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

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

17.03.2025

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.03 Математические основы защиты информации и информационной безопасности

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Специализация:

«Математические методы защиты информации»

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

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: кибербезопасности информационных систем

6. Составители программы: Сафронов Виталий Владимирович,
доцент кафедры кибербезопасности информационных систем

7. Рекомендована: НМС факультета ПММ, протокол № 6 от 17.03.2025

_____

отметки о продлении вносятся вручную)

8. Учебный год: 2027/2028 **Семестр(ы): 6**

9.Цели и задачи учебной дисциплины:

Цели дисциплины — формирование у обучающихся знания по обеспечению информационной безопасности информационно-управляющих и информационно-логистических систем.

Задачи дисциплины: дать обучающимся необходимые знания, умения и навыки, в том числе: теоретические и практические проблемы обеспечения информационной безопасности информационно-управляющих и информационно-логистических систем; навыки самостоятельного, творческого использования теоретических знаний для предотвращения незаконного использования информации в практической деятельности.

10. Место учебной дисциплины в структуре ООП: Дисциплина входит в вариативную часть программы специалитета. Изучение данного курса должно базироваться на знании дисциплин «Алгебра», «Дискретная математика», «Информатика», «Методы программирования», «Математическая логика и теория алгоритмов». Дисциплина является предшествующей для дисциплин «Методы и средства криптографической защиты данных», «Методы алгебраической геометрии в криптографии».

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
ПК-1	Способен проводить анализ требований и выполнять работы по проектированию программного обеспечения с применением математических методов защиты	ПК-1.1	Применяет различные методы разработки программного обеспечения и технологии программирования	Знать: – *методы разработки ПО и технологии программирования;* – *технологии обработки данных;* – *современные математические методы защиты информации;* – *наиболее известные симметричные криптосистемы;* – *наиболее известные криптосистемы открытого ключа.* Уметь: – *применять технологии обработки данных и анализировать возможности их использования при разработке ПО;* – *разрабатывать программные алгоритмы, реализующие современные математические методы защиты информации;* – *шифровать информацию с помощью различных симметричных криптосистем;* – *шифровать информацию с помощью различных криптосистем открытого ключа;* – *шифровать информацию с помощью различных криптосистем поточного шифрования.* Владеть: – *навыками построения модели информационной безопасности;* – *навыками создавать ЭЦП;* – *навыками работы с ключами;* – *нав*ыками вычисления хэш функций.
		ПК-1.2	Использует современные математические методы и алгоритмы функционирования для компонентов программных средств	
		ПК-1.3	Применяет технологии обработки данных, анализирует возможности их использования при разработке программного обеспечения в профессиональной деятельности	
ПК-2	Способен проводить исследования на всех этапах жизненного цикла средств защиты информации в профессиональной деятельности.	ПК-2.3	Использует типовое и специализированное программное обеспечение, проводит компьютерное исследование, формирует описание результатов и формулирует выводы.	

ПК-3	Способен осуществлять разработку, анализ и обосновывать эффективность применяемых математических методов защиты информации, возникающих при работе программных и программно-аппаратных средств защиты информации при решении профессиональных, исследовательских и прикладных задач	ПК-3.1	Формирует и применяет аналитическую модель эффективности внедрения средств защиты информации различных классов.	
		ПК-3.3	Анализирует эффективность функционирования программных средств защиты информации.	
		ПК-3.4	Разрабатывает программные алгоритмы, реализующие современные математические методы защиты информации.	

12. Объем дисциплины в зачетных единицах/час (*в соответствии с учебным планом)* **—** 2/72.

Форма промежуточной аттестации *(зачет/экзамен)* зачет.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			6 семестр
Аудиторные занятия		54	54
в том числе:	лекции	18	18
	практические	0	0
	лабораторные	36	36
Самостоятельная работа		18	18
в том числе: курсовая работа (проект)			
Форма промежуточной аттестации *(зачет – 0 час. / экзамен – 0 час.)*		0	0
Итого:		72	72

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью он-

			лайн-курса, ЭУМК *
1. Лекции			
1.1	Введение	Термины и определения. Модели безопасности, понятие компьютерной атаки. Виды защиты информации. Краткий исторический обзор развития криптографии. Криптография и криптоанализ.	Онлайн-курс «Б1.Б.51.05/Б1.В.03 Математические основы защиты информации и информационной безопасности (МОЗИ) Семестр: 8/6 ». – https://edu.vsu.ru/course/view.php?id=2069
1.2	Элементы теории чисел и модулярная арифметика	Теорема Эйлера и малая теорема Ферма; вычисление обратных по модулю величин. Операции по модулю. Системы вычетов. Квадратичные вычеты.	
1.3	Симметричные и ассиметричные криптосистемы. ЦП	Перестановки. Замены. Аналитические методы. Гаммирование. Комбинированные методы. Дискретный логарифм, задачи факторизации. Рюкзачная криптосистема; Криптосистемы Эль Гамаля и RSA. Цифровые подписи.	
1.4	Математические модели шифрования с использованием конечных полей. Идеальные криптосистемы	Первообразные корни, поля Галуа. Теоремы Шеннона, ограничения на использование теоретически-стойких криптосистем. Эллиптические кривые.	
1.5	Потоковое кодирование	Классификация поточных шифров (синхронные и самосинхронизирующиеся). Генераторы псевдослучайных последовательностей:	
1.6	Математические методы аутентификации и хэширования	Однонаправленные функции, алгоритмы электронных подписей и формирования хэш-функций	
2. Практические занятия не предусмотрены			
3. Лабораторные занятия			
3.1	Лабораторная работа №1 Тема: Алгоритм Евклида и расширенный алгоритм Евклида. Алгоритмы факторизации.	*Теоретические сведения* 1. Элементы теории чисел. Теорема и алгоритм деления. 2. Алгоритм Евклида. 3. Расширенный алгоритм Евклида. 4. Оценка сложности алгоритмов. 5. Метод пробных делений. 6. Алгоритм факторизации Ферма. *Практическая часть* 1. Реализация алгоритмов.	
3.2	Лабораторная работа №2. Тема: Проверка чисел на простоту.	*Теоретические сведения* 1. Способы проверки чисел на простоту 2. тест Соловея-Штрассена 3. тест Миллера-Рабина *Практическая часть* Реализация алгоритмов.	
3.3	Лабораторная работа №3 Тема: Выполнение операций по модулю	*Теоретические сведения* 1. *Теоретические сведения* 1. Сложение, вычитание, умножение по модулю. Деление по модулю. Сравнимость. 2. Быстрое возведение в степень. Квадратичный алгоритм. Алгоритм без двоичного представления. *Практическая часть* 1. Реализация и исследование алгоритмов.	
3.4	Лабораторная работа №4 Тема: Симметричные схемы.	*Теоретические сведения* *1.* Перестановки. *2.* Замены. *3.* Аналитические методы. *4.* Гаммирование. *5.* Комбинированные методы *Практическая часть* 1. Реализация и исследование алгоритмов по вариантам.	
3.5	Лабораторная работа №5 Тема: Асимметричные схемы..	*Теоретические сведения* *1.* Рюкзачная криптосистема. *2.* Криптосистемы Эль Гамаля. *3.* RSA	

		Практическая часть 1. Реализация и исследование алгоритмов по вариантам
3.6	Лабораторная работа №6 Тема: Поля Галуа. Эллиптические кривые.	*Теоретические сведения* 1. Эллиптические кривые. Точки эллиптических кривых. 2. Поля Галуа. *Практическая часть* 1. Реализация работы с эллиптическими кривыми по вариантам.
3.7	Лабораторная работа № 7 Тема: Алгоритмы поточного кодирования.	*Теоретические сведения* *1.* A5; *2.* RC4; *3.* Seal; *4.* Wake. *Практическая часть* 1. Реализация алгоритмов по вариантам.
3.8	Лабораторная работа № 8 Тема: Алгоритмы ЦП.	*Теоретические сведения* *1.* ГОСТ; *2.* DSA; *3.* ЦП с использованием эллиптических кривых *Практическая часть* 1. Реализация алгоритмов по вариантам.
3.9	Лабораторная работа № 9 Тема: хэширование.	*Теоретические сведения* *1.* MD5; *2.* SHA-1; *3.* SHA-2 и др. *Практическая часть* 1. Реализация алгоритмов по вариантам.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Введение	2			2	4
2	Элементы теории чисел и модулярная арифметика	3		6	3	12
3	Симметричные и ассиметричные криптосистемы. ЦП	6		12	6	24
4	Математические модели шифрования с использованием конечных полей. Идеальные криптосистемы	3		8	3	14
5	Потоковое кодирование	2		6	2	10
6	Математические методы аутентификации и хэширования	2		4	2	8
	Итого:	18		36	18	72

14. Методические указания для обучающихся по освоению дисциплины

Работа с конспектами лекций, выполнение лабораторных заданий, заданий текущей и промежуточной аттестаций.

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 *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

№ п/п	Источник
1	*Нестеров С. А., Информационная безопасность: учебник и практикум для*

	академического бакалавриата / С. А. Нестеров, М., Юрайт, 2016, 321с
2	*Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. [Электронный ресурс].*
3	*Царев, Р.Ю. Программирование на языке Си : учебное пособие / Р.Ю. Царев. – Красноярск : Сибирский федеральный университет, 2014. – 108 с. – URL: https://biblioclub.lib.vsu.ru/index.php?page=book&id=364601 (16.09.2016).*
4	*Романьков В. А. Алгебраическая криптология : монография / В.А. Романьков ; Омский гос. ун-т им. Ф.М. Достоевского Омск : Издательство Омского государственного университета, 2020 261 с. ISBN 978-5-7779-2491-9*

б) дополнительная литература:

№ п/п	Источник
5	*Кетков, Ю.Л. Введение в языки программирования С и С++ : курс / Ю.Л. Кетков. – М. : Интернет-Университет Информационных Технологий, 2008. – 252 с. – URL: https://biblioclub.lib.vsu.ru/index.php?page=book&id=234040 (16.09.2016).*
6	*Шилдт Г. С++. Базовый курс / Г. Шилдт. – М. : Вильямс, 2015. – 624 с.*
7	*Столов Е.Л. Генераторы случайных чисел в системах компьютерной безопасности[Электронный ресурс]. - Казань, 2014. - Режим доступа:: http://shelly.kpfu.ru/e-ksu/docs/F833856100/FinalGen.pdf*
8	*Воронков Б. Н. Технология двойного "затемнения" в электронных платежных системах. Алгоритмы, программа, моделирование / Б. Воронков, Ю. Крыжановская, Ю. Фельдшерова Saarbrucken : LAP LAMBERT Academic Publishing, 2014* 99 с. : ил. ISBN 978-3-659-55591-6

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

№ п/п	Источник
9	*www.lib.vsu.ru – ЗНБ ВГУ*
10	*https://e.lanbook.com/ – Электронно-библиотечная система "Лань"*
	Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению лабораторных и контрольных работ)

№ п/п	Источник
1	*Криптографические методы защиты информации [Электронный ресурс] : учебно-методическое пособие : [для студ. фак. прикладной математики, информатики и механики очной и очно-заоч. форм обучения, для направлений и специальностей: 01.03.02 - Прикладная математика и информатика, 02.03.02 - Фундаментальная информатика и информационные технологии, 01.04.02 - Прикладная математика и информатика, 10.05.01 - Компьютерная безопасность] / Воронеж. гос. ун-т ; сост.: Б.Н. Воронков, Ю.А. Крыжановская. — Электрон. текстовые дан. — Воронеж: Издательский дом ВГУ, 2018*
2	*Программные методы защиты информации : Метод. указания к спецкурсу "Теорет. основы защиты информации" : Для студ. 4 к. д/о и 5 к.в/о фак. ПММ / ВГУ. Каф. техн. кибернетики и автомат. регулирования; Сост. Ю.А.Крыжановская Ч.1 Воронеж, 2002 36 с. : ил.. табл. 7.15*
3	*Никифоров С. Н. Методы защиты информации. Шифрование данных [Электронный ресурс] : учебное пособие для спо / Никифоров С. Н. 2-е изд., стер. Санкт-Петербург : Лань, 2022 160 с. ISBN 978-5-507-44449-6*

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

При реализации дисциплины используются модульно-рейтинговая и личностно-ориентированные технологии обучения (ориентированные на индивидуальность студента, компьютерные и коммуникационные технологии). В рамках дисциплины предусмотрены следующие виды лекций: информационная, лекция-визуализация, лекция с применением обратной связи.

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий, для организации самостоятельной работы обучающихся используется онлайн-курс, размещенный на платформе Электронного университета ВГУ (LMS moodle), а также другие Интернет-ресурсы, приведенные в п.15в

18. Материально-техническое обеспечение дисциплины:

Лекционная аудитория должна быть оборудована учебной мебелью, компьютером, мультимедийным оборудованием (проектор, экран, средства звуковоспроизведения), допускается переносное оборудование.

Лабораторные занятия должны проводиться в специализированной аудитории, оснащенной учебной мебелью и персональными компьютерами с доступом в сеть Интернет (компьютерные классы, студии), мультимедийным оборудованием (мультимедийный проектор, экран, средства звуковоспроизведения). Число рабочих мест в аудитории должно быть таким, чтобы обеспечивалась индивидуальная работа студента на отдельном персональном компьютере.

Для самостоятельной работы необходимы компьютерные классы, помещения, оснащенные компьютерами с доступом к сети Интернет.

Программное обеспечение (см. файл МТО):

– ОС Windows 8 (10)

– Интернет-браузер (Google Chrome, Mozilla Firefox)

– Microsoft Visual Studio Community Edition (свободное и/или бесплатное ПО)

– Adobe Reader (свободное и/или бесплатное ПО)

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- контрольная работа
- вопросы

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.	Введение	ПК-1, ПК-3	ПК-1.3, ПК-3.1, ПК-3.3	КИМы для проведения текущей аттестации Задания для лабораторных работ
2.	Элементы теории чисел и модулярная арифметика	ПК-1, ПК-2, ПК-3	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.3, ПК-3.1, ПК-3.3, ПК-3.4	
3.	Симметричные и ассиметричные криптосистемы. ЦП	ПК-1, ПК-2, ПК-3	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.3, ПК-3.1, ПК-3.3, ПК-3.4	
4.	Математические модели шифрования с использованием конечных полей. Идеальные криптосистемы	ПК-1, ПК-2, ПК-3	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.3, ПК-3.1, ПК-3.3, ПК-3.4	
5.	Потоковое кодирование	ПК-1, ПК-2, ПК-3	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.3, ПК-3.1, ПК-3.3, ПК-3.4	
6.	Математические методы	ПК-1, ПК-2, ПК-3	ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.3, ПК-3.1, ПК-3.3, ПК-3.4	

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
	аутентификации и хэширования			
Промежуточная аттестация форма контроля – зачет				КИМы для проведения итоговой аттестации

* В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций.

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

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; защиты лабораторных работ, выполнения контрольной работы.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования. Промежуточная аттестация по итогам освоения дисциплины проводится в форме зачета. Для получения положительной итоговой оценки необходимо выполнение всех лабораторных и контрольной работ.

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью лабораторных и контрольной работ.

Текущая аттестация проводится на занятии одновременно во всей учебной группе в виде проведения очной контрольной работы и опросов по пройденным темам, адрес курса в электронной образовательной среде «Электронный университет ВГУ» https://edu.vsu.ru/course/view.php?id=14848.

Примеры контрольной работы

Контрольная работа

Вариант 1

1. Сколько ключей использует криптосистема RSA?
2. Чем является несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации?
3. Российский стандарт ИБ.
4. Оценка предельных мощностей взлома
5. Вычислить символ Якоби (129,448)
6. GF(p^n)
7. Нахождение первообразных корней. Пример
8. Современные средства и способы обеспечения информационной безопасности.
9. Типы разрушающих программных средств.
10. Решить сравнение $x^2 \equiv 10 \bmod 43$
11. суперсингулярные и несуперсингулярные эллиптические кривые
12. EdDSA

Вариант 2

1. Что такое имитовставка?
2. Перечислите основные свойства стандартов ИБ.
3. Что способствует защите от вредоносного программного обеспечения?

4. Технические, программные и организационно-правовые средства защиты информации.
5. Найти две точки кривой y^2=x^3+ax+b над полем GF(23), и вычислить сумму, если a=1+42 mod 23, b=1+42 mod 23
6. Свойства символа Лежандра. Вычислить (258,355)
7. Составить таблицу умножения ненулевых элементов в фактор- кольце $Z_2[x] / (x^3 + x + 1)$. Выписать получение произведения (x^2+1)(x+1)
8. Эллиптический аналог алгоритма открытого распределения ключей Диффи – Хеллмана
9. Схема Kerberos
10. Вычислить 6P, если P – точка кривой y^2=x^3+x+3 (mod 7)
11. ЭЦП. ГОСТ Р 34.10-2012
12. Требования к эллиптическим кривым, предназначенным для построения криптографических алгоритмов

Лабораторные работы

Примеры заданий

1. Реализовать алгоритм Эвклида, расширенный алгоритм Эвкалида.
2. Модулярный калькулятор.
3. Реализовать тест Соловея-Штрассена.
4. Реализовать алгоритм Френдберга
5. Реализовать криптосистему Эль Гамаля.
6. Реализовать работу с точками эллиптической кривой
7. Реализовать алгоритм Seal
8. ЦП DSA
9. Реализовать алгоритм SHA-2

20.2 Итоговый контроль успеваемости

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

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Зачтено – выполнены и защищены не менее трех четвертей лабораторных работ, получено больше половины верных ответов при опросах, контрольная работа выполнена с положительным результатом.	Пороговый и выше	Зачтено
Не зачтено – выполнено менее трех четвертей лабораторных работ, получено меньше половины верных ответов при опросах, контрольная работа не выполнена или выполнена с отрицательным результатом.	Ниже порогового	Не зачтено

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

ПК-1. Способен проводить анализ требований и выполнять работы по проектированию программного обеспечения с применением математических методов защиты.
ПК-2. Способен проводить исследования на всех этапах жизненного цикла средств защиты информации в профессиональной деятельности.
ПК-3. Способен осуществлять разработку, анализ и обосновывать эффективность применяемых математических методов защиты информации, возникающих при работе программных и программно-аппаратных средств защиты информации при решении профессиональных, исследовательских и прикладных задач.

Вопросы с вариантами ответов

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

1. Сопоставьте:
Способы аутентификации пользователей в КС:

1. Способ аутентификации, основанный на том, что пользователь знает некоторую подтверждающую его подлинность информацию (парольная защита и аутентификация на основе модели «рукопожатия»).

2. Способ аутентификации, основанный на том, что пользователь имеет некоторый материальный объект, который может подтвердить его подлинность (например, пластиковая карта с идентифицирующей пользователя информацией).

3. Способ аутентификации, основанный на таких данных, которые позволяют однозначно считать, что пользователь и есть тот самый субъект, за которого себя выдает (биометрические данные, особенности клавиатурного почерка и росписи мышью и т.п.).

Ответы:

1. вторая группа
2. первая группа
3. третья группа

Ответы: 1-2, 2-1, 3-3

2. К видам утечки информации НЕ ОТНОСИТСЯ:
– несанкционированный доступ
– получение защищаемой информации разведками
– разглашение
+ копирование

3. К неформальным средствам защиты относятся:
– Программные
– Технические
+ Законодательные

4. Что НЕ ОТНОСИТСЯ к физическим средствам защиты?
+ устройства шифрования
– система видеонаблюдения
– системы защиты окон и дверей

5. Протокол обеспечивает конфиденциальность обмена данными между клиентом и сервером, использующими TCP/IP, причем для шифрования используется асимметричный алгоритм с открытым ключом
– HTTP
– UDP
+ SSL

6. Несанкционированное копирование относится к угрозам:
– активным
+ пассивным
– постоянным

7. Определим символ … как:

$$\left(\frac{x}{p}\right)=\left\{\begin{array}{l}1, x=a^2 \bmod p\\ -1, x\neq a^2 \bmod p\\ 0, x=0 \bmod p\end{array}\right\},\ a\in F_p$$

+ Лежандра
– Якоби
– Кронекера

8. Отметьте правильный ответ
Управление, препятствия, маскировка, регламентация, побуждение, принуждение – это:
+ методы защиты информации
– средства защиты информации
– механизмы защиты информации

9. Существует … схемы криптографических систем.
+ 2
– 3
– 4

10. Способность криптографического алгоритма противостоять криптоанализу – это:

+ криптостойкость
– имитостойкость
– абсолютная стойкость
11. Строка бит фиксированной длины, полученная применением симметричного криптографического метода к сообщению, добавляемая к сообщению для обеспечения его целостности и аутентификации источника данных.
+ имитовставка
– дополнение
– ключ
12. … – это документы, регламентирующие основные понятия и концепции информационной безопасности на государственном или межгосударственном уровне, определяющие понятие "защищенная система" посредством стандартизации требований н критериев безопасности, образующих шкалу оценки степени защищенности ВС.
+ стандарты информационной безопасности
– политики информационной безопасности
– требования информационной безопасности
13. Примером мандатной политики безопасности является:
– типизированная матрица доступа
– модель Харрисона-Руззо-Ульмана
+ модель Белла-ЛаПадулы
14. … назначает каждому субъекту и объекту некоторый уровень безопасности из L, разбивая множество сущностей системы на классы, в пределах которых их свойства с точки зрения модели безопасности являются эквивалентными.
+ функция уровня безопасности
– решетка уровня безопасности
– уровень безопасности
15. В криптографии используются:
+ поля Галуа
– поля Хиггса
– фермионные поля
16. Стандарт шифрования ГОСТ 34.12-2018 работает с длинами ключей
– 128 бит
+ 256 бит
– 512 бит

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. … – это однопараметрическое семейство обратимых преобразований из пространства сообщений открытого текста в пространство шифрованных текстов.
+ Криптографическая система
2. Дополните
... – получение защищаемой информации заинтересованным субъектом с нарушением
правил доступа к ней.
+ Несанкционированный доступ
3. Дополните
Все субъекты и объекты КС однозначно идентифицированы; каждому объекту КС присвоена метка конфиденциальности; каждому субъекту КС присвоена степень допуска; право чтения информации из объекта получает только тот субъект, чья степень допуска не больше метки конфиденциальности данного объекта; право на запись информации в объект получает только тот субъект, чей уровень конфиденциальности не меньше метки конфиденциальности данного объекта. Это … управление доступом.
+ мандатное
4. Дополните
… каналы – это каналы утечки, использование которых для несанкционированного доступа не требует непосредственного доступа к техническим устройствам компьютерных систем.
+ Косвенные

5. Атаки по … каналам используют информацию, которая может быть получена с устройства шифрования и не является при этом ни открытым текстом, ни шифртекстом.
+ сторонним
+ побочным
6. … [a], или [a]n, — множество целых чисел, сравнимых по модулю n.
+ система вычетов

7. К моделям кода аутентификации НЕ ОТНОСИТСЯ
+ функциональная
– алгебраическая
– вероятностная

1. Безопасность шифра AES обеспечивается:
(1) размером ключа
(2) гибкостью
(3) простотой
(4) реализуемостью
2. Криптография с симметричными ключами основана на использовании:
(1) одинаковых ключей на приеме и передаче
(2) различных ключей на приеме и передаче
(3) ключей сеанса на приеме и передаче
(4) ключей раунда на приеме и передаче
3. Ева получила электронное письмо с неизвестной ей кодировкой. Перебрав все кодировки (кириллица, юникод, латиница), она прочитала его. Это была атака:
(1) грубой силы
(2) статистическая
(3) по исходному тесту
(4) по выборке исходного текста
4. Ассоциативность — это свойство, при котором результат операции над тремя элементами поля не зависит:
(1) от порядка применения операций к любой паре элементов
(2) от значений элементов
(3) от набора элементов
(4) от количества элементов
5. Количество раундов в DES:
(1) 16
(2) 2
(3) 12
(4) 4
6. Атака "вмешательство" — это угроза:
(1) готовности
(2) целостности
(3) конфиденциальности
(4) секретности
7. В режиме кодовой книги появление одной ошибки при передаче зашифрованного текста приводит к:
(1) искажению всех блоков
(2) невозможности дешифрации всей информации
(3) искажению информации только внутри блока
(4) повторной передаче блока
8. Лазейка — это свойство функции, позволяющее:
(1) легко вычислять прямую функцию и сложно — обратную функцию
(2) легко вычислять прямую функцию и обратную функцию
(3) сложно вычислять прямую функцию и обратную функцию
(4) сложно вычислять прямую функцию и легко — обратную
9. В DES последний раунд при первом способе шифрования и обратного дешифрования отличается от других:
(1) применением смесителя
(2) отсутствием устройства замены
(3) применением устройства замены и смесителя
(4) применением устройства замены
10. Злоумышленник внедряет в компьютер адрес, по которому он получает копии передаваемого сообщения. Это атака:
(1) "модификация"
(2) "вмешательство"
(3) "прекращение обслуживания запроса"
(4) "имитация источника"

1. Сообщение содержит 300 символов в 8-битовом коде ASCII, блочный шифр принимает блоки по 64 бита, тогда весь текст, предназначенный для шифрования, должен содержать ____ бит
(1) 2560
(2) 2400
(3) 2368
(4) 2496

2. Размер блока в DES:
(1) 64 бита
(2) 32 бита
(3) 16 бит
(4) 128 бит
3. Ограничение разглашения о схеме расположения оборонных объектов относится к сохранению:
(1) конфиденциальности
(2) целостности
(3) готовности
(4) секретности
4. Недостаток режима кодовой книги:
(1) большой объем кодовой книги при больших n и K
(2) необходимость большого числа кодов
(3) сложность алгоритма реализации
(4) необходимость разбиения исходного текста
5. Сколько взаимно простых чисел с простым числом p?
(1) p–1
(2) одно
(3) p
(4) p+1
6. Криптография с асимметричными ключами применяет:
(1) математические формулы
(2) подстановку символов
(3) перестановку символов
(4) подстановку и перестановку символов
7. Ева попросила молодого человека сделать ей сюрприз и прислать поздравление с днем рождения со стандартным исходным текстом с использованием шифра предприятия. Получив это письмо, она раскрыла ключ и, пользуясь тем, что период обновления ключа был большим, получила возможность читать чужую почту. Это была атака:
(1) грубой силы
(2) статистическая
(3) по выборке исходного текста
(4) по исходному тесту
8. Атака "имитация источника" — это угроза:
(1) конфиденциальности
(2) целостности
(3) готовности
(4) секретности
9. Проблемы безопасности режима кодовой книги, порождаемые независимостью блоков, могут быть преодолены:
(1) усложнением ключей шифра
(2) случайным порядком шифрования
(3) раздельным шифрованием участков текста
(4) неравномерным разбиением текста

1. Риск является функцией:
(1) вероятности реализации угрозы
(2) размера возможного ущерба
(3) числа уязвимостей в системе
2. В число классов мер процедурного уровня входят:
(1) логическая защита
(2) физическая защита
(3) планирование восстановительных работ
3. Протоколирование и аудит могут использоваться для:
(1) предупреждения нарушений ИБ
(2) обнаружения нарушений
(3) восстановления режима ИБ
4. Что из перечисленного не относится к числу основных аспектов информационной безопасности:
(1) доступность
(2) целостность
(3) конфиденциальность
(4) правдивое отражение действительности
5. Аутентификация на основе пароля, переданного по сети в открытом виде, плоха, потому что не обеспечивает защиты от:
(1) перехвата
(2) воспроизведения

(3) атак на доступность

6. Сигнатурный метод выявления атак хорош тем, что он:
(1) поднимает мало ложных тревог
(2) способен обнаруживать неизвестные атаки
(3) прост в настройке и эксплуатации

7. На межсетевой экран целесообразно возложить функции:
(1) активного аудита
(2) анализа защищенности
(3) идентификации/аутентификации удаленных пользователей

8. Среднее время наработки на отказ:
(1) пропорционально интенсивности отказов
(2) обратно пропорционально интенсивности отказов
(3) не зависит от интенсивности отказов

9. Согласно стандарту X.700, в число функций управления конфигурацией входят:
(1) запуск и остановка компонентов
(2) выбор закупаемой конфигурации
(3) изменение конфигурации системы

10. В число целей политики безопасности верхнего уровня входят:
(1) решение сформировать или пересмотреть комплексную программу безопасности
(2) обеспечение базы для соблюдения законов и правил
(3) обеспечение конфиденциальности почтовых сообщений

11. В число возможных стратегий нейтрализации рисков входят:
(1) ликвидация риска
(2) игнорирование риска
(3) принятие риска

12. В число принципов управления персоналом входят:
(1) "разделяй и властвуй"
(2) разделение обязанностей
(3) инкапсуляция наследования

13. Укажите наиболее существенные с точки зрения безопасности особенности современных российских ИС:
(1) доминирование платформы Wintel
(2) наличие подключения к Internet
(3) наличие разнородных сервисов

1. Злоумышленник перехватывает зашифрованную копию доступа обращения к банкомату и, не расшифровывая ее, использует для получения денег. Это атака:
(1) "прекращение обслуживания запроса"
(2) "наблюдение за трафиком и его анализ"
(3) "повторная передача информации"
(4) "имитация источника"

2. Из нижеперечисленного пассивная атака?
(1) "модификация"
(2) "отказ от обслуживания"
(3) "наблюдение за трафиком и его анализ"
(4) "имитация источника"

3. Меры информационной безопасности направлены на защиту от:
(1) нанесения неприемлемого ущерба
(2) нанесения любого ущерба
(3) подглядывания в замочную скважину

4. В качестве аутентификатора в сетевой среде могут использоваться:
(1) год рождения субъекта
(2) фамилия субъекта
(3) секретный криптографический ключ

5. Протоколирование само по себе не может обеспечить неотказуемость, потому что:
(1) регистрационная информация, как правило, имеет низкоуровневый характер, а неотказуемость относится к действиям прикладного уровня
(2) регистрационная информация имеет специфический формат, непонятный человеку
(3) регистрационная информация имеет слишком большой объем

6. Экран выполняет функции:
(1) разграничения доступа
(2) облегчения доступа
(3) усложнения доступа

7. Информационный сервис считается недоступным, если:
(1) его эффективность не удовлетворяет наложенным ограничениям
(2) подписка на него стоит слишком дорого

(3) не удается найти подходящий сервис

8. Туннелирование может использоваться на следующем уровне эталонной семиуровневой модели:
(1) сетевом
(2) транспортном
(3) сеансовом

9. Цифровой сертификат содержит:
(1) открытый ключ пользователя
(2) секретный ключ пользователя
(3) имя пользователя

10. Экранирование на сетевом уровне может обеспечить:
(1) разграничение доступа по сетевым адресам
(2) выборочное выполнение команд прикладного протокола
(3) контроль объема данных, переданных по TCP-соединению

1. В криптосистеме RSA используется односторонняя прямая функция "____ по модулю"
(1) умножение
(2) возведение в степень
(3) сложение
(4) деление

2. Шифр плейфеера — это многоалфавитный шифр, который позволяет менять ключи, используя:
(1) много алфавитов
(2) правила работы с таблицей
(3) таблицу соответствия места букв
(4) таблицу перестановки

3. Структурный подход опирается на:
(1) семантическую декомпозицию
(2) алгоритмическую декомпозицию
(3) декомпозицию структур данных

4. Окно опасности перестает существовать, когда:
(1) администратор безопасности узнает об угрозе
(2) производитель ПО выпускает заплату
(3) заплата устанавливается в защищаемой ИС

5. Уголовный кодекс РФ не предусматривает наказания за:
(1) создание, использование и распространение вредоносных программ
(2) ведение личной корреспонденции на производственной технической базе
(3) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

6. Уровень безопасности А, согласно "Оранжевой книге", характеризуется:
(1) произвольным управлением доступом
(2) принудительным управлением доступом
(3) верифицируемой безопасностью

7. Контейнеры в компонентных объектных средах предоставляют:
(1) общий контекст взаимодействия с другими компонентами и с окружением
(2) средства для сохранения компонентов
(3) механизмы транспортировки компонентов

8. Самыми опасными источниками внутренних угроз являются:
(1) некомпетентные руководители
(2) обиженные сотрудники
(3) любопытные администраторы

9. Действие Закона "О лицензировании отдельных видов деятельности" распространяется на:
(1) деятельность по использованию шифровальных (криптографических) средств
(2) деятельность по рекламированию шифровальных (криптографических) средств
(3) деятельность по распространению шифровальных (криптографических) средств

10. Подпись называется рандомизированной, если
(1) для разных сообщений с использованием одного и того же закрытого ключа при каждом подписывании создаются разные подписи
(2) для одного и того же сообщения с использованием одного и того же закрытого ключа при каждом подписывании создаются разные подписи
(3) для одного и того же сообщения с использованием разных закрытых ключей при каждом подписывании создаются разные подписи

11. Выберите правильное утверждение:
(1) мастер-ключ должен быть более защищенным, чем ключ сессии
(2) ключ сессии должен быть более защищенным, чем мастер-ключ
(3) мастер-ключ и ключ сессии должны иметь одинаковую степень защиты

Вопросы с вариантами ответов

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

1. Отметьте правильный ответ
Управление, препятствия, маскировка, регламентация, побуждение, принуждение.
+ это методы защиты информации
– это средства защиты информации
– это механизмы защиты информации

2. Установите соответствие

1. Гомофоническая замена
2. Моноалфавитная замена
3. Полиалфавитная
1. это замена, при которой каждой букве алфавита открытого текста ставится в соответствие одна буква шифротекста из этого же алфавита.
2. это замена, при которой используется несколько алфавитов шифротекста.
3. это замена, при которой одному символу открытого текста ставится в соответствие несколько символов шифротекста.
Ответ: 1-3, 2-1, 3-2

3. Что НЕ ОТНОСИТСЯ к области применения криптосистем, использующих асимметричные алгоритмы?
+ Выработка дайджеста сообщения
– Электронная подпись
– Шифрование

4. Какой элемент (параметр) криптосистемы (шифра), согласно правилу О. Керкхоффса, не должен быть известен злоумышленнику?
+ ключ шифрования
– особенности реализации
– шифрованный текст
– алгоритм шифрования

5. К системам с открытым ключом НЕ ОТНОСИТСЯ:
+ DES
– RSA
– El Gamal

6. Шифрсистема, в которой ключи шифрования и расшифрования легко получаются один из другого.
+ Симметричная криптосистема
– Асимметричная криптосистема
– Блочная криптосистема

7. В алгебраической модели шифры $\Sigma_A(X,K,Y,E,D)$ множество K представляет собой:
+ конечное множество возможных ключей
– множество правил зашифрования на всевозможных ключах
– правило зашифрования на определенном ключе

8. К симметричным алгоритмам относится:
+ шифр Плэйфера
– алгоритм Диффи-Хеллмана
– шифр Эль-Гамаля

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. Какие характеристики безопасности обеспечивает «Подлинность сообщения»?

+ целостность и аутентичность (авторство)
+ аутентичность, целостность,
+ целостность и авторство
+ аутентичность, целостность

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. … – функция, осуществляющая преобразование массива входных данных произвольной длины в выходную битовую строку установленной длины, выполняемое определённым алгоритмом.

+ хэш-функция
+ хеш-функция

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