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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ОЦЕНОЧНЫЕ СРЕДСТВА)

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	

Раздел 1. Компетенции обучающегося, формируемые в результате освоения образовательной программы с указанием этапов их формирования

Таблица 1 - Перечень компетенций, с указанием образовательных результатов в процессе освоения дисциплины (в соответствии с РПД)

Формируемые компетенции			
Индикаторы ее достижения	**Планируемые образовательные результаты по дисциплине**		
	знать	**уметь**	**владеть**
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	З.1 Знать основные понятия шифрования данных для защиты информации в компьютерных сетях З.2 Знать основные понятия в области защиты информации		
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	
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

Компетенции связаны с дисциплинами и практиками через матрицу компетенций согласно таблице 2.

Таблица 2 - Компетенции, формируемые в результате обучения

Код и наименование компетенции	
Составляющая учебного плана (дисциплины, практики, участвующие в формировании компетенции)	**Вес дисциплины в формировании компетенции (100 / количество дисциплин, практик)**
ПК-1 способен осваивать и использовать базовые научно-теоретические знания и практические умения по преподаваемому предмету в профессиональной деятельности	
Абстрактная и компьютерная алгебра	1,82
Архитектура компьютера	1,82
Дискретная математика	1,82
Информационные системы	1,82

Исследование операций и методы оптимизации	1,82
Компьютерное моделирование	1,82
Программирование	1,82
Сети и Интернет-технологии	1,82
Математическая логика	1,82
Математический анализ	1,82
Операционные системы	1,82
Основы искусственного интеллекта	1,82
Теоретические основы информатики	1,82
Теория алгоритмов	1,82
Робототехника	1,82
Свободное программное обеспечение	1,82
Виртуальная реальность	1,82
Программирование на языке 1С	1,82
Компьютерная графика	1,82
производственная практика (преддипломная)	1,82
Технологии создания образовательного портала	1,82
Практикум по решению задач школьного курса информатики	1,82
Актуальные проблемы защиты информации	1,82
Основы криптографии	**1,82**
Образовательная робототехника	1,82
Web-дизайн	1,82
Алгебра	1,82
Геометрия	1,82
Методика обучения и воспитания (математика)	1,82
Теория чисел	1,82
Числовые системы	1,82
Элементарная математика	1,82
Вводный курс математики	1,82
Дифференциальная геометрия и топология	1,82
Дифференциальные уравнения	1,82
Практикум по тригонометрии	1,82
Практикум по элементарной алгебре	1,82
Практикум по элементарной геометрии	1,82
Проективная геометрия	1,82
Технологии программирования	1,82
Актуальные проблемы обучения информатике	1,82
Методика обучения и воспитания (информатика)	1,82
Практикум по решению задач на ЭВМ	1,82
Физика	1,82
Теория вероятностей	1,82
Информационные технологии дистанционного обучения	1,82
Базы данных	1,82
Информационно-образовательная среда школы	1,82
учебная практика (проектно-исследовательская работа)	1,82
Методы статистической обработки информации	1,82
Теория функций комплексного и действительного переменного	1,82
Интегрирование дистанционных образовательных технологий в учебном процессе	1,82
Образовательные программы 1С	1,82
Численные методы в программировании	1,82
учебная практика (по математике и информатике)	1,82

Таблица 3 - Этапы формирования компетенций в процессе освоения ОПОП

Код компетенции	**Этап базовой подготовки**	**Этап расширения и углубления подготовки**	**Этап профессионально-практической подготовки**

ПК-1	**Абстрактная и компьютерная алгебра, Архитектура компьютера, Дискретная математика, Информационные системы, Исследование операций и методы оптимизации, Компьютерное моделирование, Программирование, Сети и Интернет-технологии, Математическая логика, Математический анализ, Операционные системы, Основы искусственного интеллекта, Теоретические основы информатики, Теория алгоритмов, Робототехника, Свободное программное обеспечение, Виртуальная реальность, Программирование на языке 1С, Компьютерная графика, производственная практика (преддипломная), Технологии создания образовательного портала, Практикум по решению задач школьного курса информатики, Актуальные проблемы защиты информации, Основы криптографии, Образовательная робототехника, Web-дизайн, Алгебра, Геометрия, Методика обучения и воспитания (математика), Теория чисел, Числовые системы, Элементарная математика, Вводный курс математики, Дифференциальная геометрия и топология, Дифференциальные уравнения, Практикум по тригонометрии, Практикум по элементарной алгебре, Практикум по элементарной геометрии, Проективная геометрия, Технологии программирования, Актуальные проблемы обучения информатике, Методика обучения и воспитания (информатика), Практикум по решению задач на ЭВМ, Физика, Теория вероятностей, Информационные технологии дистанционного обучения, Базы данных, Информационно-образоват**		производственная практика (преддипломная), учебная практика (проектно-исследовательская работа), учебная практика (по математике и информатике)

Раздел 2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 4 - Показатели оценивания компетенций на различных этапах их формирования в процессе освоения учебной дисциплины (в соответствии с РПД)

№	Раздел	
	Формируемые компетенции	
	Показатели сформированности (в терминах «знать», «уметь», «владеть»)	**Виды оценочных средств**
1	Шифрование с закрытым ключом	
	ПК-1	
	Знать знать основные понятия шифрования данных для защиты информации в компьютерных сетях Знать знать основные понятия в области защиты информации	Тест
	Уметь уметь применять методы шифрования данных для защиты информации в компьютерных сетях	Отчет по лабораторной работе
	Владеть владеть технологией шифрования данных для защиты информации в компьютерных сетях	Отчет по лабораторной работе
2	Шифрование с открытым ключом	
	ПК-1	
	Знать знать основные понятия в области защиты информации	Тест
	Уметь уметь применять методы защиты информации	Отчет по лабораторной работе
	Владеть владеть технологией защиты информации	Доклад/сообщение

Таблица 5 - Описание уровней и критериев оценивания компетенций, описание шкал оценивания

Код	**Содержание компетенции**			
Уровни освоения компетенции	**Содержательное описание уровня**	**Основные признаки выделения уровня (критерии оценки сформированности)**	**Пятибаллльная шкала (академическая оценка)**	**% освоения (рейтинговая оценка)**
ПК-1	ПК-1 способен осваивать и использовать базовые научно-теоретические знания и практические умения по преподаваемому предмету в профессиональной деят...			

Высокий (продвинутый)	Творческая деятельность	Обучающийся готов самостоятельно решать стандартные и нестандартные профессиональные задачи в предметной области дисциплины в соответствии с типами задач профессиональной деятельности осваиваемой образовательной программы. 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. Свободно демонстрирует умение 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. Свободно владеет практическими навыками в предметной области, методами базовых научно-теоретических представлений для решения профессиональных задач.	Отлично	91-100
Средний (оптимальный)	Применение знаний и умений в более широких контекстах учебной и профессиональной деятельности, нежели по образцу, с большей степенью самостоятельности и инициативы	Обучающийся готов самостоятельно решать различные стандартные профессиональные задачи в предметной области дисциплины в соответствии с типами задач профессиональной деятельности осваиваемой образовательной программы. 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, допускает незначительные ошибки. Демонстрирует умения 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. Уверенно владеет практическими навыками в предметной области, методами базовых научно-теоретических представлений для решения профессиональных задач, допускает незначительные ошибки.	Хорошо	71-90

Пороговый	Репродуктивная деятельность	Обучающийся способен решать необходимый минимум стандартных профессиональных задач в предметной области дисциплины в соответствии с типами задач профессиональной деятельности осваиваемой образовательной программы. 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, не демонстрирует глубокого понимания материала. В основном демонстрирует умения 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. Владеет практическими навыками в предметной области, методами базовых научно-теоретических представлений для решения профессиональных задач, допускает ошибки.	Удовлетворительно	51-70
Недостаточный	Отсутствие признаков удовлетворительного уровня		Неудовлетворительно	50 и менее

Раздел 3. Типовые контрольные задания и (или) иные материалы, необходимые для оценки планируемых результатов обучения по дисциплине (модулю)

1. Оценочные средства для текущего контроля

Раздел: Шифрование с закрытым ключом

Задания для оценки знаний

1. 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)

Приложение 1.
Опорные вопросы по разделу "Шифрование с закрытым ключом"

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.
6. В чем заключаются многоалфавитные подстановки?
7. Приведите пример шифра одноалфавитной замены.
8. Опишите алгоритм любого метода шифрования перестановкой. Приведите пример шифрования некоторого сообщения этим методом. Каков алгоритм расшифрования в этом методе?
9. К какой группе методов шифрования с закрытым ключом относится метод с использованием таблицы Вижинера? Каковы алгоритмы шифрования и расшифрования в этом методе? Приведите пример шифрования некоторого сообщения этим методом.
10. Каким образом можно зашифровать и расшифровать сообщение методом табличной перестановки, если размер шифруемого сообщения не кратен размеру блока?
11. Что такое монофонические шифры?Понятие об информационных системах.
12. Какой шифр называют комбинированным или композиционным шифром?
13. Какие факторы влияют на стойкость блочного алгоритма шифрования?
14. Какие простейшие операции применяются в блочных алгоритмах шифрования?
15. В чем отличие блочных алгоритмов шифрования от поточных?
16. Что понимается под "раундом" алгоритма шифрования?
17. Каковы требования к блочному алгоритму шифрования?
18. Почему блочный алгоритм шифрования должен иметь простую и понятную структуру?
19. Что понимается под требованием "высокой криптостойкости" алгоритма шифрования?
20. Что представляет собой сеть Фейштеля?

Задания для оценки умений

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

Приложение 1.
Задачи по разделу "Шифрование с закрытым ключом"

1. Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2.

Расшифруйте сообщения, зашифрованные с помощью шифра №1
- И.РЮУ.ЪФОБГНО
- СЛХГ.ЪЛХО.ФОО.ЩВ

Расшифруйте сообщение, зашифрованное с помощью шифра №2:

2. Пусть исходный алфавит содержит следующие символы:
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО сообщения:
- КРИПТОСТОЙКОСТЬ
- ГАММИРОВАНИЕ

3. Пусть исходный алфавит состоит из следующих знаков (символ "_" (подчеркивание) будем использовать для пробела):
АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_
Расшифруйте сообщения, зашифрованные с помощью шифра Вижинера и ключа ОРЕХ:
- ШВМБУЖНЯ
- ЯБХЪШЮМХ

4. Первый байт фрагмента текста в шестнадцатеричном виде имеет вид А5. На него накладывается по модулю два 4-х битовая гамма 0111 (в двоичном виде). Что получится после шифрования?

5. Первый байт фрагмента текста, зашифрованного методом гаммирования (по модулю 2), в шестнадцатеричном виде имеет вид 9А. До шифрования текст имел первый байт, равный 74 (в шестнадцатеричном виде). Какой ключ использовался при шифровании?

6. Зашифруйте методом перестановки с фиксированным периодом d=6 с ключом 436215 сообщения:
- ЖЕЛТЫЙ_ОГОНЬ
- МЫ_НАСТУПАЕМ

7. Расшифруйте сообщения, зашифрованные методом перестановки с фиксированным периодом d=8 с ключом 64275813:
- СЛПИЬНАЕ
- РОИАГДВН

8. Определите ключи в системе шифрования, использующей перестановку с фиксированным периодом d=5 по парам открытых и зашифрованных сообщений:
- МОЙ ПАРОЛЬ – ЙПМ ООЬАЛР
- СИГНАЛ БОЯ – НИСАГО ЛЯБ

9. Зашифруйте сообщения методом перестановки по таблице 5*5. Ключ указывает порядок считывания столбцов при шифровании.
- ШИРОКОПОЛОСНЫЙ УСИЛИТЕЛЬ (ключ: 41235)
- ПЕРЕДАЧА ИЗОБРАЖЕНИЯ (ключ: 24513)

10. Расшифруйте сообщения, зашифрованные методом перестановки по таблице 4*4 (символ подчеркивания заменяет пробел). Ключ указывает порядок считывания столбцов при шифровании.
- АННУНТАОАЬ_ПЖ_КК (ключ: 4123)
- ЕЬ_ЫПООЗБШВВРЛЙР (ключ: 3142)

11. Известно, что при использовании шифра пропорциональной замены каждой русской букве поставлено в соответствие одно или несколько трехзначных чисел по таблице замен:
Таблица замен для пропорционального шифра

Расшифруйте указанные сообщения.
- 353214764134136759136762849754128212350354035767106216753211
- 351 761756130532128759353134758105757213101752352763211762

Задания для оценки владений

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

Приложение 1.
Задачи по разделу "Шифрование с закрытым ключом"

1. Имеется таблица замены для двух шифров простой замены: шифра №1 и шифра №2.

Расшифруйте сообщения, зашифрованные с помощью шифра №1
- И.РЮУ.ЪФОБГНО
- СЛХГ.ЪЛХО.ФОО.ЩВ

Расшифруйте сообщение, зашифрованное с помощью шифра №2:

2. Пусть исходный алфавит содержит следующие символы:
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО сообщения:
- КРИПТОСТОЙКОСТЬ
- ГАММИРОВАНИЕ

3. Пусть исходный алфавит состоит из следующих знаков (символ "_" (подчеркивание) будем использовать для пробела):
АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_
Расшифруйте сообщения, зашифрованные с помощью шифра Вижинера и ключа ОРЕХ:
- ШВМБУЖНЯ
- ЯБХЪШЮМХ

4. Первый байт фрагмента текста в шестнадцатеричном виде имеет вид A5. На него накладывается по модулю два 4-х битовая гамма 0111 (в двоичном виде). Что получится после шифрования?

5. Первый байт фрагмента текста, зашифрованного методом гаммирования (по модулю 2), в шестнадцатеричном виде имеет вид 9A. До шифрования текст имел первый байт, равный 74 (в шестнадцатеричном виде). Какой ключ использовался при шифровании?

6. Зашифруйте методом перестановки с фиксированным периодом d=6 с ключом 436215 сообщения:
- ЖЕЛТЫЙ_ОГОНЬ
- МЫ_НАСТУПАЕМ

7. Расшифруйте сообщения, зашифрованные методом перестановки с фиксированным периодом d=8 с ключом 64275813:
- СЛПИЬНАЕ
- РОИАГДВН

8. Определите ключи в системе шифрования, использующей перестановку с фиксированным периодом d=5 по парам открытых и зашифрованных сообщений:
- МОЙ ПАРОЛЬ – ЙПМ ООЬАЛР
- СИГНАЛ БОЯ – НИСАГО ЛЯБ

9. Зашифруйте сообщения методом перестановки по таблице 5*5. Ключ указывает порядок считывания столбцов при шифровании.
- ШИРОКОПОЛОСНЫЙ УСИЛИТЕЛЬ (ключ: 41235)
- ПЕРЕДАЧА ИЗОБРАЖЕНИЯ (ключ: 24513)

10. Расшифруйте сообщения, зашифрованные методом перестановки по таблице 4*4 (символ подчеркивания заменяет пробел). Ключ указывает порядок считывания столбцов при шифровании.
- АННУНТАОАЬ_ПЖ_КК (ключ: 4123)
- ЕЬ_ЫПООЗБШВВРЛЙР (ключ: 3142)

11. Известно, что при использовании шифра пропорциональной замены каждой русской букве поставлено в соответствие одно или несколько трехзначных чисел по таблице замен:
Таблица замен для пропорционального шифра

Расшифруйте указанные сообщения.
- 353214764134136759136762849754128212350354035767106216753211
- 351 761756130532128759353134758105757213101752352763211762

Раздел: Шифрование с открытым ключом

Задания для оценки знаний

1. 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

Приложение 1.
Тест по разделу "Шифрование с открытым ключом"

1. Алгоритмы шифрования с открытым ключом по-другому называются

1) асимметричными алгоритмами шифрования
2) симметричными алгоритмами шифрования
3) односторонними алгоритмами шифрования
4) помехоустойчивыми алгоритмами шифрования

2. Асимметричные алгоритмы шифрования по-другому называются

5) алгоритмами шифрования с открытым ключом
6) симметричными алгоритмами шифрования
7) односторонними алгоритмами шифрования
8) помехоустойчивыми алгоритмами шифрования

3. Когда в криптографии стало использоваться асимметричное шифрование?

1) в первой половине XIX;
2) во второй половине XIX;
3) в первой половине XX;
4) во второй половине XX

4. Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии

1) криптографической функцией
2) односторонней функцией
3) функцией Диффи-Хеллмана
4) функцией Эйлера

5. Односторонние функции, то есть функции, которые относительно легко вычислить, но практически невозможно найти по значению функции соответствующее значение аргумента, можно использовать для

1) формирования хеш-кодов
2) шифрования сообщений
3) формирования цифровой подписи
4) контроля и исправления ошибок при передаче информации

6. Односторонние функции с люком можно использовать для

5) формирования хеш-кодов
6) шифрования сообщений
7) формирования цифровой подписи
8) контроля и исправления ошибок при передаче информации

7. Что является особенностью систем шифрования с открытым ключом по сравнению с симметричными системами шифрования?

1) возможность шифрования как текстовой, так и графической информации
2) высокая скорость процессов шифрования/расшифрования
3) использование малого количества вычислительных ресурсов

4) отсутствие необходимости предварительной передачи секретного ключа по надёжному каналу связи

8. Для решения каких задач можно использовать алгоритмы шифрования с открытым ключом?

1) для шифрования передаваемых и хранимых данных в целях их защиты от несанкционированного доступа
2) для формирования цифровой подписи под электронными документами
3) для распределения секретных ключей, используемых потом при шифровании документов симметричными методами
4) для помехоустойчивого кодирования передаваемых сообщений

9. Что является недостатком системы шифрования с открытым ключом?

1) низкая скорость процессов шифрования-расшифрования
2) необходимость обновления ключа после каждого факта передачи
3) отсутствие необходимости предварительной передачи секретного ключа по надёжному каналу
4) необходимость предварительной передачи секретного ключа по надёжному каналу

10. Что называют закрытым ключом в асимметричных методах шифрования?
1) ключ, который должен храниться в секрете
2) ключ, который необязательно хранить в секрете
3) любой ключ, используемый для шифрования или расшифрования
4) ключ, который используется для выработки имитовставки

11. Что называют открытым ключом в асимметричных методах шифрования?

1) ключ, который должен храниться в секрете
2) ключ, который не обязательно хранить в секрете
3) любой ключ, используемый для шифрования или расшифрования
4) ключ, который используется для выработки имитовставки

12. Как называется ключ, используемый в асимметричных криптографических алгоритмах, который можно не хранить в секрете?

1) закрытый ключ
2) открытый ключ
3) тайный ключ
4) явный ключ
5) (5) ключ шифрования

13. Сколько ключей используется в криптографических алгоритмах с открытым ключом?

1) ноль
2) один
3) два
4) три

14. Что общего имеют все методы шифрования с закрытым ключом?

1) в них для шифрования информации используется один ключ, а для расшифрования – другой ключ
2) в них для шифрования и расшифрования информации используется один и тот же ключ
3) в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов
4) в них для операций шифрования и расшифрования используется два разных ключа – открытый и закрытый

15. Что общего имеют все методы шифрования с открытым ключом?

1) в них для шифрования информации используется один ключ, а для расшифрования – другой ключ
2) в них для шифрования и расшифрования информации используется один и тот же ключ
3) в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов
4) эти методы позволяют производить коррекцию ошибок при передаче по зашумленным каналам связи

16. Укажите требования к алгоритмам шифрования с открытым ключом

1) вычислительно легко создавать пару (открытый ключ, закрытый ключ)
2) вычислительно легко зашифровать сообщение открытым ключом
3) вычислительно легко, зная открытый ключ, определить соответствующий закрытый ключ
4) вычислительно легко, зная только открытый ключ и зашифрованное сообщение, восстановить исходное сообщение

17. Укажите требования к алгоритмам шифрования с открытым ключом

1) вычислительно невозможно создавать пару (открытый ключ, закрытый ключ)
2) вычислительно невозможно зашифровать сообщение открытым ключом
3) вычислительно невозможно, зная открытый ключ, определить соответствующий закрытый ключ
4) вычислительно невозможно, зная только открытый ключ и зашифрованное сообщение, восстановить исходное сообщение

18. Укажите требования к алгоритмам шифрования с открытым ключом

1) вычислительно легко зашифровать сообщение открытым ключом
2) вычислительно легко расшифровать сообщение, используя закрытый ключ
3) вычислительно невозможно, зная открытый ключ, определить соответствующий закрытый ключ
4) вычислительно невозможно, зная только открытый ключ и зашифрованное сообщение, восстановить исходное сообщение

19. Какие ключи и как должны применяться при использовании асимметричных криптографических алгоритмов для шифрования передаваемых данных?

1) отправитель шифрует сообщение открытым ключом получателя, а получатель расшифровывает сообщение своим закрытым ключом
2) отправитель шифрует сообщение закрытым ключом получателя, а получатель расшифровывает сообщение своим открытым ключом
3) отправитель шифрует сообщение своим открытым ключом, а получатель расшифровывает сообщение закрытым ключом отправителя
4) отправитель шифрует сообщение своим закрытым ключом, а получатель расшифровывает сообщение открытым ключом отправителя

20. Какие ключи и как должны применяться при использовании асимметричных криптографических алгоритмов для формирования электронной цифровой подписи?

1) отправитель использует для шифрования открытый ключ получателя, а получатель использует для расшифрования свой закрытый ключ
2) отправитель использует для шифрования закрытый ключ получателя, а получатель использует для расшифрования свой открытый ключ
3) отправитель использует для шифрования свой открытый ключ, а получатель использует для расшифрования закрытый ключ отправителя
4) отправитель использует для шифрования свой закрытый ключ, а получатель использует для расшифрования открытый ключ отправителя

21. Какие ключи и как должны применяться при использовании асимметричных криптографических алгоритмов для шифрования сеансовых ключей?

1) отправитель шифрует сеансовый ключ открытым ключом получателя, а получатель расшифровывает полученный ключ своим закрытым ключом
2) отправитель шифрует сеансовый ключ закрытым ключом получателя, а получатель расшифровывает полученный ключ своим открытым ключом
3) отправитель шифрует сеансовый ключ своим открытым ключом, а получатель расшифровывает полученный ключ закрытым ключом отправителя
4) отправитель шифрует сеансовый ключ своим закрытым ключом, а получатель расшифровывает полученный ключ открытым ключом отправителя

22. Каким требованиям должна удовлетворять электронная цифровая подпись?

1) подпись воспроизводится только одним лицом, а подлинность ее может быть удостоверена многими
2) подпись воспроизводится многими лицами, а ее подлинность может быть удостоверена только одним лицом
3) подпись неразрывно связывается с данным сообщением и не может быть перенесена на другой документ

4) подпись не связывается с конкретным сообщением и может быть перенесена на другой документ

23. Каким требованиям должна удовлетворять электронная цифровая подпись?

1) после того, как документ подписан, его невозможно изменить
2) после того, как документ подписан, его можно изменять
3) подпись неразрывно связывается с данным сообщением и не может быть перенесена на другой документ
4) подпись не связывается с конкретным сообщением и может быть перенесена на другой документ

24. Каким требованиям должна удовлетворять электронная цифровая подпись?

1) от поставленной подписи невозможно отказаться, то есть лицо, подписавшее документ, не сможет потом утверждать, что не ставило подпись
2) подпись воспроизводится многими лицами, а ее подлинность может быть удостоверена только одним лицом
3) подпись неразрывно связывается с данным сообщением и не может быть перенесена на другой документ
4) подпись не связывается с конкретным сообщением и может быть перенесена на другой документ

Задания для оценки умений

1. Отчет по лабораторной работе:

Подготовить отчеты по лаборыторным работам
1. Алгоритмы шифрования с открытым ключом
2. Электронная цифровая подпись

Приложение 1.
Задания к лабораторной работе
1. Пусть Mi – блок исходного сообщения, hi – значение хеш-функции на i-том этапе, g – блочный алгоритм шифрования, используемый в режиме простой замены (см.таблицу), – поразрядная операция сложения по модулю 2. Для каждого сообщения найдите хеш-код, используя значение хеш-функции и схему формирования хеш-функций:hi=g(Mi hi-1) hi-1.
2. Вычислите закрытые ключи Y1, Y2 и общий ключ Z для системы Диффи-Хеллмана с параметрами A, P, X1, X2, приведенными в таблице. Опишите процесс формирования общего ключа.

Задания для оценки владений

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

2. Оценочные средства для промежуточной аттестации

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

Раздел 4. Методические материалы, определяющие процедуры оценивания значни, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1. Для текущего контроля используются следующие оценочные средства:

1. 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.

2. Отчет по лабораторной работе

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

3. 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.

2. Описание процедуры промежуточной аттестации

Оценка за зачет/экзамен может быть выставлена по результатам текущего рейтинга. Текущий рейтинг – это результаты выполнения практических работ в ходе обучения, контрольных работ, выполнения заданий к лекциям (при наличии) и др. видов заданий.

Результаты текущего рейтинга доводятся до студентов до начала экзаменационной сессии.

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.

Зачет может проводиться как в формате, аналогичном проведению экзамена, так и в других формах, основанных на выполнении индивидуального или группового задания, позволяющего осуществить контроль знаний и полученных навыков.

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».