МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
декан факультета прикладной математики, информатики и механики

_____А.И. Шашкин
подпись, расшифровка подписи

24.06.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ Б1.О.54.03 Программная реализация криптоалгоритмов

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

Математические методы защиты информации

3. Квалификация (степень) выпускника: Специалист по защите информации

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

ERP-систем и бизнес-процессов

6. Составители программы:

Сафронов Виталий Владимирович, доцент кафедры ERP-систем и бизнес-процессов

7. **Рекомендована:** Научно-методическим советом факультета прикладной математики, информатики и механики 15.06.2021 г., протокол № 10

8. Учебный год: 2023/2024 **Семестр(ы):** 6

9. Цели и задачи учебной дисциплины

Цель: освоение студентами принципов криптографических преобразований и методов программной реализации криптоалгоритмов, применяемых при защите компьютерных систем

Задачи:

– ознакомить студентов с математическими принципами криптографических преобразований для наилучшего понимания построения криптографических систем;

– ознакомить студентов с наиболее известными криптоалгоритмами с симметричным и асимметричным ключом, их применением;

– ознакомить студентов с функциями хеширования, их использования в криптографии;

– обучить студентов основным методам программной реализацией криптоалгоритмов;

– обучить студентов методам программной реализации криптографической защиты при передаче информации по незащищенному каналу;

– обучить студентов основам методов криптоанализа и условий их применения;

– обучить студентов универсальным методам классической стеганографии и условиями их применения, а также ознакомить с практической реализацией алгоритмов стеганографии.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к обязательной части блока Б1 дисциплин учебного плана.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ОПК-8	*Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей*	ОПК-8.15	Умеет применять методы экспериментального исследования при решении профессиональных задач	Знание: основных современных криптографических протоколов, используемых в информационных сетях передачи данных; принципов работы шифров; методов разработки криптографических протоколов. Умение: разрабатывать математические модели криптографических протоколов и реализовывать их на современном языке программирования; разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств. Владение: подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализациикриптографических протоколов,
ОПК-2.1	*Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации.*	ОПК-2.1.5	Способен разрабатывать программные алгоритмы с применением математических моделей для оценки безопасности компьютерных систем.	
ОПК-2.2	*Способен разрабатывать и анализировать математически е модели механизмов защиты информации*	ОПК-2.2.6	Разрабатывает математические модели для оценки безопасности компьютерных систем	

ОПК-2.3	*Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математически х методов*	ОПК-2.3.3	Проводит оценку эффективности программных, программно-аппаратных и технических средств, подсистем защиты информации.	моделирования с помощьюсовременных языков программирования и математических пакетов современных криптографических протоколов.

12. Объем дисциплины в зачетных единицах/час - 3/108.
Форма промежуточной аттестации – зачет с оценкой, курсовая работа.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			6			
Аудиторные занятия	54		54			
в том числе: лекции	18		18			
Практические	0		0			
Лабораторные	36		36			
Самостоятельная работа	54		54			
Контроль						
Итого:	108		108			
Форма промежуточной аттестации	Зачет с оценкой, КР		Зачет с оценкой, КР			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Криптография как аспект информационной безопасности.	Криптография как один из аспектов информационной безопасности. Основы криптографии. Терминология. Введение в криптоанализ.	https://edu.vsu.ru/course/view.php?id=29545

1.2	Классификация криптоалгоритмов.	Классификация криптоалгоритмов. Простейшие криптографические алгоритмы. Принципы построения симметричных криптографических систем.	
1.3	Современные криптографические протоколы.	Криптографическая реализация блочного симметричного шифра DES. Криптографическая реализация блочного симметричного шифра AES. Асимметричные криптографические системы.	
1.4	Реализация криптографических протоколов в современных языках программирования	Криптографические библиотеки. Методы использования криптографических протоколов при написании программ. Разработка и отладка механизмов взаимодействия клиент-сервер с использованием криптографических протоколов.	
2. Лабораторные работы			
2.1	Реализация работы криптографических протоколов	Реализация алгоритма двойной перестановки. Реализация алгоритма шифрования Виженера. Реализация ассиметричного алгоритма шифрования RSA.	https://edu.vsu.ru/course/view.php?id=29545
2.2	Анализ свойств криптографической системы	Исследование свойств программного генератора случайных чисел.	
2.3	Методы стеганографии	Использование стеганографических методов шифрования информации.	
2.4	Моделирование инфраструктуры открытых ключей	Изучение работы программ для формирования и работы с ЭЦП на примере программного продукта Kleopatra.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Криптография как аспект информационной безопасности.	4		0	4		8
1.2	Классификация криптоалгоритмов.	4		0	4		8
1.3	Современные криптографические протоколы.	6		0	6		12
1.4	Реализация криптографических протоколов в современных языках программирования	4			4		8
2.1	Реализация работы криптографических протоколов	0		18	18		36
2.2	Анализ свойств криптографической системы	0		6	6		12
2.3	Методы стеганографии	0		8	8		16
2.4	Моделирование инфраструктуры открытых ключей	0		4	4		8
	Итого:	18		36	54		108

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторные занятия и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины. Лабораторные занятия предназначены для формирования умений и навыков, закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор лабораторных заданий, подготовку к экзамену.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Корниенко, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Корниенко, М. Л. Глухарев. – Санкт-Петербург : ПГУПС, [б. г.]. – Часть 1 – 2017. – 64 с. – ISBN 978-5-7641-1053-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/111765 (дата обращения: 10.02.2020). – Режим доступа: для авториз. пользователей.
2	Корниенко, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Корниенко, М. Л. Глухарев. – Санкт-Петербург : ПГУПС, 2018 – Часть 2 – 2018. – 63 с. – ISBN 978-5-7641-1215-2. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/138103 (дата обращения: 10.02.2020). – Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
3	Пугин, В. В. Криптографические протоколы : учебное пособие / В. В. Пугин. – Самара : ПГУТИ, 2019. – 68 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/223319 (дата обращения: 20.01.2020). – Режим доступа: для авториз. пользователей.
4	Салий В. Н. Криптографические методы и средства защиты информации / В. Н. Салий. – 2010. (URL:http://www.sgu.ru/files/nodes/11017/V.N._Saliy._Kriptograficheskie_metody_i_sredstva_zashchity_informacii.doc) (дата обращения: 12.05.2019)

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
5	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
6	Электронный каталог Научной библиотеки Воронежского государственного университета. - Режим доступа: http//:www.lib.vsu.ru.
7	Криптографические протоколы (10.05.01)/Степанец Ю.А. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа

студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по лабораторным работам, подготовка к экзамену.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению заданий лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение)

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Программная реализация криптоалгоритмов (10.05.01)» - https://edu.vsu.ru/course/view.php?id=29545 размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины

Учебная аудитория для лекций: специализированная мебель, компьютер преподавателя, мультимедийный проектор, экран.
Учебная аудитория для лабораторных занятий: специализированная мебель, персональные компьютеры, мультимедийный проектор, экран, лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности.
Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

Программное обеспечение (см.файл МТО): ОС Windows v.7, 8, 10, набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader, программа для виртуализации Oracle VirtualBox, среда разработки Visual Studio

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Криптография как аспект информационной безопасности.	ОПК-8	ОПК-8.15	Тестирование
2	Классификация криптоалгоритмов.	ОПК-8	ОПК-8.15	Тестирование
3	Современные криптографические протоколы.	ОПК-8	ОПК-8.15	Тестирование
4	Реализация криптографических протоколов в современных языках программирования	ОПК-2.1	ОПК-2.1.5	Тестирование
5	Реализация работы криптографических протоколов	ОПК-2.1	ОПК-2.1.5	Лабораторные работы

6	Анализ свойств криптографической системы	ОПК-2.2	ОПК-2.2.6	Лабораторные работы
7	Методы стеганографии	ОПК-2.1	ОПК-2.1.5	Лабораторные работы
8	Моделирование инфраструктуры открытых ключей	ОПК-2.3	ОПК-2.3.3	Лабораторные работы
Промежуточная аттестация, форма контроля - зачет с оценкой				Перечень вопросов (КИМ №1)

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- тестирование,
- лабораторные работы,
- курсовые работы.

Перечень тем для проведения тестирования:

1. Составляющие информационной безопасности.
2. Атаки на информационную систему.
3. Противодействие компьютерным атакам.
4. Основные определения и терминология криптографии.
5. Проблемы криптографии.
6. Стойкость криптосистем.
7. Виды криптографических атак.
8. Классические и современные методы криптоанализа.
9. Классификация криптоалгоритмов по типу преобразования исходного текста.
10. Классификация криптоалгоритмов с точки зрения количества ключей.
11. Моноалфавитные и полиалфавитные шифры подстановки.
12. Роторные машины.
13. Шифры простой и сложной перестановки.
14. Одноразовая система шифрования с использованием ключевого блокнота.
15. Шифрование методом гаммирования.
16. Шифр Хилла.
17. Блочные симметричные криптографические алгоритмы.
18. Сеть Фейстеля.
19. Блочный шифр DES.
20. Блочный шифр AES.
21. Асимметричный алгоритм шифрования RSA.

Технология проведения

Студент получает десять вопросов с тремя вариантами ответов. Выбирает вариант ответа, ориентируясь на свои знания. Необходимо ответить на все вопросы. По результатам теста выставляется оценка. За каждый правильный ответ начисляется 2 балла, что соответствует 10% правильных ответов.

Критерии оценивания

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Необходимо набрать минимум 90% правильных ответов	Повышенный уровень	Отлично
Необходимо набрать минимум 70% правильных ответов	Базовыйуровень	Хорошо
Необходимо набрать минимум 50% правильных ответов	Пороговыйуровень	Удовлетворительно
Набрано меньше 50% правильных ответов	–	Неудовлетворительно

Перечень лабораторных работ

1	Лабораторная работа №1 Тема: Программная реализация алгоритма двойной перестановки.	*Теоретические сведения* 1. Определение шифра перестановки. 2. Шифр перестановки, основанный на шифре «Решетка Кардано». 3. Шифр двойной перестановки. *Практическая часть* Реализация алгоритма двойной перестановки с помощью какого-либо языка программирования. Программа должна осуществлять шифрование и расшифровку по приведенному алгоритму, вывод на экран незашифрованного, зашифрованного и расшифрованного сообщения.
2	Лабораторная работа №2 Тема: Программная реализация алгоритма шифрования Виженера.	*Теоретические сведения* 1. Определение шифра Виженера. 2. Реализация шифра Виженера с помощью таблицы. 3. Реализация шифра Виженера с помощью формул. 4. Криптоанализ шифра Виженера. *Практическая часть* Реализация алгоритма шифрования Виженера с помощью какого-либо языка программирования. Программа должна осуществлять шифрование и расшифровку по приведенному алгоритму, вывод на экран незашифрованного, зашифрованного и расшифрованного сообщения.
3	Лабораторная работа №3 Тема: Программная реализация асимметричного алгоритма шифрования RSA.	*Теоретические сведения* 1. Системы шифрования с открытым ключом. 2. Преимущества и недостатки СОК. 3. Алгоритм шифрования RSA. 4. Схема шифрования по алгоритму RSA. *Практическая часть* Реализация алгоритма асимметричного шифрования RSA с помощью какого-либо языка программирования. Программа должна вычислять числа n, φ(n), e, d, осуществлять шифрование и расшифровку по приведенному алгоритму, вывод на экран незашифрованного, зашифрованного и расшифрованного сообщения, открытый и закрытые ключи, а также число φ(n).
4	Лабораторная работа №4 Тема: Исследование свойств программного генератора случайных чисел.	*Теоретические сведения* 1. Генераторы случайных чисел. 2. Генератор Блюм-Блюм-Шуба. 3. Тесты проверки на случайность: - частотный тест; - тест на последовательность одинаковых бит. *Практическая часть* Реализация программы позволяющей сгенерировать последовательность псевдослучайных чисел (ПСЧ) используя программный генератор ПСЧ и проверить на «истинную» случайность с помощью статистических тестов.
5	Лабораторная работа №5 Тема: Использование стеганографических методов шифрования информации.	*Теоретические сведения* 1. Понятие стеганографии. 2. Частотные методы стеганографии. 3. Пространственные методы стеганографии. 4. Преимущества и недостатки стеганографии. 5. Реализация метода стеганографии «LSB» в файле формата BMP. *Практическая часть* Реализация программы использующей стеганографические методы шифрования информации.

6	Лабораторная работа №6 Тема: Изучение работы программ для формирования и работы с ЭЦП на примере программного продукта Kleopatra.	*Теоретические сведения* 1. Электронно-цифровая подпись. 2. Сертификат открытого ключа (сертификат электронной подписи). 3. Принцип формирования и работы ЭЦП. *Практическая часть* Изучение принципов формирования и использования электронно-цифровой подписи (ЭЦП) и освоение программного продукта Kleopatra.

Пример формирования задания к лабораторной работе

1. Ознакомиться с криптографическим протоколом RSA.
2. Реализовать на каком либо языке программированияалгоритм шифрования RSA.
3. Ответить на контрольные вопросы.
4. Составить отчёт о проделанной работе.

Технология проведения

Все лабораторные работы обязательны для выполнения. Задание является общим для всех, различаются только входными параметрами, определяемыми индивидуально, в зависимости от варианта.

Критерии оценивания

- оценивается «зачтено», если работа выполнена в полном объеме (все задания лабораторной работы выполнены правильно, даны пояснения, приведена постановка задачи, сделаны выводы по работе, если это требуется, приведен код программы с комментариями);
- оценивается «не зачтено», работа выполнена не полностью или в представленной части много ошибок

Курсовые работы (примерный перечень тем курсовых работ)

1. Криптографические средства защиты информации в операционных системах и их применение
2. Контроль целостности данных с помощью хеш-функций.
3. Разработка программы для криптоанализа алгоритма шифрования Виженера.
4. Разработка программы для реализации алгоритма шифрования «Сеть Фейстеля».
5. Разработка программы для реализации алгоритма шифрования Эль-Гамаля.
6. Квантовая криптография: основные принципы и перспективы использования квантовых систем для защиты информации.
7. Защита сетевой инфраструктуры предприятия с использованием криптографического программно-аппаратного комплекса ViPNet.
8. Основные проблемы криптографии.
9. Криптография в облачных вычислениях: проблемы и решения для обеспечения безопасности данных в облачных средах.
10. Криптография в блокчейн-технологиях.
11. Криптографические алгоритмы в сетевых протоколах и их роль в обеспечении безопасности передачи данных.

Тема курсовой работы может быть предложена обучающимся, должна быть согласована с руководителем и должна соответствовать содержанию (направлению) дисциплины

Критерии оценивания

Для оценивания результатов обучения при выполнении студентом курсовой работы используются следующие показатели:

Знание основных современных криптографических протоколов, используемых в информационных сетях передачи данных; принципов работы шифров; методов разработки криптографических протоколов.

Умение разрабатывать математические модели криптографических протоколов и реализовывать их на современном языке программирования; разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств.

Владение подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализации криптографических протоколов, моделирования с помощью современных языков программирования и математических пакетов современных криптографических протоколов.

Для оценивания результатов выполнения курсовой работы используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов выполнения курсовой работы:

Показатель оценивания компетенции	Критерии оценивания компетенций	Шкала оценок
Обучающийся знает все основные современные криптографические протоколы, используемые в информационных сетях передачи данных; принципы работы шифров; методы разработки криптографических протоколов. Умеет разрабатывать математические модели криптографических протоколов и реализовывать их на современном языке программирования; разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств. Уверенно владеет подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализации криптографических протоколов, моделирования с помощью современных языков программирования и математических пакетов криптографических протоколов.	В ходе выполнения и защиты курсовой работы обучающийся продемонстрировал знание основных современных криптографических протоколов, используемых в информационных сетях передачи данных; принципов работы шифров; методов разработки криптографических протоколов. Умеет разрабатывать математические модели криптографических протоколов и реализовывать их на современном языке программирования; разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств. Владеет подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализации криптографических протоколов, моделирования с помощью современных языков программирования и математических пакетов современных криптографических протоколов. Привел логичное, доказательное	Отлично

	решение некоторой конкретной задачи, проанализировал полученные в ходе ее решения результаты. Курсовая работа оформлена в соответствии с требованиям по оформлению. В соответствии с методикой оценивания оценка за выполнение курсовой работы – 5 баллов.	
Обучающийся знает основные современные криптографических протоколы, используемые в информационных сетях передачи данных; принципы работы шифров; методы разработки криптографических протоколов. Умеет разрабатывать математические модели криптографических протоколов и реализовывать их на современном языке программирования; разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств. Владеет подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализации криптографических протоколов, моделирования с помощью современных языков программирования и математических пакетов современных криптографических протоколов.	В ходе выполнения и защиты курсовой работы обучающийся продемонстрировал знание основных современные криптографические протоколы, используемые в информационных сетях передачи данных; принципов работы шифров; методов разработки криптографических протоколов. Умеет разрабатывать математические модели криптографических протоколов и реализовывать их на современном языке программирования; разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств. Привел решение некоторой конкретной задачи, проанализировал полученные в ходе ее решения результаты, но в ходе решения допустил небольшие неточности. Курсовая работа оформлена в соответствии с требованиям по оформлению. В соответствии с методикой оценивания оценка за выполнение курсовой работы . – 4 балла.	Хорошо
Обучающийся знает современные криптографических протоколы, используемые в информационных сетях передачи данных; принципы работы шифров; методы разработки криптографических протоколов. Умеет разрабатывать математические модели криптографических протоколов и	В ходе выполнения и защиты курсовой работы обучающийся показал знание основных понятий, построения криптографических протоколов, принципов работы шифров и методов разработки математических моделей криптографических протоколов и реализации их на современном языке программирования, умение их примененять для изучения конкретной практической задачи,	Удовлетво-рительно

реализовывать их на современном языке программирования; разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств. Владеет подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализации криптографических протоколов, моделирования с помощью современных языков программирования и математических пакетов современных криптографических протоколов.	привел решение поставленной задачи, проанализировал полученные результаты. Курсовая работа оформлена с замечаниями. В соответствии с методикой оценивания оценка за выполнение курсовой работы – 3 балла.	
Обучающийся фрагментарно знает основные криптографических протоколы, используемые в информационных сетях передачи данных; принципы работы шифров; методы разработки криптографических протоколов. Частично умеет разрабатывать математические модели криптографических протоколов и с трудом может реализовать их на современном языке программирования; при развертывании инфраструктуры открытых ключей для решения криптографических задач допускает существенные ошибки; Не умеет проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств. Частично владеет подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализации криптографических протоколов, моделирования с помощью современных языков программирования и математических пакетов современных криптографических протоколов.	Обучающийся не справился с выполнением курсовой работы, результаты работы не соответствуют указанным выше критериям. Курсовая работа не оформлена в соответствии с требованиями. В соответствии с методикой оценивания оценка за выполнение курсовой работы составляет менее 3 баллов.	Неудовлет-ворительно

В ходе выполнения курсовой работы обучающийся демонстрирует знания, умения и навыки, полученные в результате освоения дисциплины.

Теоретический блок курсовой работы:

2 балла – теоретический материал соответствует теме курсовой работы, в полном объеме отражает ее (приведены необходимые доказательства);

1 балл - теоретический материал соответствует теме курсовой работы, кратко отражает ее (отсутствуют необходимые доказательства);

0 баллов - теоретический материал не соответствует теме курсовой работы.

Практический блок курсовой работы:

2 балла – приведенная задача отражает применение теоретического материала, ее решение верно и логично описано;

1 балл – приведенная задача отражает применение теоретического материала, но ее решение кратко или содержит ошибки;

0 баллов – задача отсутствует, или приведенная задача не является практическим применением теоретического материала курсовой работы.

Защита курсовой работы:

1 балл – в процессе подготовки к выполнению курсовой работы и ее написания обучающийся продемонстрировал самостоятельность, самоорганизованность, инициативность, ответственность; во время защиты курсовой работы студент показал знание материала курсовой работы, ответил на дополнительные вопросы по теме работы;

0 баллов – во время подготовки к выполнению курсовой работы и ее написания обучающийся проявил неорганизованность, безынициативность, безответственность; во время защиты курсовой работы студент неуверенно отвечал на вопросы по теме работы, допускал ошибки.

Таким образом, максимальное количество баллов, которое обучающий может получить за курсовую работу, равно 5. Критерии выставления оценки («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») за выполнение курсовой работы приведены выше.

Курсовая работа имеет следующую структуру:

- титульный лист;
- содержание;
- текст работы – содержательная часть курсовой работы;
- список литературы;
- приложения (при необходимости).

Содержательная часть курсовой работы представляет собой 2 блока: теоретический (теоретический материал по теме курсовой работы) и практический (применение теории к решению конкретной задачи). В завершении данной части стоит подвести итог выполненной работы (что было изучено и какой результат получен).

Текст работы располагается на одной стороне листа белой бумаги формата А4 по ГОСТ 2.30168 (размер 210 × 297 мм). допускается представлять иллюстрации и таблицы на листах формата не более 420 × 594 мм, должны соблюдаться следующие размеры полей:

- левое - не менее 30 мм;
- правое - не менее 10 мм;
- верхнее - не менее 15 мм;
- нижнее - не менее 20 мм.

Текст работы может быть набран в текстовом редакторе Microsoft Word шрифтом Times New Roman (14 пунктов) через полтора интервала. Абзацный отступ равен 10-17 мм.

На страницах номер проставляют, как правило, сверху по центру. На титульном листе номер не ставится, но включается в общую нумерацию работы. Объем работы составляет 10-20 листов. Количество используемых библиографических источников – не менее 5.

Скрепленная и оформленная надлежащим образом курсовая работа предоставляется обучающимся на проверку преподавателю. В срок, установленный календарным учебным графиком, через 1-3 рабочих дня после предоставления обучающимся работы преподавателю на проверку, происходит защита курсовой работы, в ходе которой обучающийся должен показать уверенное знание материала работы.

20.2.Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к зачету.

Перечень вопросов к зачету (КИМ №1)

1. **Основные определения и принципы криптографии.**
2. **Четыре периода развития криптографии. Отличительные черты и характерные особенности.**
3. **Основные проблемы криптографии.**
4. **Понятие криптографической атаки. Виды атак.**
5. **Криптоанализ: основные понятия и методы. Пример метода криптоанализа.**
6. **Методы криптографического преобразования информации. Виды и характеристики.**
7. **Классификация криптоалгоритмов по типу преобразования исходного текста.**
8. **Классификация криптоалгоритмов с точки зрения количества ключей.**
9. **Перестановочные и подстановочные криптоалгоритмы – основные отличия. Примеры перестановочных и подстановочные криптоалгоритмов.**
10. **Перестановочные криптоалгоритмы: определение, виды, достоинства, недостатки. Примеры перестановочных криптоалгоритмов.**
11. **Реализация шифров простой и сложной перестановки. Шифр двойной перестановки. Примеры реализации перестановочных шифров.**
12. **Подстановочные криптоалгоритмы: определение, виды, достоинства, недостатки. Примеры подстановочных криптоалгоритмов.**
13. **Реализация моноалфавитных и полиалфавитные шифров подстановки. Примеры реализации подстановочных шифров.**
14. **«Идеальный» криптоалгоритм. Описание и характеристики. Недостатки «идеальной» криптосистемы.**
15. **Роторные машины: принцип работы, достоинства, недостатки. Пример.**
16. **Поточные криптоалгоритмы – описание и характеристики. Достоинства и недостатки.**
17. **Шифрование методом гаммирования. Описание и характеристики. Пример реализации.**
18. **Понятие симметричных и асимметричных криптоалгоритмов, их преимущества и недостатки. Привести примеры.**
19. **Блочные симметричные криптоалгоритмы – описание и характеристики. Достоинства и недостатки. Примеры блочных симметричных криптоалгоритмов.**
20. **Компоненты современного блочного шифра: описание и характеристики. Принципы построения современного блочного шифра.**
21. **Сеть Фейстеля: описание, основные компоненты и их характеристики, принцип построения и работы.**
22. **Алгоритм шифрования DES: описание и характеристики, структура, схема работы, основные блоки. Достоинства и недостатки.**
23. **Алгоритм шифрования AES: описание и характеристики, структура, схема работы, основные блоки. Достоинства и недостатки.**
24. **Асимметричное криптоалгоритмы – описание и характеристики. Достоинства и недостатки. Примеры асимметричных криптоалгоритмов.**
25. **Алгоритм шифрования RSA: описание и характеристики, структура, схема работы, основные блоки. Достоинства и недостатки.**
26. **Электронно-цифровая подпись. Реализация. Область применения. Сертификат ЭЦП. Центры сертификации.**
27. **Стеганография. Виды и способы реализации.**
28. **Хеширование. Криптографические хеш-функции. Область применения. Примеры реализации алгоритмов хеширования.**
29. **Генерация случайных и псевдослучайных последовательностей. Тесты**

проверки на случайность.

Критерии оценки ответов на вопросы

Для оценивания результатов обучения на экзамене используется – 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», критерии оценивания приведены ниже.

Оценка «отлично» - студент демонстрирует глубокое понимание темы, умеет распространять вытекающие из теории выводы.
Оценка «хорошо» - студент демонстрирует понимание теоретических положений темы и базовых понятий, но допускает неточности в ответах, испытывает затруднения в применении знаний к анализу состояния проекта.
Оценка «удовлетворительно» - студент отвечает не на все предложенные вопросы, но не менее, чем на половину из них; не демонстрирует способности применения теоретических знаний для анализа ситуаций.
Оценка «неудовлетворительно» - студент демонстрирует непонимание теоретических основ и базовых понятий курса.

Оценка промежуточной аттестации формируется как интегральная оценка по следующей формуле:

$$Q_{пром\_ат} = 0{,}1Q_{T1} + 0{,}1Q_{T2} + 0{,}1Q_{T3} + 0{,}1Q_{T4} + 0{,}6Q_{ЗАЧ}$$

При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены.

20.3. Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

ОПК-2.1 Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации

ОПК-2.2 Способен разрабатывать и анализировать математические модели механизмов защиты информации;

Вопросы с вариантами ответов

Критерий оценивания	Шкала оценок
Верный ответ	1 балл
Неверный ответ	0 баллов

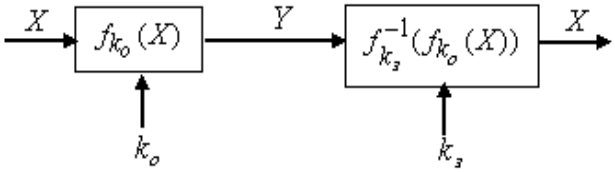
1. Какие шифры не являются шифрами замены:
   a) Гаммирование
   b) Шифр Порта
   c) Решетка Кардано
   d) Шифр Вернама
   e) Метод Ришелье
2. Какие из режимов шифрования не требуют синхропосылки:
   a) Режим электронной кодировочной книги
   b) Режим сцепления блоков шифротекста
   c) Режим обратной связи по шифротексту
   d) Режим обратной связи по выходу
3. Какие из криптографических методов не являются шифрами в полном смысле этого слова:
   a) Скитала

b) Метод магических квадратов
c) Атбаш
d) Линейка Энея

4. Алгебраическая модель шифра имеет вид:
   a) $f: X \times Y \to K$, где f инъективна и сюръективна
   b) $f: X \times K \to Y$, где f инъективна и сюръективна
   c) $f: X \times K \to Y$, где f инъективна
   d) $f: X \times Y \to K$, где f сюръективна
   e) $f: X \times K \to Y$, где f инъективна, сюръективна и транзитивна
5. Шифр, для которого верно $\forall\, x \in X\ y \in Y\ p(x|y) = p(x)$ является:
   a) Шифром гаммирования с равновероятной гаммой
   b) Шифром с марковским источником открытых текстов
   c) Совершенным
   d) Идемпотентным
6. При генерация раундового ключа в AES производится:
   a) Отбрасывание битов четности, используемых для помехоустойчивости
   b) Расширение ключа на основе закрытого ключа
   c) Расширение ключа на основе предыдущего раундового ключа
   d) Построение ключа на основе образующего полинома поля Галуа
7. Наличие слабых и полуслабых ключей является характерным недостатком алгоритмов:
   a) AES
   b) DES
   c) Любой схемы Фейстеля
   d) Полиалфавитных шифров
8. К методам взлома полиалфавитных шифров относятся:
   a) Частотный метод
   b) Метод бумеранга
   c) Метод чтения в колонках
   d) Линейный криптоанализ
   e) Метод Касински
9. Теоретическую стойкость шифра не определяют:
   a) То, что знание шифртекста не влечет перераспределение вероятностей на множестве шифруемых текстов
   b) Априорное допущение об информированности противника о криптосистеме с точностью до ключевой информации
   c) Стремление к нулю средней вероятности правильной дешифровки открытого текста с ростом длины сообщения
   d) Возможность подбора эффективного метода взлома по принципу оптимального соотношения минимальной трудоемкости и максимальной вероятности верной дешифровки
10. Расстояние единственности шифра это:
    a) минимальное натуральное L, при котором по известному шифротексту e_L однозначно восстанавливается открытый текст m_L
    b) количество букв открытого текста, которое можно убрать до наступления нечитаемости открытого текста.
    c) мера ненадежности открытого текста и ключа
    d) среднее расстояние между периодическими m-граммами в шифротексте полиалфавитных шифров
11. Метод криптоанализа, основанный на замене функции криптопреобразования ее статистическим аналогом называется:
    a) Дискретный криптоанализ
    b) Метод встречи посередине
    c) Линейный криптоанализ
    d) Метод Симпсона
12. Криптология включат в себя следующие дисциплины:

a) Критографию и стеганографию
b) Криптографию и криптоанализ
c) Криптографию, криптоанализ и стеганографию
d) Стеганографию и криптоанализ

13. На рисунке представлена

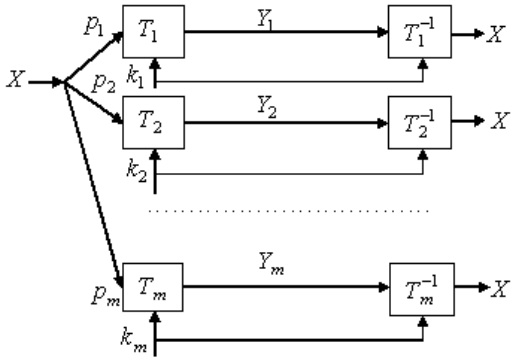


a) Общая схема симметричной киптосистемы
b) Общая схема ассиметричной криптосистемы
c) Общая схема электронной цифровой подписи
d) Общая схема поточной криптосистемы

14. К вероятностным моделям источников открытых сообщений не относятся:
a) Источники независимых символов
b) Источники марковски зависимых букв
c) Нестационарные источники
d) Самосинхронизирующиеся источники

15. К видам криптопреобразований не относятся:
a) Шифры замены
b) Шифры престановки
c) Композиционные шифры
d) Поточные шифры

16. На рисунке изображена



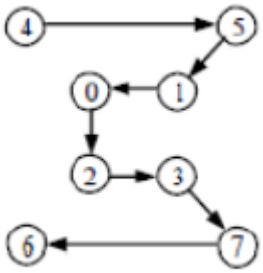
a) Сумма криптосистем
b) Произведение криптосистем
c) Транзитивная криптосистема
d) Идемпотентная криптосистема

Вопросы с кратким текстовым ответом

Критерий оценивания	Шкала оценок
Должен быть сформулирован ответ из указанных вариантов (один или несколько) или аналогичные по сути ответы с альтернативными терминами и определениями	2 балла
Неверный ответ	0 баллов

2 – верный ответ
0 – неверный ответ

1. Зашифруйте открытый текст «Юстас Алексу» шифром Виженера с ключом «жираф»
Ответ дщваежухкещ
2. Зашифруйте открытый текст «Юстас Алексу» маршрутной перестановкой по указанному гамильтонову пути с заполнителем *



Ответ саютлсеас*ку**

3. Как называется подход, при котором криптопреобразования производятся над прямоугольными массивами данных, называемыми состояниями?
   Ответ KASTL-сеть
4. Для какого источника открытых текстов вероятности появления *k* -грамм в тексте зависят от их места в тексте?
   Ответ Нестационарный
5. Какая криптоатака основана на знании открытого текста для случайных фрагментов шифротекста?
   Ответ: на основе открытых текстов
6. Какой шифр описывает криптопреобразование $f = (f_0 \dots f_{n-1})$ для открытого текста $X = x_0 \dots x_{n-1}$ дающее шифротекст $Y = y_0 \dots y_{n-1} = x_{f(0)} \dots x_{f(n-1)}$?
   Ответ шифр перестановки
7. Какой метод криптоанализа заключается в анализе изменения несходства между парой открытых текстов в процессе прохождения через циклы шифрования с одним и тем же ключом
   Ответ Дифференциальный

Вопросы с вариантами ответов

Критерий оценивания	Шкала оценок
Верный ответ	1 балл
Неверный ответ	0 баллов

1. Отметьте правильный ответ

… — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

+ информационная система
– информационно-телекоммуникационная сеть
– информационные ресурсы

2. Управление, препятствия, маскировка, регламентация, побуждение, принуждение.

+ это методы защиты информации
– это средства защиты информации
– это механизмы защиты информации

3. Установите соответствие

1. Полный взлом
2. Глобальная дедукция
3. Частичная дедукция
4. Информационная дедукция

1. криптоаналитик разрабатывает функциональный эквивалент исследуемого алгоритма, позволяющий зашифровывать и расшифровывать информацию без знания ключа.
2. криптоаналитику удается расшифровать или зашифровать некоторые сообщения.
3. криптоаналитик извлекает секретный ключ.
4. криптоаналитик получает некоторую информацию об открытом тексте или ключе.

Ответ: 1-3, 2-1, 3-2, 4-4

4. Что НЕ ОТНОСИТСЯ к области применения криптосистем, использующих асимметричные алгоритмы?

+ Выработка дайджеста сообщения
– Электронная подпись
– Шифрование
5. Какой элемент (параметр) криптосистемы (шифра), согласно правилу О. Керкхоффса, не должен быть известен злоумышленнику?
+ ключ шифрования
– особенности реализации
– шифрованный текст
– алгоритм шифрования
6. К системам с открытым ключом НЕ ОТНОСИТСЯ:
+ DES
– RSA
– El Gamal
7. Шифрсистема, в которой ключи шифрования и расшифрования легко получаются один из другого.
+ Симметричная криптосистема
– Асимметричная криптосистема
– Блочная криптосистема
8. В алгебраической модели шифры $\Sigma_A(X,K,Y,E,D)$ множество К представляет собой:
+ конечное множество возможных ключей
– множество правил зашифрования на всевозможных ключах
– правило зашифрования на определенном ключе
9. К симметричным алгоритмам относится:
+ шифр Плэйфера
– алгоритм Диффи-Хеллмана
– шифр Эль-Гамаля
10….– это информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
+ электронная подпись (ЭП)
– автограф
– подпись
11. Шифрсистема, в которой ключи шифрования и расшифрования легко получаются один из другого.
+ Симметричная криптосистема
– Асимметричная криптосистема
– Поточная криптосистема
12. Число a называется …по модулю m , если сравнение $x^2 \equiv a(mod\ m)$ имеет решение при некотором целом x
+ квадратичным вычетом
– квадратичным невычетом
13. Для любого простого нечетного p и целого a символ … определяется следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, \text{ если } a \text{ делится на } p; \\ 1, \text{ если } a \text{ - квадратичный вычет } (mod\ p); \\ -1, \text{ если } a \text{ - квадратичный невычет } (mod\ p). \end{cases}$$

+ Лежандра
– Якоби
– Кронекера
14. … — это наименьший показатель степени элемента в мультипликативной группе, при котором он обращается в нейтральный элемент.
+ Порядок элемента группы
– Порядок группы

Вопросы с кратким текстовым ответом

Критерий оценивания	Шкала оценок

Должен быть сформулирован ответ из указанных вариантов (один или несколько) или аналогичные по сути ответы с альтернативными терминами и определениями	2 балла
Неверный ответ	0 баллов

2 – верный ответ
0 – неверный ответ

1. Назовите метод криптоанализа, использующий то, что вероятности появления отдельных букв, а также их порядок в словах и фразах естественного языка подчиняются задокументированным статистическим закономерностям.
+ частотный анализ
2. Система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения – криптосисема ...
+ асиметричная
+ с открытым ключом
3. Если n — количество букв в алфавите, m_j — номер буквы открытого текста, k_j — номер буквы ключа в алфавите, то шифрование … можно записать следующим образом:
$c_j = (m_j + k_j) \bmod n$
+ Виженера
+ Вижинера
4. … – раздел прикладной математики, в котором изучаются модели, методы, алгоритмы, программные и аппаратные средства преобразования информации в целях сокрытия ее содержания, проверки подлинности, предотвращения видоизменения или несанкционированного использования.
+ криптография
+ Криптография
5. Дополните
Защита … электронных документов оказывается необходимой при использовании вычислительных систем и сетей для обработки, хранения и передачи информационных объектов (сообщений, файлов, баз данных), содержащих в себе приказы, платежные поручения, контракты и другие распорядительные, договорные, финансовые документы.
+ юридической значимости

ОПК-2.3 Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов

2 Какой слой в структуре системы управления кибербезопасности выделяется в последнее время в качестве отдельного?
- Процессы, персонал
- Правила, нормативная база
- **Данные**
- Технологии, средства защиты информации

3 Какой процесс ITSM необходимо внедрять в первую очередь при построении системы кибербезопасности в организации?
- Управление инцидентами
- Управление изменениями
- **Управление активами**
- Управление конфигурациями

4. Какие стадии кибератаки рассматриваются в модели Kill Chain? Выберите все правильные ответы.
1. **Разведка**
2. Расшифровка
3. Мониторинг

4. **Реализация**
5. **Управление**
6. Прослушивание
7. **Запуск**
8. Анализ

5. Какой подход наиболее эффективен в обеспечении кибербезопасности устройств интернета вещей?
1. Установка антивируса на устройства IoT
2. Физическая безопасность
3. Назначение сложных паролей
4. **Поведенческий анализ на основе моделей машинного обучения**

6. Какой способ начала кибератаки самый распространенный в настоящее время?
1. Подбор пароля по словарю
2. **Фишинг**
3. Сканирование портов
4. Перехват сетевого трафика

7. Что понимается под управлением уязвимостями?
1. Управление обновлениями программного обеспечения
2. **Выявление, оценка, устранение уязвимостей безопасности в информационных системах и составление отчетов**
3. Выявление, оценка, устранение уязвимостей безопасности в программном коде на всех этапах разработки
4. Исследование и оценка методов эксплуатации уязвимостей хакерскими группами

8. С каким типом атаки не может справиться брандмауэр
1. **DDOS**
2. Сканирование портов
3. UDP-шторм

9. Набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP носит название
1. IPS
2. **IPsec**
3. IPC
4. IPCrypt
5. IPEnc

10. Атака типа UPD-шторм используется в том случае, если на жертве открыт как минимум
1. 1 порт
2. **2 порта**
3. 3 порта
4. 4 порта
5. 5 портов

1. Укажите, как называется этап тестирования удобства использования пользовательского интерфейса, который проводится после разработки низкоуровневых требований и детализированного прототипа пользовательского интерфейса:
(1) исследовательский
(2) оценочный
(3) валидационный
(4) сравнительный

2. Укажите, каким утверждением нельзя охарактеризовать возможности RDF в настоящее время:
(1) взаимообмен данными
(2) семантика доступная для понимания компьютерами
(3) унифицированные средства для поиска ресурсов
(4) большая точность в процессе анализа ресурса, чем полнотекстовый поиск
(5) более стойкие к изменениям приложения

3. Укажите верную последовательность основных фаз процесса разработки в MSF:

(1) выработка концепции, Планирование, Разработка, Внедрение

(2) выработка концепции, Планирование, Разработка, Стабилизация, Внедрение

(3) планирование, Выработка концепции, Разработка, Стабилизация, Внедрение

(4) планирование, Разработка, Внедрение

(5) планирование, Разработка, Внедрение, Стабилизация

4. При каком типе атаки степень активности криптоаналитика наивысшая?

а) криптоатака с использованием криптограмм;

б) криптоатака с использованием открытых текстов и соответствующих криптограмм;

в) криптоатака с использованием выбираемых криптоаналитиком открытых текстов и соответствующих криптограмм.

5. В каких типах криптоатак используется метод "опробования"? (Укажите несколько верных вариантов ответа.)

а) криптоатака с использованием криптограмм;

б) криптоатака с использованием открытых текстов и соответствующих криптограмм;

в) криптоатака с использованием выбираемых криптоаналитиком открытых текстов и соответствующих криптограмм;

г) все ответы верны.

6. Время, затрачиваемое алгоритмом для решения задачи, рассматриваемое как функция размера задачи или количества входных данных, – это:

а) временная сложность;

б) время воспроизведения алгоритма;

в) время решения алгоритма.

7. Отсутствие изменений в передаваемой или хранимой информации по сравнению с ее исходной записью – это:

а) целостность;

б) единство;

в) синтез;

г) полнота.

8. Что такое целостность информации?

1) Свойство информации, заключающееся в возможности ее изменения любым субъектом

2) Свойство информации, заключающееся в возможности изменения только единственным пользователем

3) Свойство информации, заключающееся в ее существовании в виде единого набора файлов

4) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)

9. В чем состоит задача криптографа?

1) взломать систему защиты

2) обеспечить конфиденциальность и аутентификацию передаваемых сообщений

10. Уровень секретности — это

1) ответственность за модификацию и НСД информации

2) административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов

1. Хищение информации – это

1. ***Несанкционированное копирование информации***

2. Утрата информации

3. Блокирование информации

4. Искажение информации

5. Продажа информации

2. Документированная информация, доступ к которой ограничивается в соответствии с законодательством российской федерации - это:

1. ***Конфиденциальная информация***

2. Факс

3. Личный дневник
4. Законы РФ

3. Обеспечение информационной безопасности есть обеспечение…
1. Независимости информации
2. Изменения информации
3. Копирования информации
4. ***Сохранности информации***
5. Преобразования информации

4. Степени секретности информации, составляющей гостайну:
а. особо секретно;
б. конфиденциально;
в. строго конфиденциально;
г. совершенно конфиденциально;
д. секретно;
е. особой важности.

5. Не подлежат отнесению к государственной тайне сведения:
а. о состоянии обороноспособности объектов жизнеобеспечения населения;
б. о фактах нарушения прав и свобод человека и гражданина;
в. о размерах золотого запаса и государственных валютных резервах Российской Федерации;
г. о состоянии и средствах защиты государственной тайны;
д. о состоянии здоровья высших должностных лиц Российской Федерации;

6. К видам информации с ограниченным доступом не относятся:
а. коммерческая тайна;
б. государственная тайна;
в. сведения для служебного пользования;
г. персональные данные;
д. запрещенные к распространению сведения;
е. нотариальная тайна.

7. Контроль над выполнением требований в сфере защиты персональных данных выполняют:
а)ФСБ РФ;
б) ФСТЭК России и Роскомнадзор;
в) все перечисленные организации.

8. За несоблюдение положений закона 152-ФЗ «О персональных данных» предусматривается:
а) гражданская, уголовная, административная ответственность; б) дисциплинарная и другие виды ответственности;
в) все перечисленные виды ответственности.

9. Субъект персональных данных:
а) имеет право на доступ к своим персональным данным во всех случаях;
б) не имеет право на доступ к своим персональным данным;
в) имеет право на доступ к своим персональным данным за исключением случаев, предусмотренных законом.

10. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, при обработке персональных данных в государственных информационных системах осуществляются:
а) ФСТЭК России и ФСБ России;
б) ФСТЭК России и органами Роскомнадзора;
в) ФСБ России и органами Роскомнадзора.

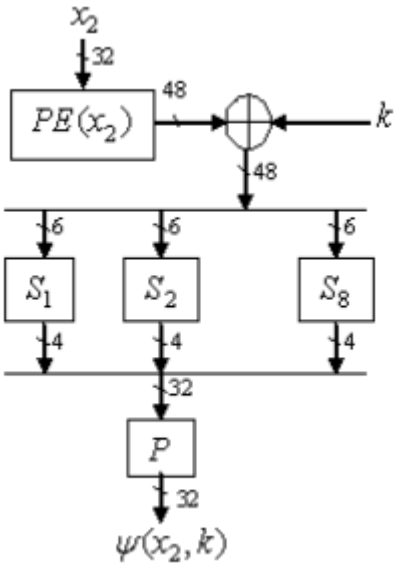
11. Какой нормативный акт является основным в сфере регулирования электронной подписи:
а) федеральный закон №1-ФЗ от 10.01.2002 «Об электронной цифровой подписи»;
б) федеральный закон №63-ФЗ от 06.04.2011 «Об электронной подписи»;
в) постановление Правительства Российской Федерации № 111 от 9 февраля 2012 г. «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой».

ОПК-8.15. Умеет применять методы экспериментального исследования при решении профессиональных задач.

Вопросы с вариантами ответов

Критерий оценивания	кала оценок
Верный ответ	1 балл
Неверный ответ	0 баллов

1. Какие шифры основаны на действиях с полиномами в поле Галуа:
   a) DES
   b) AES
   c) ГОСТ 28147-89
   d) KASTL
2. Определите правильную последовательность действий для шифра DES:
   a) ОТ(64 б) → Начальная перестановка → Схема Фейстеля (16 раундов с 48 битным ключом) → Конечная перестановка → Шифртекст (64 б)
   b) ОТ(64 б) → Начальная перестановка → Конечная перестановка → Схема Фейстеля (16 раундов с 64 битным ключом) → Шифртекст (64 б)
   c) ОТ(64 б) → Начальная перестановка → Конечная перестановка → Схема Фейстеля (12 раундов с 64 битным ключом) → Шифртекст (64 б)
   d) ОТ(64 б) → Начальная перестановка → Схема Фейстеля (16 раундов с 64 битным ключом) → Конечная перестановка → Шифртекст (64 б)
3. Дифференциальный криптоанализ относится к атакам:
   a) На основе шифртекста
   b) На основе открытых текстов
   c) На основе подобранного открытого текста
   d) На основе адаптивно подобранного открытого текста
4. Схема на рисунке представляет:



   a) Общий вид схемы Фейстеля
   b) Функцию усложнения DES
   c) Схему расширения ключа AES
   d) Функцию усложнения AES

Вопросы с кратким текстовым ответом (2)

Критерий оценивания	Шкала оценок
Должен быть сформулирован ответ из указанных вариантов (один или несколько) или аналогичные по сути ответы с альтернативными терминами и	2 балла

определениями	
Неверный ответ	0 баллов

2 – верный ответ

0 – неверный ответ

1. Зашифруйте при помощи блочной криптосистемы с размером блока в один байт и синхропосылкой (начальным вектором) y_0=0x02 открытый текст из шестнадцатеричных чисел «0x4C 0x4F 0x4C» шифром простого гаммирования (XOR) с гаммой γ=0xB2 в режиме обратной связи по шифротексту
   Ответ **0x4E 0xB3 0x4D**
2. Как называется блок шифротекста, формирующийся из всего объема открытого текста при помощи суммирования по модулю 2 шифрованных блоков?
   Ответ: имитовставка

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).