Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Кургалин Сергей Дмитриевич

Кафедра цифровых технологий

25.06.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.08 Основы криптографии

1. Код и наименование направления подготовки/специальности:

02.03.01 Математика и компьютерные науки

2. Профиль подготовки/специализация:

Квантовая теория информации

3. Квалификация (степень) выпускника:

Бакалавриат

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра цифровых технологий

6. Составители программы:

Стадная Надежда Павловна, к.ф.-м.н.

7. Рекомендована:

протокол НМС ФКН № 5 от 10.03.2021

8. Учебный год:

2023-2024

9.Цели и задачи учебной дисциплины:

Цели дисциплины: ознакомление студентов с основными принципами криптографических алгоритмов защиты информации (симметричных и асимметричных классических алгоритмов, квантовых протоколов распределения ключей), областями их использования; ознакомление с основами нейрокриптографии (протоколы обмена ключами между двумя нейронными сетями, принцип хэширования с использованием искусственной нейросети).

Задачами дисциплины являются: изучение базовых криптографических алгоритмов, как классических, так и квантовых; знакомство с математической теорией, использующейся для построения криптографических
алгоритмов, использование имеющихся знаний по математическим дисциплинам, квантовым вычислениям и принципам работы нейросетей для получения навыков реализации простейших криптографических алгоритмов.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к части учебного плана, формируемой участниками образовательных отношений, блок Б1. Для успешного освоения дисциплины необходимо предварительное изучение алгебры, статистики, а также наличие навыков программирования.

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

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПК-1 Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий.	ПК-1.1 Обладает базовыми знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий	Знает основы теории чисел, алгебры эллиптических кривых, основы квантовых вычислений, принципы работы нейросетей; принципы работы и структуру классических симметричных и асимметричных криптографических систем (протоколы генерации и распределения ключей, шифрования и дешифрования), основные принципы хэширования, российские и международные стандарты шифрования, хэширования, формирования электронной цифровой подписи (ЭЦП); методы нейрокриптографической защиты данных.

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПК-3 Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий и программирования и компьютерной техники.	ПК-3.1 Знает основные методы проектирования и производства программного продукта, принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программных продуктов и программных комплексов, их сопровождения, администрирования и развития (эволюции)	Знает современные программно-технические средствапреобразования и защиты данных в информационно-вычислительных системах на основе технологий искусственных нейронных сетей (нейропакет Java Neural Network Simulator (JavaNNS), Emergent (C++), Neural Lab (C++, MVS), STATISTICA Automated Neural Networks и др.) основной пакет для работы MATLAB Neural Network Toolbox; основные базовые протоколы квантового распределения ключей; основные фундаментальные принципы работы и устройство современных систем квантового распределения криптографических ключей (квантово-оптические коммуникации); доказательство стойкости систем квантовой криптографии; различные виды атак на квантовые каналы связи и методы противодействия им; основные принципы действия квантовых нейронных сетей.

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПК-3 Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий и программирования и компьютерной техники.	ПК-3.2 Умеет использовать методы проектирования и производства программного продукта, принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программного продукта	Умеет создавать модели работы классических симметричных и асимметричных криптографических систем (S-DES, AES, RSA, Эль-Гамаля, шифрование на эллиптических кривых), создавать модели ЭЦП; хэш-функций; разрабатывать программные средства защиты данных на основе методов нейрокриптографии (на основе платформ TensorFlow, Scikit-learn, PyTorch и др.); использовать прикладные средства защиты данных с использованием криптографии и нейросетевых технологий при решении практических задач; разрабатывать программные модели квантовых протоколов распределения ключей (язык программирования Python с подключенными библиотеками SymPy, NumPy, Qiskit) разработанной для симуляции различных алгоритмов квантовых вычислений).
ПК-3 Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий и программирования и компьютерной техники.	ПК-3.3 Имеет практический опыт применения указанных выше методов и технологий	Имеет навыки работы со стандартами шифрования; работы с криптографическими алгоритмами DES, RSA, Эль-Гамаля, шифрования на эллиптических кривых, работы с ЭЦП и функциями хэширования; работы с квантовыми протоколами распределения ключей BB84 и B92.

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПК-1 Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий.	ПК-1.2 Умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в математике и информатике	Умеет проводить простейшие вычисления: в теории чисел (применение основных теорем, вычисление дискретных логарифмов); на эллиптических кривых.
ПК-1 Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий.	ПК-1.3 Имеет практический опыт научно-исследовательской деятельности в математике и информатике	Владеет навыками проектирования и использования средств защиты данных на основе криптографии и нейросетевых технологий; моделирования квантовых протоколов распределения ключей.

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Зачет

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 6	Всего
Аудиторные занятия	48	48
Лекционные занятия	32	32
Практические занятия		0
Лабораторные занятия	16	16
Самостоятельная работа	60	60
Курсовая работа		0
Промежуточная аттестация	0	0
Часы на контроль		0
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1	Введение. Предмет и задачи криптографии	Предмет и задачи курса. Основные этапы развития криптографии. Основные понятия и определения. Криптосистема. Виды алгоритмов с использованием ключей; требования к криптографическим системам; основные допущения; безопасность алгоритма.	https://edu.vsu.ru/course/view.php?id=4160
2	Историческое шифрование	Исторические шифры: подстановочные и перестановочные. Шифр Цезаря, квадрат Полибия, решётка Кардано, таблица Виженера, шифр Плейфейера, шифр Вернама, шифр Хилла. Простейшие методы криптоанализа. Лингвистический анализ.	https://edu.vsu.ru/course/view.php?id=4160
3	Введение в теорию чисел.	Основные понятия теории чисел (делители, НОД, простые числа, взаимно простые числа); модулярная арифметика. Теоремы Ферма и Эйлера. Функция Эйлера. Алгоритм Евклида. Расширенный алгоритм Евклида для поиска мультипликативного обратного. Китайская теорема об остатках. Дискретные логарифмы.	https://edu.vsu.ru/course/view.php?id=4160

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
4	Классические криптосистемы.	Симметричные алгоритмы Традиционное шифрование. Поточные и блочные шифры. Шифр Файстеля (сеть Файстеля). Диффузия и конфузия. Алгоритмы DES и S-DES, AES. Использование алгоритмов в системах защиты.	https://edu.vsu.ru/course/view.php?id=4160
5	Классические криптосистемы. Асимметричные алгоритмы.	Общие принципы работы криптосистем с открытым ключом. Принципы построения криптосистем с открытым ключом: шифрование, дешифрование, создание электронной цифровой подписи (ЭЦП), обмен ключами. Условия применимости. Подходы к криптоанализу. Проктол Диффи-Хеллмана.	https://edu.vsu.ru/course/view.php?id=4160

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
6	Классические криптосистемы. Асимметричные алгоритмы. Алгоритмы RSA и Эль-Гамаля.	Описание алгоритмов RSA и Эль-Гамаля: протоколы генерации и распределения ключей; шифрование и дешифрование; анализ стойкости; основные методы атак; современное использование алгоритмов в системах защиты информации; подходы к криптоанализу. Проблемы факторизации числа на простые множители; проблема поиска дискретного логарифма.	https://edu.vsu.ru/course/view.php?id=4160
7	Классические криптосистемы. Асимметричные алгоритмы. Шифрование на эллиптических кривых.	Эллиптические кривые. Определение. Накладываемые условия. Алгебраические операции на кривых. Целочисленные точки на эллиптической кривой. Модулярная арифметика на кривой. Принципы шифрования, дешифрования и формирования ЭЦП с использованием эллиптических кривых. Генерация и обмен ключами. Применение в системах защиты информации. Стойкость алгоритма. Методы атак.	https://edu.vsu.ru/course/view.php?id=4160

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
8	Электронная цифровая подпись. Хэширование.	Принципы формирования ЭЦП на основе асимметричных криптографических систем. Выработка и верификация ЭЦП. Хэширование: терминология, коллизии, свойства, основные этапы формирования хэш-функции. Функция хэширования SHA.	https://edu.vsu.ru/course/view.php?id=4160
9	Криптографические стандарты.	Знакомство с основными стандартами шифрования. ГОСТ 34.10-2018, ГОСТ 34.11-2018, ГОСТ 34.12-2018, FIPS PUB 180-4 SHS, стандарт DSS.	https://edu.vsu.ru/course/view.php?id=4160

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
10	Использование нейронных сетей для криптографических приложений.	Нейрокриптография как наука. Современные области применения (обучение перестановкам, обучение протоколам шифрования с открытым ключом – генерации и обмена ключами, хэширование). Архитектура нейронных сетей на основе целых чисел. Модель сети Кинцеля-Кантера для согласования тайной (ключевой) информации. Анализ архитектуры сети на основе действительных чисел (TPM). Процесс синхронизации архитектур TPM на основе моделей Хебба и анти-Хебба. Безопасность процесса. Атаки на нейросетевые структуры на основе TPM. Возможности использования открытых платформ TensorFlow, Scikit-learn, PyTorch. Обзор библиотек для машинного обучения. Принципы алгоритма хэширования с использованием нейронных сетей. Достоинства и недостатки существующих методов.	https://edu.vsu.ru/course/view.php?id=4160

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
11	Основы квантовой криптографии. Начальные понятия.	Основы квантовых вычислений. Основные понятия, определения. Матричный и дираковский формализм в вычислениях. Знакомство с библиотеками SymPy, NumPy, Qiskit (язык программирования Python).	https://edu.vsu.ru/course/view.php?id=4160
12	Основы квантовой криптографии. Протоколы распределения ключей.	Задача факторизации в алгоритме шифрования RSA. Взлом шифра RSA с использованием алгоритма Шора для факторизации. Квантовый канал связи. Квантовая запутанность. Квантовая телепортация. Защита посредством неортогональных состояний: теорема о запрете клонирования. Защита посредством перепутывания. Связь по квантовым каналам с шумом. Исправление квантовых ошибок. Достоинства и недостатки квантовых каналов связи. Существующие реализации. Практическое применение квантовых каналов связи.	https://edu.vsu.ru/course/view.php?id=4160

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
13	Квантовые нейронные сети в криптографии. Квантовый стохастический однокубитовый нейрон.	Квантовое распределение ключей. Секретность и когерентность информации. Протокол квантового распределения ключей BB84: общая схема, стойкость протокола, стратегии подслушивателя. Другие протоколы квантовой криптографии: протокол B92, протокол 4+2, протокол SARG04. Безопасность квантового распределения ключей.	https://edu.vsu.ru/course/view.php?id=4160
14	Квантовые нейронные сети в криптографии (обзорная лекция).	Модель квантового однокубитового нейрона. Принцип работы квантовых нейронных сетей (КНС). Методы обучения КНС. Виды квантовых нейронных сетей. Возможные перспективы использования КНС в криптографии.	https://edu.vsu.ru/course/view.php?id=4160

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Введение. Предмет и задачи криптографии	2		0	0	2
2	Историческое шифрование	2		2	4	8
3	Введение в теорию чисел.	2		2	6	10

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
4	Классические криптосистемы.	2		2	2	6
5	Классические криптосистемы. Асимметричные алгоритмы.	2		0	2	4
6	Классические криптосистемы. Асимметричные алгоритмы. Алгоритмы RSA и Эль-Гамаля.	2		2	4	8
7	Классические криптосистемы. Асимметричные алгоритмы. Шифрование на эллиптических кривых.	2		2	6	10
8	Электронная цифровая подпись. Хэширование.	2		2	2	6
9	Криптографические стандарты.	2		0	4	6
10	Использование нейронных сетей для криптографических приложений.	6		2	20	28
11	Основы квантовой криптографии. Начальные понятия.	2		0	0	2
12	Основы квантовой криптографии. Протоколы распределения ключей.	2		2	5	9

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
13	Квантовые нейронные сети в криптографии. Квантовый стохастический однокубитовый нейрон.	2		0	2	4
14	Квантовые нейронные сети в криптографии (обзорная лекция).	2		0	3	5
		32	0	16	60	108

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины складывается из аудиторной работы (учебной деятельности, выполняемой под руководством преподавателя) и внеаудиторной работы (учебной деятельности, реализуемой обучающимся самостоятельно).

Аудиторная работа состоит из работы на лекциях и выполнения практических (или лабораторных) заданий в объёме, предусмотренном учебным планом. Лекция представляет собой последовательное и систематическое изложение учебного материала, направленное на знакомство обучающихся с основными понятиями и теоретическими положениями изучаемой дисциплины. Лекционные занятия формируют базу для практических (или лабораторных) занятий, на которых полученные теоретические знания применяются для решения конкретных практических задач. Обучающимся для успешного освоения дисциплины рекомендуется вести конспект лекций и практических (лабораторных) занятий.

Самостоятельная работа предполагает углублённое изучение отдельных разделов дисциплины с использованием литературы, рекомендованной преподавателем, а также конспектов лекций, презентационным материалом (при наличии) и конспектов практических (лабораторных) занятий. В качестве плана для самостоятельной работы может быть использован раздел 13.1 настоящей рабочей программы, в котором зафиксированы разделы дисциплины и их содержание. В разделе 13.2 рабочей программы определяется количество часов, отводимое на самостоятельную работу по каждому разделу дисциплины. Большее количество часов на самостоятельную работу отводится на наиболее трудные разделы дисциплины. Для самостоятельного изучения отдельных разделов дисциплины используется перечень литературы и других ресурсов, перечисленных в пунктах 15 и 16 настоящей рабочей программы.

Успешность освоения дисциплины определяется систематичностью и глубиной аудиторной и внеаудиторной работы обучающегося.

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей, вовремя подключаться к online занятиям, ответственно подходить к заданиям для самостоятельной работы.

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

№ п/п	Источник
1	Басалова, Г. В. Основы криптографии : курс лекций / Г.В. Басалова ; Национальный Открытый Университет "ИНТУИТ" .— Москва : Интернет-Университет Информационных Технологий, 2011 .— 253 с. — http://biblioclub.ru/ .— <URL:http://biblioclub.ru/index.php?page=book&id=233689>.
2	Орлов, В.А. Теория чисел в криптографии : учебное пособие / Орлов В.А., Медведев Н.В., Шимко Н.А., Домрачева А.Б. — Москва : МГТУ им. Н.Э. Баумана, 2011 .— 223 с. — Теория чисел в криптографии [Электронный ресурс]: учеб. пособие / В.А. Орлов, Н.В. Медведев, Н.А. Шимко, А.Б. Домрачева - М. : Издательство МГТУ им. Н. Э. Баумана, 2011. — ISBN 5-7038-3520-3 .— <URL:https://www.studentlibrary.ru/book/ISBN9785703835203.html>.
3	Ищукова, Е. А. Криптографические протоколы и стандарты : учебное пособие / Е.А. Ищукова, Е.А. Лобова ; Министерство образования и науки РФ ; Южный федеральный университет ; Инженерно-технологическая академия .— Таганрог : Издательство Южного федерального университета, 2016 .— 80 с. : ил. — Библиогр. в кн .— http://biblioclub.ru/ .— ISBN 978-5-9275-2066-4 .— <URL:http://biblioclub.ru/index.php?page=book&id=493059>.

б) дополнительная литература:

№ п/п	Источник
1	Фороузан, Б. А. Математика криптографии и теория шифрования / Б.А. Фороузан .— 2-е изд., испр. — Москва : Национальный Открытый Университет «ИНТУИТ», 2016 .— 511 с. : ил., схем. — (Основы информационных технологий) .— Библиогр. в кн .— http://biblioclub.ru/ .— ISBN 978-5-9963-0242-0 .— <URL:http://biblioclub.ru/index.php?page=book&id=428998>.
2	Авдошин, С.М. Дискретная математика. Модулярная алгебра, криптография, кодирование : учебно-методическое пособие / Авдошин С.М., Набебин А.А. — Москва : ДМК-пресс, 2017 .— 352 с. — Дискретная математика. Модулярная алгебра, криптография, кодирование [Электронный ресурс] / Авдошин С. М., Набебин А. А. - М. : ДМК Пресс, 2017. — ISBN 5-94074-408-3 .— <URL:https://www.studentlibrary.ru/book/ISBN9785940744083.html>.
3	Применение искусственных нейронных сетей и системы остаточных классов в криптографии : монография .— Москва : Физматлит, 2012 .— 279 с. — http://biblioclub.ru/. — ISBN 978-5-9221-1386-1 .— <URL:http://biblioclub.ru/index.php?page=book&id=468705>.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	ЗНБ ВГУ: https://lib.vsu.ru/

№ п/п	Источник
2	Электронно-библиотечная система "Университетская библиотека online": http://biblioclub.ru/
3	Электронно-библиотечная система "Лань": https://e.lanbook.com/
4	Электронно-библиотечная система "Консультант студента": http://www.studmedlib.ru
5	Электронный университет ВГУ: https://edu.vsu.ru/

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Басалова, Г. В. Основы криптографии : курс лекций / Г.В. Басалова ; Национальный Открытый Университет "ИНТУИТ" .— Москва : Интернет-Университет Информационных Технологий, 2011 .— 253 с. — http://biblioclub.ru/ .— <URL:http://biblioclub.ru/index.php?page=book&id=233689>.

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

При реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологии на базе портала edu.vsu.ru, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 477

Учебная аудитория: специализированная мебель, ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, 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, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 505п

Учебная аудитория: специализированная мебель, компьютер преподавателя i5-3220-3.3ГГц, монитор с ЖК 17’’, мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 292

Учебная аудитория: специализированная мебель, компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17’’, мультимедийный проектор, экран. Система для видеоконференций Logitech ConferenceCam

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 297

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

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, 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, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 290

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

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 291

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-3220-3,3ГГц, мониторы ЖК 19» (16 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 293

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-8100-3,6ГГц, мониторы ЖК 22» (17 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 295

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-9100-3,6ГГц, мониторы ЖК 24» (14 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 382

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i5-9600KF-3,7ГГц, мониторы ЖК 24» (16 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 383

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i7-9700F-3ГГц, мониторы ЖК 27» (16 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 384

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-2120-3,3ГГц, мониторы ЖК 22» (16 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 385

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-2120-3,3ГГц, мониторы ЖК 19» (16 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 301п

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-2120-3,3ГГц, мониторы ЖК 17» (15 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 303п

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-8100-3,9ГГц, мониторы ЖК 24» (13 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 314п

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-7100-3,6ГГц, мониторы ЖК 19» (16 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, Foxit PDF Reader

394018, г. Воронеж, площадь Университетская, д. 1, ауд. 316п

Компьютерный класс: специализированная мебель, персональные компьютеры на базе i3-9100-3,6ГГц, мониторы ЖК 19» (30 шт.), мультимедийный проектор, экран.

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Дистрибутив Anaconda/Python, MATLAB “Total Academic Headcount – 25”, 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	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Разделы 1-14	ПК-1	ПК-1.1	Лабораторная работа №1 «Исторические шифры»
2	Разделы 1-14	ПК-3	ПК-3.1	Лабораторная работа №3 «Асимметричные криптографические алгоритмы»
3	Разделы 1-14	ПК-3	ПК-3.2	Лабораторная работа №4 «Криптография на эллиптических кривых» Лабораторная работа №5 «Программная реализация модели TPM» или «Программная реализация хэширования с использованием нейросетей» Самостоятельная работа №2 «Основы квантовой криптографии»
4	Разделы 1-14	ПК-3	ПК-3.3	Лабораторная работа №6 «Моделирование работы квантового протокола BB84 (B92)»
5	Разделы 1-14	ПК-1	ПК-1.2	Самостоятельная работа №1 «Теория чисел»
6	Разделы 1-14	ПК-1	ПК-1.3	Лабораторная работа №2 «Симметричные криптографические алгоритмы»

Промежуточная аттестация

Форма контроля - Зачет

Оценочные средства для промежуточной аттестации

Перечень вопросов к зачёту

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:
– лабораторные работы
– самостоятельные работы

Лабораторная работа №1 «Исторические шифры»

Задание: студентам предлагается индивидуально на выбор написать программу шифрования и дешифрования с элементами криптоанализа для одного из выбранных исторических шифров:
1) Шифр Цезаря (в случае выбора этого метода необходим обязательно полноценный криптоанализ на основе частотного лингвистического анализа);
2) Шифр Виженера;
3) Решётка Кардано;
4) Квадрат Полибия;
5) Шифр Хилла.

Критерии оценки:

Оценка «зачтено» выставляется студенту в случае предоставления рабочего кода, шифрующего, дешифрующего сообщения; содержащего простейшие варианты криптоанализа (для шифров Цезаря, Виженера, квадрата Полибия). Студент должен при сдаче кода отвечать на вопросы по коду и по содержанию алгоритмов исторических шифров.
Оценка «незачтено» выставляется студенту, если в рабочем коде отсутствует один из трёх обязательных элементов: шифрование, дешифрование, криптоанализ. Студент не способен ответить на вопросы, связанные с записанным кодом, а также не может ответить на вопросы, касающиеся содержания алгоритмов исторических шифров.

Лабораторная работа №2 «Симметричные криптографические алгоритмы»

Задание: студентам предлагается написать программу шифрования и дешифрования учебного алгоритма S-DES. Обязательные условия для программы:
1) Перевод текста в двоичный код;
2) Генерация ключей;
3) Шифрование;
4) Дешифрование;
5) Перевод зашифрованного сообщения из двоичного кода в текст.

Критерии оценки:
Оценка «зачтено» выставляется студенту в случае предоставления и пояснений рабочего кода, в котором будут присутствовать составляющие, отвечающие всем пяти прописанным условиям. Студент отвечает на вопросы, связанные с работой алгоритма.
Оценка «незачтено» выставляется студенту, если в рабочем коде отсутствует хотя бы одно из условий или студент не может пояснить код и суть алгоритма.

Лабораторная работа №3 «Асимметричные криптографические алгоритмы»

Задание: студентам предлагается написать программу шифрования и дешифрования алгоритма RSA или Эль-Гамаля (на выбор).

Обязательныеусловия:
1) Работа в парах, взаимодействие двух участников, передающих друг другу зашифрованные

сообщения по каналу связи, используя открытые ключи друг друга, сгенерированные по предварительной договорённости;
2) Перевод текста в двоичный код;
3) Генерация открытого и закрытого ключей; обмен ключами;
4) Шифрование;
5) Дешифрование;
6) Обмен сообщениями;
7) Перевод зашифрованного сообщения из двоичного кода в текст.

Критерии оценки:
Оценка «зачтено» выставляется студентам в случае предоставления и пояснений рабочего кода, в котором будут присутствовать составляющие, отвечающие всем прописанным условиям. Студенты отвечают на вопросы, связанные с работой алгоритма.
Оценка «незачтено» выставляется студенту, если в рабочем коде отсутствует хотя бы одно из условий или студент не может пояснить код и суть алгоритма.

Лабораторная работа №4 «Криптография на эллиптических кривых»

Задание: студентам предлагается написать программу шифрования и дешифрования с использованием эллиптических кривых.
Обязательные условия:
1) Работа в парах, взаимодействие двух участников, передающих друг другу зашифрованные сообщения по каналу связи, используя открытые ключи друг друга, сгенерированные по предварительной договорённости;
2) Перевод текста в двоичный код;
3) Генерация открытого и закрытого ключей; обмен ключами;
4) Шифрование;
5) Дешифрование;
6) Обмен сообщениями;
7) Перевод зашифрованного сообщения из двоичного кода в текст.

Критерии оценки:
Оценка «зачтено» выставляется студентам в случае предоставления и пояснений рабочего кода, в котором будут присутствовать составляющие, отвечающие всем прописанным условиям. Студенты отвечают на вопросы, связанные с работой алгоритма.
Оценка «незачтено» выставляется студенту, если в рабочем коде отсутствует хотя бы одно из условий или студент не может пояснить код и суть алгоритма.

Лабораторная работа №5 «Программная реализация модели TPM»
или
«Программная реализация хэширования с использованием нейросетей»

Задание: студентам предлагается реализовать модель TPM с указанными преподавателем параметрами сетей, исследовать процесс синхронизации параметров весовых коэффициентов персептронов двух сетей TPM. Или
разработать приложение для вычисления хэш-функций на основе нейросетевой технологии.
Обязательные условия:
1) Работа в мини-группах (3-4 человека);
2) Реализация модели TPM, использование нейропакета Java Neural Network Simulator (JavaNNS), или MATLAB Neural Network Toolbox;
3) Анализ процесса синхронизации параметров весовых коэффициентов персептронов двух сетей TPM.

В случае выполнения второй работы разработка приложения для вычисления хэш-функции, в котором по входным данным выдаётся сгенерированная нейросетью хэш-функция.

Критерии оценки:
Оценка «зачтено» выставляется студентам в случае предоставления и пояснений рабочего кода, в котором будут присутствовать составляющие, отвечающие всем прописанным условиям. Студенты отвечают на вопросы, связанные с работой алгоритма.
Оценка «незачтено» выставляется студенту, если в рабочем коде отсутствует хотя бы одно из условий или студент не может пояснить код и суть алгоритма.

Лабораторная работа №6 «Моделирование работы квантового протокола BB84 (B92)»

Задание: студентам предлагается реализовать модель квантовых протоколов (на выбор BB84 или B92). Обязательные условия:
1) Работа в парах;
2) Реализация алгоритма, использование Python и библиотек SymPy, NumPy, Qiskit;
3) Генерация и обмен ключами. Анализ возможных атак. Моделирование атаки.

Критерии оценки:
Оценка «зачтено» выставляется студентам в случае предоставления и пояснений рабочего кода, в котором будут присутствовать составляющие, отвечающие всем прописанным условиям. Студенты отвечают на вопросы, связанные с работой алгоритма.
Оценка «незачтено» выставляется студенту, если в рабочем коде отсутствует хотя бы одно из условий или студент не может пояснить код и суть алгоритма.

Самостоятельная работа №1 «Теория чисел»

Задание 1 (8 баллов). Вычислить $27^{253} \bmod 11$; $12^{2132} \bmod 7$.

Задание 2 (4 балла). Докажите, что $2222^{5555} + 5555^{2222}$ делится на 7.

Задание 3 (8 баллов). Составить два задания и выполнить:

а) выбрать основание $10<a<20$, простой модуль $23<p<43$ (p – простое число); показатель $n>100$ и вычислить $a^n \bmod p$, используя теорему Ферма;

б) выбрать основание $10<a<20$, модуль $23<n<43$ (n – составное); показатель $m>100$ и вычислить $a^m \bmod n$, используя теорему Эйлера.

Задание 4 (4 балла). Проверить, являются ли первообразными корнями числа 2,3 и 5 по модулю 11.

Критерии оценки:

Оценка «зачтено» выставляется, если студент набрал не менее 15 баллов.

Оценка «незачтено» выставляется, если студент набрал менее 15 баллов.

Самостоятельная работа №2 «Основы квантовой криптографии»

Задание 1 (12 баллов). Было приготовлено состояние $|0\rangle$. Вычислить вероятности каждого из исходов при измерении его наблюдаемой

а) $M_+ : M_+^0 = |0\rangle\langle 0|,\ M_+^1 = |1\rangle\langle 1|$.

б) $M_\times : M_\times^0 = \frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|);\ M_\times^1 = \frac{1}{2}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)$.

В каком состоянии окажется система после измерения в обоих случаях?

Задание 2 (8 баллов). Было приготовлено состояние $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Затем оно было измерено

а) наблюдаемой (а) из предыдущего задания;

б) наблюдаемой (б) из предыдущего задания.

Результат наблюдения неизвестен. В каком состоянии будет система после измерения?

Задание 3 (12 баллов). Ева атакует протокол B92 методом приёма-перепосыла. Параметр протокола – угол между сигнальными состояниями, - равен $\cos\alpha$. Параметр атаки – вероятность измерения каждого сигнала, – равен p. Найти величину ошибки на приёмной стороне, до которой ошибка Евы при такой атаке оказывается больше.

Критерии оценки:

Оценка «зачтено» выставляется, если студент набрал не менее 24 баллов.

Оценка «незачтено» выставляется, если студент набрал менее 24 баллов.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

– собеседование по вопросам к зачёту

Перечень вопросов к зачёту

1. Основные элементы криптографических систем.
2. Арифметика в классе вычетов: сложение, вычитание, умножение, деление.
3. Теорема Ферма. Привести примеры использования.
4. Функция Эйлера. Теорема Эйлера. Примеры.
5. Понятие о мультипликативном обратном. Расширенный алгоритм Евклида.
6. Дискретные логарифмы. Примеры вычислений.
7. Симметричные и асимметричные криптосистемы. Общая схема.
8. Общая схема генерирования открытого и закрытого ключей. Протокол Диффи-Хеллмана.
9. Блочные алгоритмы. Алгоритм DES. Общая структура. Анализ устойчивости.
10. Алгоритм RSA. Общая структура. Анализ устойчивости.
11. Электронная цифровая подпись. Пример формирования подписи с помощью RSA.
12. Алгоритм Эль-Гамаля. Общая структура. Анализ устойчивости.
13. Эллиптические кривые, применяемые в криптографии. Привести примеры поиска кривой.
14. Криптография на эллиптических кривых. Общая структура. Анализ устойчивости.
15. Хэш-функции. Применение. Уязвимости. Хэш-функции с ключами и без ключа. Алгоритм SHA-256.
16. Нейронные сети. Общие понятия. Технология нейронных сетей. Взаимодействие нейронных сетей.
17. Синхронизация дискретных весовых коэффициентов персептронов. Модели Хебба и анти-Хебба.
18. Архитектура нейронных сетей на основе целых действительных чисел.
19. Модель сети Кинцеля-Кантера для согласования тайной информации.
20. Анализ архитектуры сети на основе действительных чисел (TPM).
21. Процесс синхронизации архитектур TPM на основе моделей Хебба и антиХебба.

22. Безопасность процесса синхронизации архитектур TPM23.Хеш-функции, основанные на нейронных сетях. Сети QNNHF (Quaternion
Neural Network Hash Function).
24. Анализ безопасности хеш-функции, основанной на архитектуре нейронной сети.
25. Основные понятия и определения в квантовой криптографии.
26. Матричный и дираковский формализм в квантовых вычислениях.
27. Факторизация в шифровании RSA. Взлом шифра с использованием алгоритма Шора.
28. Понятие о квантовой запутанности. Квантовая телепортация. Теорема о запрете клонирования.
29. Связь по квантовым каналам с шумом. Коррекция ошибок.
30. Квантовый протокол распределения ключей BB84.
31. Квантовый протокол распределения ключей B92.
32. Квантовый протокол распределения ключей SARG04.
33. Квантовый протокол распределения ключей 4+2.
34. PNS-атака.

Для оценивания результатов обучения на зачёте используются оценки: «зачтено» и «не зачтено».

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Ответа обучающегося соответствует хотя бы половине из перечисленных критериев. Сформированные знания основных понятий, определений и теорем, изучаемых в курсе, возможно с затруднениями при воспроизведении.	Пороговый уровень	Зачтено
Ответ на контрольно-измерительный материал не соответствует более чем половине из перечисленных показателей. Обучающийся демонстрирует отрывочные знания (либо их отсутствие) основных понятий, определений и теорем, используемых в курсе.	–	Не зачтено