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

УТВЕРЖДАЮ
Заведующий кафедрой

Сирота Александр Анатольевич
Кафедра технологий обработки и защиты информации
03.05.2023

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.42 Информационная безопасность

1. Код и наименование направления подготовки/специальности:

09.03.04 Программная инженерия

2. Профиль подготовки/специализация:

Информационные системы и сетевые технологии

3. Квалификация выпускника:

Бакалавриат

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

6. Составители программы:

Мальцев Алексей Сергеевич, к.т.н.

7. Рекомендована:

Протокол №7 от 03.05.2023

8. Учебный год: 2026-2027 **Семестр(ы)/Триместр(ы):** 8

9. **Цели и задачи учебной дисциплины**

Целями освоения учебной дисциплины являются:

Изучение теоретических основ информационной безопасности, защиты информации от несанкционированного доступа, обеспечения конфиденциальности обмена информацией в информационно-вычислительных системах, вопросов защиты исходных и байт кодов программ; овладение практическими навыками применения методов криптографии, стеганографии, получение профессиональных компетенций в области современных технологий защиты информации.

Задачи учебной дисциплины:

- обучение студентов теоретическим и практическим аспектам обеспечения информационной безопасности;
- обучение студентов базовым принципам защиты конфиденциальной информации, методам идентификации, аутентификации пользователей информационной системы, принципам организации скрытых каналов передачи информации, принципам защиты авторских прав на объекты цифровой интеллектуальной собственности;
- овладение практическими навыками применения теоретических знаний для шифрования конфиденциальной информации, стеганографического скрытия информации, контроля за целостностью информации, решения задач идентификации и аутентификации.

10. Место учебной дисциплины в структуре ООП:

Входит в блок обязательных дисциплин Б1.О.

Входные знания в области устройства ЭВМ и операционных систем, принципах их работы, сетевых технологий, информатики.

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

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ОПК-1.1	Знает основы математики, физики, вычислительной техники и программирования	Знать: основные теоретические и практические аспекты обеспечения информационной безопасности.
		ОПК-1.2	Умеет решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования	Уметь: применять на практике теоретические знания в области криптографии и стеганографии. Владеть: практическими навыками разработки и применения в профессиональной деятельности криптографических и стеганографических алгоритмов.

12. Объем дисциплины в зачетных единицах/час. — 4/144.

Форма промежуточной аттестации Экзамен.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра 8	№ семестра	…
Аудиторные занятия		60	60		
в том числе:	лекции	48	48		
	практические				
	лабораторные	12	12		
Самостоятельная работа		48	48		
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(экзамен – __час.)*		36	36		
Итого:		144	144		

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Основы государственной информационной политики и информационной безопасности Российской Федерации	Понятие национальной безопасности. Информационная безопасность в системе национальной безопасности Российской Федерации. Государственная информационная политика. Информационные ресурсы. Проблемы информационной войны. Проблемы информационной безопасности в сфере государственного и муниципального управления.	Создан электронный курс, размещены материалы к лекции.
1.2	Информационная безопасность автоматизированных систем	Современная постановка задачи защиты информации. Организационно-правовое обеспечение, информационной безопасности. Информационные системы. Угрозы информации. Методы и модели оценки уязвимости информации.	Создан электронный курс, размещены материалы к лекции.
1.3	Методы и модели оценки уязвимости информации	Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза - защита».	Создан электронный курс, размещены материалы к лекции.
1.4	Рекомендации по использованию моделей оценки уязвимости информации	Рекомендации по использованию моделей оценки уязвимости информации	Создан электронный курс, размещены материалы к лекции.
1.5	Методы определения требований к защите информации	Методы определения требований к защите информации	Создан электронный курс, размещены материалы к лекции.
1.6	Функции и задачи защиты информации	Общие положения. Методы формирования функций защиты. Классы задач защиты информации. Функции защиты. Состояния и функции системы защиты информации	Создан электронный курс, размещены материалы к лекции.
1.7	Стратегии защиты информации	Стратегии защиты информации.	Создан электронный курс, размещены материалы к лекции.
1.8	Способы и средства защиты информации	Способы и средства защиты информации.	Создан электронный курс, размещены

			материалы к лекции.
1.9	Криптографические методы защиты информации	Требования к криптосистемам. Основные алгоритмы шифрования. Цифровые подписи. Криптографические хеш-функции. Криптографические генераторы случайных чисел. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы. Цифровые водяные знаки (ЦВЗ), виды реализации, практические области применения.	Создан электронный курс, размещены материалы к лекции.
1.10	Архитектура систем защиты информации	Требования к архитектуре СЗИ. Построение СЗИ. Ядро системы защиты информации. Ресурсы системы защиты информации.	Создан электронный курс, размещены материалы к лекции.
2. Практические занятия			
3. Лабораторные занятия			
3.1	Криптографические методы защиты информации	1. Практическое изучение работы алгоритмов блочного симметричного шифрования. 2. Изучение криптографических генераторов случайных чисел. 3. Практическое изучение работы асимметричных алгоритмов шифрования. 4. Изучение частотных характеристик текстовых сообщений. 5. Изучение алгоритмов стеганографического скрытия данных в пространственной и частотной области контейнеров (на примере цифровых изображений). 6. Практическое изучение принципов и методов стегоанализа (на примере визуального и статистического стегоанализа цифровых изображений).	Создан электронный курс. Размещены индивидуальные задания для выполнения лабораторных работ.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Основы государственной информационной политики и информационной безопасности Российской Федерации	8			4	12
2	Информационная безопасность автоматизированных систем	4			4	8
3	Методы и модели оценки уязвимости информации	4			4	8
4	Рекомендации по использованию моделей оценки уязвимости информации	2			4	6
5	Методы определения требований к защите информации	2			4	6
6	Функции и задачи защиты информации	4			4	8
7	Стратегии защиты информации	4			4	8
8	Способы и средства защиты информации	4			4	8
9	Криптографические ме-	12		12	12	36

	тоды защиты информации					
10	Архитектура систем защиты информации	4			4	8
	Итого:	48		12	48	108

14. Методические указания для обучающихся по освоению дисциплины:

1) При изучении дисциплины рекомендуется использовать следующие средства:

- рекомендуемую основную и дополнительную литературу;

- методические указания и пособия;

- контрольные задания для закрепления теоретического материала;

- электронные версии учебников и методических указаний для выполнения лабораторно - практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала.

Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении лабораторных занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций он-лайн и проведения лабораторно- практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

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

а) основная литература:

№ п/п	Источник
1	Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи : учебник / Б.И. Филиппов, О.Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499170
2	Баранова, Елена Константиновна. Информационная безопасность и защита информации : учебное пособие : [для студ., обучающихся по направлению "Прикладная информатика"] / Е.К. Баранова, А.В. Бабаш .— 4-е изд. перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019 .— 334, [1] с. : ил., табл. — (Высшее образование) .— Библиогр.: с. 327-330.

б) дополнительная литература:

№ п/п	Источник
1	Элементы теории чисел и критозащита : учебное пособие / Воронеж. гос. ун-т; сост. : Б.Н. Воронеков, А.С. Щеголеватых .— Воронеж : ИПЦ ВГУ, 2008 .— 87 с. : ил .— Библиогр.: с.87 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-95.pdf>.

2	Криптографические методы защиты информации : учебное пособие для вузов / Воронеж. гос. ун-т; сост. Б.Н. Воронков .— Воронеж : ИПЦ ВГУ, 2008 .— 58 с. : ил .— Библиогр.: с.52-58 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m08-17.pdf>.
3	Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2002. – 272 с.
4	*Теоретические основы компьютерной безопасности (учебное пособие для ВУЗов) / П.Н. Девянин [и др.]. – М.: Радио и связь, 2000 – 192с.*

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
2	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
3	ЭБС Лань – Лицензионный договор №3010-14/37-23 от 07.03.2023 (срок предоставления с 12.03.2023 по 11.03.2024)
4	ЭБС «Университетская библиотека online» – Контракт №3010-06/23-22 от 30.12.2022(срок предоставления с 12.01.2023 по 11.01.2024)
5	ЭБС «Консультант студента» – Лицензионный договор №3010-06/22-22 от 30.12.2022 (с дополнительным соглашение №1 от 09.01.2023) (срок предоставления с 12.01.2023 по 11.01.2024)

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Основы информационной безопасности [Электронный ресурс] : учеб. пособие / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов .— М. : Горячая линия – Телеком, 2011 .— 559 с. : ил. — ISBN 5-93517-292-5 .— ISBN 978-5-93517-292-5 .— Режим доступа: https://rucont.ru/efd/202786

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

Для реализации учебного процесса используется:

ПО ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019.

При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ" (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

18. Материально-техническое обеспечение дисциплины:

1) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 479

Учебная аудитория: специализированная мебель, компьютер преподавателя i5-8400-2,8ГГц, монитор с ЖК 19’’, мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры).

2) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 292

Учебная аудитория: специализированная мебель, компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для видеоконференций Logitech ConferenceCam Group и ноутбук 15.6’’ FHD Lenovo V155-15API

ПО: ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

3) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 380

Учебная аудитория: специализированная мебель, компьютер преподавателя i3-3240-3,4ГГц, монитор с ЖК 17'', мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

4) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 290

Учебная аудитория: специализированная мебель, персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27'' (12 шт.), мультимедийный проектор, экран.

Лабораторное оборудование искусственного интеллекта: рабочие места – персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27" (12 шт.); модули АО НПЦ «ЭЛВИС»: процессорный Салют-ЭЛ24ПМ2 (9 шт.), отладочный Салют-ЭЛ24ОМ1 (9 шт.), эмулятор MC-USB-JTAG (9 шт.).

Лабораторное оборудование электроники, электротехники и схемотехники: рабочие места – персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27" (12 шт.); стенд для практических занятий по электрическим цепям (KL-100); стенд для изучения аналоговых электрических схем (KL-200); стенд для изучения цифровых схем (KL-300).

ПО: ОС Windows v.7, 8, 10, Visual Studio, v. 2010-2019, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Разделы 1-10 Основы государственной информационной политики и информационной безопасности Российской Федерации. Информационная безопасность автоматизированных систем. Методы и модели оценки уязвимости информации. Рекомендации по использованию моделей оценки уязвимости информации. Методы определения требований к защите информации. Функции и задачи защиты информации. Стратегии защиты информации. Способы и средства защиты информации. Криптографические методы защиты информации. Архитектура систем защиты информации.	ОПК-1	ОПК-1.1	Собеседование, контрольная работа по соответствующим разделам. Лабораторные работы 1-6.
2.	Разделы 1-10 Основы государственной информационной политики и информационной безопасности Российской Федерации. Информационная безопасность автоматизированных систем.	ОПК-1	ОПК-1.2	Собеседование, контрольная работа по соответствующим разделам. Лабораторные работы 1-6.

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
	Методы и модели оценки уязвимости информации. Рекомендации по использованию моделей оценки уязвимости информации. Методы определения требований к защите информации. Функции и задачи защиты информации. Стратегии защиты информации. Способы и средства защиты информации. Криптографические методы защиты информации. Архитектура систем защиты информации.			
Промежуточная аттестация форма контроля – экзамен				

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

Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 20.2
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 20.2
3	Лабораторная работа	Содержит 6 лабораторных заданий, предусматривающих разработку и тестирование криптографических и стеганографических алгоритмов	При успешно выполнении работы осуществляется допуск к контрольной работе, в противном случае обучающийся не допускается к контрольной работе.
4	КИМ промежуточной аттестации	Каждый контрольно- измерительный материал для проведения промежуточной аттестации включает 2 вопроса для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 20.2

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Пример задания для выполнения лабораторной работы

Лабораторная работа №3

«Изучение асимметричных алгоритмов шифрования»

Цель работы:

Изучение работы асимметричных алгоритмов шифрования на примере алгоритма RSA.

Форма контроля: *отчёт в электронном виде*

Количество отведённых аудиторных часов: *4*

Задание:

Получите у преподавателя вариант задания и напишите код, реализующий заданный алгоритм. Составьте отчёт о проделанной работе, в котором отразите следующие пункты:

1. ФИО исполнителя и номер группы.
2. Название и цель лабораторной работы.

3. Номер своего варианта.
4. Код, написанный исполнителем.
5. Результаты работы программы.

Примеры контрольных вопросов:

1. На чем основывается надежность алгоритма RSA?
2. Какие преобразования лежат в основе криптосистем с открытым ключом?

Пример варианта задания:

Провести дешифрование текста, зашифрованного алгоритмом RSA, на основе известного открытого ключа Kp и шифрованного текста C.

Kp = {n=471090785117207; e=12377}

C = 3149991122810652053617063415173219874910986 67.

Описание технологии проведения

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Требования к выполнению заданий (или шкалы и критерии оценивания)

При оценивании используется количественная шкала. Критерии оценивания приведены выше в таблице раздела 20.2.

Приведённые ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний по дисциплине.

Задания закрытого типа

1. Шифр – это

а) состояние, выражающее процесс образования зашифрованных данных из открытых данных;

б) ключевое запоминающее устройство;

в) совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с использованием ключей;

г) значение исходных открытых параметров алгоритма криптографического преобразования

2. Для создания подписи следует использовать

а) свой закрытый ключ;

б) свой открытый ключ;

в) закрытый ключ получателя;

г) открытый ключ получателя

3. Криптосистемы с последовательным выполнением преобразований над элементами открытого текста называются

а) блочными шифрами;

б) поточными шифрами;

в) двоичными аддитивными шифрами;

г) криптосистемами с ключом однократного применения

4. Алгоритм Диффи-Хеллмана основан на следующей математической задаче

а) факторизации числа;

б) нахождения простых чисел;

в) дискретного логарифмирования

5. Целостность – это

а) невозможность несанкционированного просмотра информации;

б) невозможность несанкционированного доступа к информации;

в) невозможность несанкционированного изменения информации

6. Функция, предназначенная для сжатия строки произвольной длины до нескольких десятков или сотен бит

а) ЭЦП;
б) логарифмическая функция;
в) функция Эйлера;
г) хеш-функция

7. Максимальная длина ключа в алгоритме Blowfish

а) 512 бит;
б) 128 бит;
в) 256 бит;
г) 448 бит

8. Размер общего ключа алгоритма 3DES (все ключи разные)

а) 56 бит;
б) 112 бит;
в) 168 бит;
г) 256 бит

9. Название криптосистем, в которых ключ шифрования и ключ дешифрования совпадают

а) симметричные;
б) асимметричные;
в) простые;
г) гибридные

10. Установление санкционированным получателем того факта, что полученное сообщение послано санкционированным отправителем

а) идентификация;
б) авторизация;
в) аутентификация;
г) контроль целостности

11. Алгоритм Диффи-Хеллмана дает возможность

а) безопасно обменяться общим секретом при условии аутентификации сторон;
б) безопасно обменяться общим секретом;
в) зашифровать сообщение;
г) подписать сообщение

12. Порядок использования операций шифрования и расшифровки в алгоритме 3DES при создании зашифрованного сообщения

а) $C = E_{K1}[D_{K2}[E_{K1}[M]]]$, $K1 \neq K2$ $(E \rightarrow D \rightarrow E)$;
б) $C = D_{K1}[E_{K2}[D_{K1}[M]]]$, $K1 \neq K2$ $(D \rightarrow E \rightarrow D)$;
в) не имеет значения

13. Какой из алгоритмов реализует асимметричное шифрование и м. использоваться для ЭЦП

а) 3DES;
б) Blowfish;
в) AES;
г) RSA

14. Алгоритм RSA основан на следующей математической задаче

а) дискретного логарифмирования;
б) факторизации числа;
в) нахождения простых чисел

15. Другое название линейного поточного шифрования данных

а) перестановка;
б) гаммирование;
в) подстановка;
г) имитовставка

16. Разрядность шифруемых блоков данных в алгоритме RSA

а) больше разрядности ключа;
б) равна разрядности ключа;
в) меньше разрядности ключа;
г) произвольная

17. Хеш-функция должна обладать следующими свойствами (несколько ответов)
а) для любого данного значения хеш-кода h вычислительно сложно найти M такое, что H(M) = h;
б) хеш-функция H должна применяться к блоку данных фиксированной длины;
в) хеш-функция H создает выход фиксированной длины;
г) хеш-функция H должна создавать выход произвольной длины;
д) для любого данного x вычислительно сложно найти y ≠ x, что H(y) = H(x);
е) для любого данного x вычислительно сложно найти H (x)

18. Отличие самосинхронизирующихся поточных шифров от блочных
а) шифрограмма есть результат наложения последовательности текста и последовательности работающего генератора гамма;
б) шифрограмма есть результат наложения последовательности текста и последовательности гаммы, зависящей от входной последовательности;
в) для шифрования и расшифровки используются разные ключи;
г) каждый блок открытого текста шифруется независимо от остальных блоков

19. Отличие синхронных поточных шифров от блочных
а) шифрограмма есть результат наложения последовательности текста и последовательности гаммы, зависящей от входной последовательности;
б) для шифрования и расшифровки используются разные ключи;
в) каждый блок открытого текста шифруется независимо от остальных блоков;
г) шифрограмма есть результат наложения последовательности текста и последовательности работающего генератора гамма

20. Аутентификация сторон в алгоритме Диффи-Хеллмана необходима, потому что
а) в противном случае атакующий может взломать дискретный логарифм;
б) в противном случае атакующий может перехватить передаваемые открытые ключи и заменить их своим открытым ключом;
в) в противном случае стороны не смогут вычислить общий секрет;

21. Режим шифрования, сохраняющий статистические особенности открытого текста
а) Cipher block chaining (CBC);
б) Cipher feed back (CFB);
в) Electronic code book (ECB)

22. Задачей дискретного логарифмирования является
а) нахождение степени, в которую следует возвести простое число для получения заданного целого числа;
б) нахождение степени, в которую следует возвести целое число для получения заданного целого числа;
в) разложение числа на простые сомножители

23. Электронная подпись – это
а) имитовставка;
б) информация, необходимая для шифрования и расшифровки сообщений;
в) способ преобразования исходного секретного сообщения с целью его защиты;
г) присоединяемый к сообщению блок данных, полученный с использованием криптографического преобразования

24. Функция, для которой легко найти прямое отображение и очень сложно найти обратное
а) нелинейная;
б) односторонняя;
в) линейная;
г) многозначная

25. Режим CBC используется для того, чтобы
а) одинаковые незашифрованные блоки преобразовывались в различные зашифрованные блоки;

б) не было необходимости разбивать сообщение на целое число блоков достаточно большой длины;

в) увеличить скорость шифрования

26. Наука, изучающая математические методы нарушения конфиденциальности и целостности информации

а) криптоанализ;
б) ктиптология;
в) криптография;
г) стегоанализ

27. Ситуация, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст

а) коллизия;
б) избыточность;
в) хеширование;
г) атака повтора

28. Протокол Нидхема-Шредера применяется для

а) шифрования;
б) аутентификации;
г) выработки электронной подписи

29. Метод построения блочных шифров, используемый в алгоритме AES

а) SP-сеть;
б) сеть Фейстеля

30. Разрядность ключа алгоритма шифрования ГОСТ Р 34.12-2015

а) 128 бит;
б) 192 бита;
в) 256 бит;
г) 320 бит

Задания открытого типа

1. Набор криптографических преобразований, предназначенных для работы в единой технологической цепочке с целью решения определенной задачи защиты информационного процесса.

2. Событие, в результате которого произошла или могла произойти утрата одного из свойств криптографического ключа, обеспечивающего безопасность криптосистемы

3. Механизм, генерирующий случайные величины для дальнейшего их использования в качестве инициализационного вектора ГПСЧ.

4. Устройство или алгоритм, который выдает последовательность статистически независимых и несмещенных бит.

5. Генераторы случайных чисел по способу получения чисел делятся на

6. Задача обращения функции g^x в некоторой конечной мультипликативной группе G называется.

7. Специальные таблицы поиска для обращения криптографических хеш-функций (использующие различные функции редукции).

8. Средство для обеспечения имитозащиты в протоколах аутентификации сообщений с доверяющими друг другу участниками – специальный набор символов, добавляемый к сообщению, предназначенный для обеспечения его целостности и аутентификации источника данных.

9. Перечислите известные алгоритмы диверсификации секретных ключей на основе строковых значений пароля (минимум 2 алгоритма).

10. Порядок использования ключей в асимметричных криптосистемах при шифровании и расшифровании данных. Шифрование на … ключе, расшифрование на … ключе.

11. Порядок использования ключей при создании и проверке электронной подписи (асимметричный вариант). Создание подписи на … ключе, проверка на … ключе.

12. Вид злоумышленных действий, при котором абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле послал.

13. Описание распределенного алгоритма, в процессе выполнения которого два (или более) участников последовательно выполняют определенные действия и обмениваются сообщениями.

Задания с развёрнутым ответом

1. Дайте определение электронной подписи. Нарисуйте обобщенную схему подписывания п проверки подписи. Распишите схему электронной подписи на основе алгоритма RSA (с двумя ключевыми парами).

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение электронной подписи. Корректную схему подписывания и проверки электронной подписи, а также корректную схему электронной подписи на основе алгоритма RSA.	3 балла
Обучающийся приводит полное и безошибочное определение электронной подписи. Приводит схему подписывания и проверки электронной подписи, а также схему электронной подписи на основе алгоритма RSA. Описание может содержать незначительные неточности.	2 балла
Представлено корректное определение электронной подписи. Схема подписывания и проверки электронной подписи может содержать незначительные неточности. Схема электронной подписи на основе алгоритма RSA не приведена или содержит существенные ошибки.	1 балл
Представлено неполное или содержащее грубые ошибки определение электронной подписи. Схема подписывания и проверки электронной подписи отсутствует или имеет существенные ошибки. Схема электронной подписи на основе алгоритма RSA не приведена или содержит существенные ошибки.	0 баллов

2. Опишите основные режимы выполнения алгоритмов блочного симметричного шифрования (ECB, CBC, CFB, OFB, CTR), приведите схемы их работы. Сформулируйте рекомендации по использованию каждого их режимов.

Критерии оценивания	Шкала оценок
Обучающийся приводит подробное описание режимов выполнения алгоритмов блочного симметричного шифрования, а также схемы их работы. Приводит корректные рекомендации по использованию каждого из режимов.	3 балла
Обучающийся приводит достаточно развернутое описание режимов выполнения алгоритмов блочного симметричного шифрования. Описание может содержать незначительные неточности. Приводит корректные рекомендации по использованию каждого из режимов.	2 балла
Представлено достаточно развернутое, но содержащее незначительные неточности описание режимов выполнения алгоритмов блочного симметричного шифрования. Отсутствуют схемы и рекомендации по использованию каждого из режимов.	1 балл
Представлено неполное или содержащее грубые ошибки описание режимов выполнения алгоритмов блочного симметричного шифрования. Отсутствуют схемы и рекомендации по использованию каждого из режимов.	0 баллов

3. Опишите принципы работы и приведите примеры генераторов псевдослучайных числовых последовательностей (ГПСЧП). Приведите не менее четырех статистических критериев, используемых для проверки выхода ГПСЧП на стохастичность.

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое описание принципов работы ГПСЧП, приводит примеры генераторов. Рассматривает не менее четырех статистических критериев для проверки генерируемых псевдослучайных последовательностей на стохастичность.	3 балла
Обучающийся приводит достаточно развернутое описание принципов работы ГПСЧП, но не приводит примеры генераторов. Рассматривает не менее трех статистических критериев для проверки генерируемых псевдослучайных последовательностей на стохастичность.	2 балла
Представлено достаточно полное описание принципов работы ГПСЧП. Примеры генераторов отсутствуют. Рассмотрено менее трех тестов на стохастичность генерируемых последовательно-	1 балл

стей. В описании содержатся неточности.	
Представлено неполное или содержащее грубые ошибки описание принципов работы ГПСЧП. Примеры генераторов и тестов на стохастичность последовательностей отсутствуют.	0 баллов

4. Опишите принципы работы регистров сдвига с линейной (LFSR) и нелинейной обратной связью (NLFSR). Приведите примеры генераторов псевдослучайных двоичных последовательностей на основе сдвиговых регистров. Нарисуйте схему, реализующую линейный сдвиговый регистр, задаваемый полиномом $x^7 + x^4 + x^3 + 1$.

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое описание принципов работы линейных и нелинейных регистров сдвига. Приводит примеры генераторов на основе сдвиговых регистров, а также корректную схему, реализующую линейный сдвиговый регистр, заданный полиномом.	3 балла
Обучающийся приводит достаточно развернутое описание принципов работы линейных и нелинейных регистров сдвига. Приводит корректную схему, реализующую линейный сдвиговый регистр, заданный полиномом. Допускаются незначительные неточности, отсутствуют примеры генераторов.	2 балла
Представлено достаточно полное и корректное описание принципов работы линейных и нелинейных регистров сдвига. Отсутствуют примеры генераторов. Приведенная схема сдвигового регистра, соответствующая заданному полиному, содержит неточности.	1 балл
Представлены неполное или содержащее грубые ошибки описание принципов работы линейных и нелинейных регистров сдвига. Отсутствуют примеры генераторов. Отсутствует или приведена некорректная схема сдвигового регистра, соответствующая заданному полиному.	0 баллов

5. Дайте определение криптографической хеш-функции. Сформулируйте требования, предъявляемые к криптографическим хеш-функциям. Распишите схему Меркла-Дамгарда.

Критерии оценивания	Шкала оценок
Обучающийся приводит безошибочное определение криптографической хеш-функции. Приводит полные и корректные требования, предъявляемые к криптографическим хеш-функциям, корректную схему Меркла-Дамгарда.	3 балла
Обучающийся приводит безошибочное определение криптографической хеш-функции. Приводит полные требования, предъявляемые к криптографическим хеш-функциям, а также схему Меркла-Дамгарда. Описание может содержать незначительные неточности.	2 балла
Представлено корректное определение криптографической хеш-функции. Требования, предъявляемые к криптографическим хеш-функциям, приведены частично. Схема Меркла-Дамгарда содержит неточности.	1 балл
Представлено неполное или содержащее ошибки определение криптографической хеш-функции. Требования, предъявляемые к криптографическим хеш-функциям, приведены частично и содержат ошибки. Схема Меркла-Дамгарда не приведена или содержит существенные ошибки.	0 баллов

6. Распишите схему распределения ключей Диффи-Хеллмана в классическом варианте и в варианте на эллиптических кривых.

Критерии оценивания	Шкала оценок
Обучающийся приводит корректные схемы распределения ключей Диффи-Хеллмана в классическом варианте и в варианте на эллиптических кривых, а также развернутое их описание.	3 балла
Обучающийся приводит схемы распределения ключей Диффи-	2 балла

Хеллмана в классическом варианте и в варианте на эллиптических кривых и краткое их описание. Описание может содержать незначительные неточности.	
Приведены обе схемы распределения ключей Диффи-Хеллмана, но в них содержатся неточности. Приведена только одна из схем распределения ключей Диффи-Хеллмана (классический вариант либо вариант на эллиптических кривых).	1 балл
Представлена одна их схем распределения ключей Диффи-Хеллмана (классический вариант либо вариант на эллиптических кривых). Схема содержит существенные ошибки.	0 баллов

7. Дайте определение криптографического протокола. Распишите схему работы симметричного и асимметричного варианта протокола Нидхема-Шредера для аутентификации и обмена ключами.

Критерии оценивания	Шкала оценок
Обучающийся приводит полное и безошибочное определение криптографического протокола. Приводит корректное описание этапов работы симметричного и асимметричного варианта протокола Нидхема-Шредера для аутентификации и обмена ключами.	3 балла
Обучающийся приводит полное и безошибочное определение криптографического протокола. Приводит описание основных этапов работы симметричного и асимметричного варианта протокола Нидхема-Шредера для аутентификации и обмена ключами. Описание может содержать незначительные неточности.	2 балла
Обучающийся приводит корректное определение криптографического протокола. Приводит только один из вариантов (симметричный или асимметричный) протокола Нидхема-Шредера. Описание может содержать неточности.	1 балл
Представлено неполное или некорректное определение криптографического протокола. Приведены неполные или некорректные описания вариантов протокола Нидхема-Шредера для аутентификации и обмена ключами.	0 баллов

8. Отпишите алгоритм шифрования Эль-Гамаля.

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое и безошибочное описание алгоритма шифрования Эль-Гамаля.	3 балла
Обучающийся приводит развернутое описание алгоритма шифрования Эль-Гамаля, которое может содержать незначительные неточности.	2 балла
Обучающийся приводит недостаточно развернутое описание алгоритма шифрования Эль-Гамаля. Описание может содержать отдельные неточности.	1 балл
Представлено неполное или некорректное описание алгоритма шифрования Эль-Гамаля. Присутствуют грубые ошибки или неточности.	0 баллов

9. Опишите схему централизованного управления распределением открытых ключей.

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое и безошибочное описание схемы централизованного управления распределением открытых ключей.	3 балла
Обучающийся приводит развернутое описание схемы централизованного управления распределением открытых ключей, которое может содержать незначительные неточности.	2 балла
Обучающийся приводит недостаточно развернутое описание схемы централизованного управления распределением открытых ключей. Описание может содержать отдельные неточности.	1 балл

Представлено неполное или некорректное описание схемы централизованного управления распределением открытых ключей. Присутствуют грубые ошибки или неточности.	0 баллов

10. Опишите основные этапы жизненного цикла криптографических ключей.

Критерии оценивания	Шкала оценок
Обучающийся приводит развернутое и полностью корректное описание основных этапов жизненного цикла криптографических ключей.	3 балла
Обучающийся приводит развернутое описание основных этапов жизненного цикла криптографических ключей. Описание может содержать незначительные неточности.	2 балла
Обучающийся приводит частичное описание жизненного цикла криптографических ключей.	1 балл
Представлено неполное или некорректное описание основных этапов жизненного цикла криптографических ключей. Присутствуют грубые ошибки или неточности.	0 баллов

20.2. Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае невыполнения в течение семестра), проверку выполнения установленного перечня лабораторных заданий, позволяющих оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

Для оценки теоретических знаний используется перечень контрольно-измерительных материалов. Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает два задания - вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции. При оценивании используется количественная шкала. Критерии оценивания приведены в таблице ниже.

Для оценивания результатов обучения на экзамене используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

- знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;
- умение проводить обоснование и представление основных теоретических и практических результатов;
- умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторных заданий;
- умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;
- владение навыками программирования в рамках выполняемых лабораторных заданий.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций; пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки. Не выполнены лабораторные работы в соответствии с установленным перечнем.	–	Неудовлетворительно

Примерный перечень вопросов к экзамену

№	Содержание
1	Основы государственной информационной политики и информационной безопасности Российской Федерации
2	Угрозы информационной безопасности, модели нарушителей
3	Методы и модели оценки уязвимости информации
4	Рекомендации по использованию моделей оценки уязвимости информации
5	Функции и задачи защиты информации
6	Предметная область криптографии
7	Алгоритмы симметричного шифрования, сеть Фейстеля
8	Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB)
9	Криптосистемы с открытым ключом, однонаправленные функции
10	Однонаправленные хэш-функции
11	Электронная подпись
12	Программные датчики ПСП чисел
13	Принципы работы криптоаналитических алгоритмов.
14	Предметная область стеганографии
15	Стеганографическое скрытие данных в пространственной области контейнера
16	Стеганографическое скрытие данных в частотной области контейнера, методы кодирова-

	ния с расширением спектра
17	Статистические и структурные методы скрытия информации
18	Цифровые водяные знаки
19	Стегоанализ. Визуальный, статистический, универсальный стегоанализ.
20	Архитектура систем защиты информации
21	Общие требования к построению надежной системы защиты

Пример контрольно-измерительного материала

УТВЕРЖДАЮ

Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота

__.__.2023

Направление подготовки / специальность 09.03.04 Программная инженерия

Дисциплина Б1.О.42 Информационная безопасность

Форма обучения Очное

Вид контроля Экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Режимы выполнения алгоритмов симметричного шифрования (ECB, CBC, CFB, OFB).
2. Цифровые водяные знаки.

Преподаватель _____ А.С. Мальцев