература: 2, 4	2

3.3 СРС

Наименование раздела дисциплины (модуля)/ Тема для самостоятельного изучения	**Трудоемкость (кол-во часов)**
1. Шифрование с закрытым ключом	***30***
Формируемые компетенции, образовательные результаты: ПК-1: З.1 (ПК.1.1), З.2 (ПК.1.1), У.1 (ПК.1.2), В.1 (ПК.1.3)	
1.1. Основные понятия криптографии. ***Задание для самостоятельного выполнения студентом:*** Подготовить ответы на вопросы по лекции 1. Поясните общую схему симметричного шифрования. 2. Что общего имеют все методы шифрования с закрытым ключом? 3. Назовите основные группы методов шифрования с закрытым ключом. 4. Приведите примеры шифров перестановки. 5. Сформулируйте общие принципы для методов шифрования подстановкой. Учебно-методическая литература: 1, 3	5

1.2. Простейшие методы шифрования с закрытым ключом ***Задание для самостоятельного выполнения студентом:*** Подготовить ответы на вопросы по лекции 1. Шифр Цезаря 2. Шифр Виженера Учебно-методическая литература: 1, 2	5
1.3. Принципы построения блочных шифров с закрытым ключом ***Задание для самостоятельного выполнения студентом:*** Решение задач из лабораторных работ. Подготовка отчета. Пример задачи: Расшифруйте сообщения, зашифрованные с помощью шифра Вижинера и ключа OPEX: • ШВМБУЖНЯ, ЯБХЪШЮМХ Учебно-методическая литература: 3	5
1.4. Симметричные блочные шифры ***Задание для самостоятельного выполнения студентом:*** Подготовка отчета по лабораторной работе. Решение задач. Учебно-методическая литература: 3	5
1.5. Многократное блочное шифрование ***Задание для самостоятельного выполнения студентом:*** Подготовка отчета по лабораторной работе. Решение задач. Пример задачи: Зашифровать с использованием сети Фейштелячисла 52 и 39, используя 4 раунда и функцию F(L, n) = (2*L+n) % 256 Учебно-методическая литература: 2, 3	5
1.6. Криптографические хеш-функции ***Задание для самостоятельного выполнения студентом:*** Поточные шифры Принципы использования генераторов псевдослучайных чисел при потоковом шифровании Линейный конгруэнтный генератор псевдослучайных чисел Метод Фибоначчи с запаздыванием Учебно-методическая литература: 1, 2	5
2. Шифрование с открытым ключом	***30***
Формируемые компетенции, образовательные результаты: ПК-1: В.2 (ПК.1.3), У.2 (ПК.1.2), З.2 (ПК.1.1)	
2.1. Введение в криптографию с открытым ключом ***Задание для самостоятельного выполнения студентом:*** Подготовить ответы на вопросы: Проблемы передачи информации и их комплексное решение. Помехоустойчивое кодирование Учебно-методическая литература: 1, 2	5
2.2. Алгоритмы шифрования с открытым ключом ***Задание для самостоятельного выполнения студентом:*** Подготовка отчета по лабораторной работе. Решение задач. Пример задачи: С помощью обобщенного алгоритма Евклида найдите числа x и y, удовлетворяющие уравнению 33x + 16y = НОД(33,16). Учебно-методическая литература: 3	5
2.3. Электронная цифровая подпись ***Задание для самостоятельного выполнения студентом:*** Подготовка отчета по лабораторной работе. Пример решения задачи: абоненты некоторой сети применяют цифровую подпись по алгоритму Эль-Гамаля с общими заданными параметрами P и A.Найдите открытый ключ одного из абонентов сети и вычислите его цифровую подпись для заданного X = 3, значения параметров k и m подобрать самостоятельно. Учебно-методическая литература: 4	5

2.4.	Криптографические способы защиты данных в компьютерных сетях ***Задание для самостоятельного выполнения студентом:*** Плдготовка докладов по криптографической защите в компьютерных сетях. Работа в парах. Вопросы: 1. Идентификация и аутентификация субъектов доступа и объектов доступа 2. Управление доступом субъектов доступа к объектам доступа 3. Ограничение программной среды 4. Защита машинных носителей информации 5. Регистрация событий безопасности 6. Антивирусная защита 7. Обнаружение (предотвращение) вторжений 8. Контроль (анализ) защищенности информации 9. Обеспечение целостности ИС и информации 10. Обеспечение доступности информации 11. Защита среды виртуализации 12. Защита технических средств 13. Защита информационной системы, ее средств, систем связи и передачи данных Учебно-методическая литература: 4	5
2.5.	Средства защиты от несанкционированного доступа ***Задание для самостоятельного выполнения студентом:*** Плдготовка к тесту. Вопросы: 1. Аутентификация 2. Идентификация 3. Защита при администрировании систем: a. обработка регистрационных журналов b. определение прав доступа к ресурсам c. запуск системы защиты на ЭВМ d. демонтированные системы защиты с ЭВМ 4. Способы регистрации событий a. нарушения прав доступа b. вход/выход пользователя из системы 5. Контроль работоспособности и целостности систем защиты 6. Поддержание информационной безопасности при ремонтно-профилактических работах и аварийных ситуациях Учебно-методическая литература: 4	5
2.6.	Коды с исправлением ошибок в криптографии ***Задание для самостоятельного выполнения студентом:*** Подготовка к тесту. Изучение вопросов 1. Введение в коды с исправлением ошибок. 2. Исправление ошибок при передаче данных. 3. Коды Хэмминга для исправления ошибок в криптографических системах Учебно-методическая литература: 2, 4	5

4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Ссылка на источник в ЭБС
Основная литература		
1	Алферов А.П. Основы криптографии / Зубов А.Ю. Кузьмин А.С. Черемушкин А.В. Зубов А.Ю. Кузьмин А.С. Черемушкин А.В. - М.: 2002. - 480 с.	
2	Бескид, П. П. Криптографические методы защиты информации. Часть 1. Основы криптографии : учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург : Российский государственный гидрометеорологический университет, 2010. — 95 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/17925.html (дата обращения: 20.10.2020). — Режим доступа: для авторизир. пользователей	http://www.iprbookshop.ru/17925.html
3	Кукина, Е. Г. Введение в криптографию : сборник задач и упражнений / Е. Г. Кукина, В. А. Романьков. — Омск : Омский государственный университет им. Ф.М. Достоевского, 2013. — 91 c. — ISBN 978-5-7779-1588-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/24876.html (дата обращения: 20.10.2020). — Режим доступа: для авторизир. пользователей	http://www.iprbookshop.ru/24876.html
Дополнительная литература		
4	Криптография и безопасность цифровых систем : учебное пособие / В. Г. Грибунин, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко ; под редакцией А. И. Астайкин. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2011. — 411 c. — ISBN 978-5-9515-0166-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/60851.html (дата обращения: 20.10.2020). — Режим доступа: для авторизир. пользователей	http://www.iprbookshop.ru/60851.html

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

5.1. Описание показателей и критериев оценивания компетенций

Код компетенции по ФГОС				
Код образовательного результата дисциплины	Текущий контроль			Промежуточная аттестация
	Доклад/сообщение	Отчет по лабораторной работе	Тест	Зачет/Экзамен
ПК-1				
З.1 (ПК.1.1)			+	+
З.2 (ПК.1.1)			+	+
У.1 (ПК.1.2)		+		+
У.2 (ПК.1.2)		+		+
В.1 (ПК.1.3)		+		+
В.2 (ПК.1.3)	+			+

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

5.2.1. Текущий контроль.

Типовые задания к разделу "Шифрование с закрытым ключом":

1. Отчет по лабораторной работе

Отчеты по лабораторным работам:
1. Простейшие методы шифрования с закрытым ключом
2. Принципы построения блочных шифров с закрытым ключом
3. Симметричные блочные шифры
4. Многократное блочное шифрование

Количество баллов: 40

2. Тест

Пример1.
Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты:

Пример 2.
Установите последовательность действий для алгоритма Эль-Гамаля:

Пример 3.
Определите ключ шифра Цезаря, если известна следующая пара открытый текст - шифротекст:
ГРУША-ЮЛОУЫ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЪЭЮЯ)

Количество баллов: 20

Типовые задания к разделу "Шифрование с открытым ключом":

1. Доклад/сообщение

Подготовка докладов по следующим темам (работа в парах):

1. Идентификация и аутентификация субъектов доступа и объектов доступа
2. Управление доступом субъектов доступа к объектам доступа
3. Ограничение программной среды
4. Защита машинных носителей информации
5. Регистрация событий безопасности
6. Антивирусная защита
7. Обнаружение (предотвращение) вторжений
8. Контроль (анализ) защищенности информации
9. Обеспечение целостности ИС и информации
10. Обеспечение доступности информации
11. Защита среды виртуализации
12. Защита технических средств
13. Защита информационной системы, ее средств, систем связи и передачи данных

Количество баллов: 10

2. Отчет по лабораторной работе

Подготовить отчеты по лаборыторным работам

1. Алгоритмы шифрования с открытым ключом
2. Электронная цифровая подпись

Количество баллов: 20

3. Тест

Пример 1.

Что такое пространство ключей k?

а) набор возможных значений ключа

б) длина ключа

в) нет правильного ответа

Пример 2.

На какие виды подразделяют криптосистемы?

а) симметричные, ассиметричные, с открытым ключом

б) хэш функции, сети Фейштеля

Пример 3.

Количество используемых ключей в системах с открытым ключом:

а) 2

б) 3

в) 1

Количество баллов: 20

5.2.2. Промежуточная аттестация

Промежуточная аттестация проводится в соответствии с Положением о текущем контроле и промежуточной аттестации в ФГБОУ ВО «ЮУрГГПУ».

Первый период контроля

1. Зачет

Вопросы к зачету:

1. Предмет и задачи криптографии
2. Основные определения
3. Реализация криптографических методов
4. Криптографические атаки
5. Пример шифра Юлия Цезаря
6. Криптографический протокол
7. Общая схема симметричного шифрования
8. Методы замены
9. Одноалфавитная замена
10. Пропорциональные шифры
11. Многоалфавитные подстановки
12. Методы гаммирования
13. Методы перестановки
14. Перестановка с фиксированным периодом

15. Перестановка по таблице
16. Понятие композиционного шифра
17. Операции, используемые в блочных алгоритмах симметричного шифрования
18. Структура блочного алгоритма симметричного шифрования
19. Сеть Фейштеля
20. Требования к блочному алгоритму шифрования
21. Понятие хеш-функции
22. Использование блочных алгоритмов шифрования для формирования хеш-функции
23. Обзор алгоритмов формирования хеш-функций
24. Алгоритмы шифрования с открытым ключом
25. Цифровая подпись на основе алгоритмов с открытым ключом
26. Цифровая подпись на основе алгоритма Эль-Гамаля
27. Стандарты на алгоритмы цифровой подписи
28. Новый отечественный стандарт электронной цифровой подписи
29. Аутентификация
30. Идентификация
31. Защита при администрировании систем
32. Обработка регистрационных журналов
33. Определение прав доступа к ресурсам
34. Запуск системы защиты на ЭВМ
35. Демонтированные системы защиты с ЭВМ
36. Способы регистрации событий: нарушения прав доступа
37. Способы регистрации событий: вход/выход пользователя из системы
38. Введение в коды с исправлением ошибок.
39. Исправление ошибок при передаче данных.
40. Коды Хэмминга для исправления ошибок в криптографических системах

5.3. Примерные критерии оценивания ответа студентов на экзамене (зачете):

Отметка	Критерии оценивания
"Отлично"	- дается комплексная оценка предложенной ситуации - демонстрируются глубокие знания теоретического материала и умение их применять - последовательное, правильное выполнение всех заданий - умение обоснованно излагать свои мысли, делать необходимые выводы
"Хорошо"	- дается комплексная оценка предложенной ситуации - демонстрируются глубокие знания теоретического материала и умение их применять - последовательное, правильное выполнение всех заданий - возможны единичные ошибки, исправляемые самим студентом после замечания преподавателя - умение обоснованно излагать свои мысли, делать необходимые выводы
"Удовлетворительно" ("зачтено")	- затруднения с комплексной оценкой предложенной ситуации - неполное теоретическое обоснование, требующее наводящих вопросов преподавателя - выполнение заданий при подсказке преподавателя - затруднения в формулировке выводов
"Неудовлетворительно" ("не зачтено")	- неправильная оценка предложенной ситуации - отсутствие теоретического обоснования выполнения заданий

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

1. Лекции

Лекция - одна из основных форм организации учебного процесса, представляющая собой устное, монологическое, систематическое, последовательное изложение преподавателем учебного материала с демонстрацией слайдов и фильмов. Работа обучающихся на лекции включает в себя: составление или слежение за планом чтения лекции, написание конспекта лекции, дополнение конспекта рекомендованной литературой.

Требования к конспекту лекций: краткость, схематичность, последовательная фиксация основных положений, выводов, формулировок, обобщений. В конспекте нужно помечать важные мысли, выделять ключевые слова, термины. Последующая работа над материалом лекции предусматривает проверку терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. В конспекте нужно обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.

2. Лабораторные

Лабораторные занятия проводятся в специально оборудованных лабораториях с применением необходимых средств обучения (лабораторного оборудования, образцов, нормативных и технических документов и т.п.).

При выполнении лабораторных работ проводятся: подготовка оборудования и приборов к работе, изучение методики работы, воспроизведение изучаемого явления, измерение величин, определение соответствующих характеристик и показателей, обработка данных и их анализ, обобщение результатов. В ходе проведения работ используются план работы и таблицы для записей наблюдений.

При выполнении лабораторной работы студент ведет рабочие записи результатов измерений (испытаний), оформляет расчеты, анализирует полученные данные путем установления их соответствия нормам и/или сравнения с известными в литературе данными и/или данными других студентов. Окончательные результаты оформляются в форме заключения.

3. Зачет

Цель зачета − проверка и оценка уровня полученных студентом специальных знаний по учебной дисциплине и соответствующих им умений и навыков, а также умения логически мыслить, аргументировать избранную научную позицию, реагировать на дополнительные вопросы, ориентироваться в массиве информации.

Подготовка к зачету начинается с первого занятия по дисциплине, на котором обучающиеся получают предварительный перечень вопросов к зачёту и список рекомендуемой литературы, их ставят в известность относительно критериев выставления зачёта и специфике текущей и итоговой аттестации. С самого начала желательно планомерно осваивать материал, руководствуясь перечнем вопросов к зачету и списком рекомендуемой литературы, а также путём самостоятельного конспектирования материалов занятий и результатов самостоятельного изучения учебных вопросов.

По результатам сдачи зачета выставляется оценка «зачтено» или «не зачтено».

4. Тест

Тест это система стандартизированных вопросов (заданий), позволяющих автоматизировать процедуру измерения уровня знаний и умений обучающихся. Тесты могут быть аудиторными и внеаудиторными. Преподаватель доводит до сведения студентов информацию о проведении теста, его форме, а также о разделе (теме) дисциплины, выносимой на тестирование.

При самостоятельной подготовке к тестированию студенту необходимо:

− проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;

− выяснить все условия тестирования заранее. Необходимо знать, сколько тестов вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.

− работая с тестами, внимательно и до конца прочесть вопрос и предлагаемые варианты ответов; выбрать правильные (их может быть несколько); на отдельном листке ответов выписать цифру вопроса и буквы, соответствующие правильным ответам. В случае компьютерного тестирования указать ответ в соответствующем поле (полях);

− в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.

− решить в первую очередь задания, не вызывающие трудностей, к трудному вопросу вернуться в конце.

− оставить время для проверки ответов, чтобы избежать механических ошибок.

5. Отчет по лабораторной работе

При составлении и оформлении отчета следует придерживаться рекомендаций, представленных в методических указаниях по выполнению лабораторных работ по дисциплине.

6. Доклад/сообщение

Доклад − развернутое устное (возможен письменный вариант) сообщение по определенной теме, сделанное публично, в котором обобщается информация из одного или нескольких источников, представляется и обосновывается отношение к описываемой теме.

Основные этапы подготовки доклада:

1. четко сформулировать тему;
2. изучить и подобрать литературу, рекомендуемую по теме, выделив три источника библиографической информации:

− первичные (статьи, диссертации, монографии и т. д.);

− вторичные (библиография, реферативные журналы, сигнальная информация, планы, граф-схемы, предметные указатели и т. д.);

− третичные (обзоры, компилятивные работы, справочные книги и т. д.);

3. написать план, который полностью согласуется с выбранной темой и логично раскрывает ее;
4. написать доклад, соблюдая следующие требования:

− структура доклада должна включать краткое введение, обосновывающее актуальность проблемы; основной текст; заключение с краткими выводами по исследуемой проблеме; список использованной литературы;

− в содержании доклада общие положения надо подкрепить и пояснить конкретными примерами; не пересказывать отдельные главы учебника или учебного пособия, а изложить собственные соображения по существу рассматриваемых вопросов, внести свои предложения;

5. оформить работу в соответствии с требованиями.

7. ПЕРЕЧЕНЬ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

1. Проблемное обучение
2. Цифровые технологии обучения

8. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ

1. компьютерный класс – аудитория для самостоятельной работы
2. учебная аудитория для лекционных занятий
3. компьютерный класс
4. Лицензионное программное обеспечение:
   - Операционная система Windows 10
   - Microsoft Office Professional Plus
   - Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition
   - Справочная правовая система Консультант плюс
   - 7-zip
   - Adobe Acrobat Reader DC
   - Интернет-браузер