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

УТВЕРЖДАЮ

Заведующий кафедрой
электроники
Усков Г.К.

20.05.2025 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.26 Защита информации

1. Код и наименование направления подготовки/специальности:

11.03.02 Инфокоммуникационные технологии и системы связи

2. Профиль подготовки/специализация:

Инфокоммуникационные технологии и системы связи

3. Квалификация (степень) выпускника: *бакалавр*

4. Форма обучения: *очная*

5. Кафедра, отвечающая за реализацию дисциплины: *электроники*

6. Составители программы: Овчинникова Татьяна Михайловна, к.ф.-м.н., доцент

7. Рекомендована: НМС физического факультета 20.05.2025, № протокола: 5

8. Учебный год: *2027/2028* **Семестр(ы):** 7

9. Цели и задачи учебной дисциплины

Приобретение теоретических и практических знаний о современной криптографии, необходимых для разработки программных систем защиты информации.

10. Место учебной дисциплины в структуре ООП

Для освоения теоретического материала курса необходимы знания основ информатики и дискретной теории вероятностей. Лабораторные работы дополнительно требуют навыков программирования на языках C, C++ или Python, уверенной работы с командной строкой Linux или иной операционной системы.

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

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-3	Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ОПК-3.1	Выбирает и использует необходимые информационно-коммуникационные технологии для поиска, хранения, обработки, анализа и представления информации	Обеспечивает защиту пользовательских данных для задач профессиональной деятельности
		ОПК-3.2	Осуществляет поиск, сбор, хранение, обработку, представление информации в требуемом формате при решении задач профессиональной деятельности	Владеет основными принципами защиты информации для решения задач профессиональной деятельности
		ОПК-3.4	Знает и соблюдает основные требования информационной безопасности	Использует современные специальные программные продукты для защиты информации в рамках задач профессиональной деятельности
ОПК-4	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-4.1	Информационные технологии и документационное обеспечение профессиональной деятельности	Опирается на основные нормативные акты и законы в области защиты информации
		ОПК-4.2	Понимает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы реализации таких процессов и методов	Разрабатывает документацию по использованию защищенных данных

		ОПК-4.3	Выбирает и применяет современные информационные технологии и программные средства для решения задач профессиональной деятельности	Проектирует протоколы для передачи информации в зашифрованном виде Документирует процесс разработки программного обеспечения с точки зрения защиты данных Выявляет и описывает возможные проблемы с безопасностью программных продуктов

12. Объем дисциплины в зачетных единицах/час: 4 / 144**.**
Форма промежуточной аттестации: экзамен**.**

13. Виды учебной работы

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		7		
Аудиторные занятия	68	68		
в том числе: лекции	34	34		
практические				
лабораторные	34	34		
Самостоятельная работа	40	40		
Форма промежуточной аттестации (зачет – 0 час. / экзамен – 36 час.)	36	36		
Итого:	144	144		

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1. Лекции		
1.1	Криптография в истории и культуре	Цели и задачи криптографии. Классификации шифросистем: симметричные и асимметричные, с закрытым и открытым ключом. Краткая история шифров и криптографии. Частотный анализ как способ взлома классических шифров. Шифры в литературе и современной культуре.
1.2	Потоковые шифры	Одноразовый блокнот и теоретико-информационная криптостойкость, шифр Вернама. Генераторы псевдослучайной чисел (ГПСЧ). Статистические тесты на ГПСЧ и криптостойкость ГПСЧ. Примеры ГПСЧ, непригодных для криптосистем (линейный конгруэнтный генератор, регистр сдвига с линейной обратной связью). Примеры ГПСЧ и криптосистем с известными уязвимостями (RC4, CSS) Атака «встречи посередина» на примере CSS. Семантическая криптостойкость.
1.3	Блочные шифры	Понятия псевдослучайной функции (ПСФ) и псевдослучайной перестановки (ПСП) как основы блочных шифров. Криптостойкость ПСФ и ПСП. Построение потокового шифра на основе блочного. Краткая история стандартизации шифров DES и AES. Сеть Фейстеля и её свойства. Теорема о стойкости трёхзвенной сети Фейстеля. Построение блочного шифра на основе потокового. Внутреннее устройство шифров DES и AES. Известные атаки на DES и AES. Усовершенствованные версии DES: шифры 3DES и DESX. Понятия о линейном и дифференциальном криптоанализе блочных шифров, а также атаках по сторонним каналам. О роли компиляторных оптимиизаций в уязвимости к атакам по времени.
1.4	Режимы работы блочных шифров	Стойкость блочных шифров для длинных сообщений. Режимы работы «электронной кодовой книги» (ECB), с детерминированным счётчиком CTR и обратной связью по шифротексту (CBC). Рандомизированные шифры, инициализирующие вектора (IV) и однократно используемые

		числа (nonce) как способы предотвращения атак на основе подобранного открытого теста. Паддинг последнего блока сообщения. Пределы безопасного использования шифров в режимах CTR и CBC.
1.5	Аутентификация сообщений	Контрольные суммы, коды аутентификации (MAC) и хеш-функции и их отличия друг от друга. Криптографическая стойкость MAC. Построение MAC на основе ПСФ. Распространённые конструкции MAC на основе ПСФ: ECBC MAC, NMAC, PMAC. Паддинг последнего блока как средство противодействия атакам удлинения сообщения. Определение хеш-функций. Коллизии хеш-функций и их стойкость к коллизиям. Парадокс дней рождения и поиск хеш-коллизии полным перебором. Структура Меркла-Дамгора как способ построения хеш-функций длинных сообщений. Теорема о коллизиях меркл-дамгоровых хеш-функций. Структуры Дэвиса-Мейера и Миягути-Пренеля как одни из вариантов построения односторонней функции сжатия для использования в структуре Меркла-Дамгора. HMAC как способ построение MAC на основе хеш-функций. Краткий обзор хеш-функций, используемых в современных шифросистемах. О стойкости HMAC-SH1 и HMAC-MD5. О допустимости использования усечённых хеш-функций семейства SHA как префиксного MAC.
1.6	Аутентифицирующее шифрование	Понятие целостности шифротекста и атаки на основе подобранного шифротекста (CCA). Шифры с аутентификацией (AE-шифры) как средство противодействия CCA. Примеры ситуаций, в которых необходимо использование CCA-стойких шифров. Способы построение AE-шифра при помощи симметричного шифра и MAC. Ассоциированные данные AE-шифротекста (AEAD). Использование AE-шифров в TLS 1.2.
1.7	Типовые задачи защиты информации	Шифрование отдельных файлов и каталогов. Полнодисковое шифрование. Контроль прав пользователей в многопользовательских операционных системах. Идентификация, авторизация и аутентификация пользователей в компьютерных сетях и онлайн-сервисах. Защита сетевых протоколов при помощи TLS. Обзор технологии для создания VPN-сетей. Инфраструктура открытых ключей (PKI). Физические средства защиты информации. Юридические средства защиты информации: базовые сведения из области авторского и патентного права, режим коммерческой тайны. Законы о криптографии в разных странах. Отечественные криптографические алгоритмы.
2. Практические занятия		
3. Лабораторные работы		
3.1	Криптография в истории и культуре	Программная реализация шифров Цезаря и Виженера. Взлом шифров простой замены при помощи частотного анализа.
3.2	Потоковые шифры	Исследование статистических свойств линейного конгруэнтного генератора. Использование батареи статистических тестов dieharder для тестирования ГПСЧ. Шифрование файлов при помощи консольной команды openssl. Использование библиотеки Crypto++.
3.3	Блочные шифры	Ускорение вычисления AES при помощи инструкций aesenc/aesenclast.
3.4	Режимы работы блочных шифров	Реализация блочного шифрования в режимах AES-128-CBC и AES-128-CTR.
3.5	Аутентификация сообщений	Использование инструментов командной строки Linux для вычисления хеш-функций файлов. Использование модуля hashlib стандартной библиотеки Python для вычисления хеш-функций. Поиск коллизии хеш-функции MD5 методом полного перебора.
3.6	Аутентифицирующее шифрование	Аутентифицирующее шифрование сообщения при помощи Chacha20+Poly1305.
3.8	Типовые задачи защиты информации	Настройка полнодискового шифрования при помощи Veracrypt и cryptsetup/LUKS. Управления правами пользователей при помощи консольных команд Linux и групповых политик Windows. Настройка VPN-сети при помощи OpenVPN и Wireguard.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1.	Криптография в	3	0	4	3	10

	истории и культуре					
2.	Потоковые шифры	6	0	6	6	18
3.	Блочные шифры	6	0	6	6	18
4.	Режимы работы блочных шифров	4	0	3	5	12
5.	Аутентификация сообщений	6	0	4	6	16
6.	Аутентифицирующее шифрование	3	0	3	6	12
7.	Типовые задачи защиты информации	6	0	8	8	22
	Итого:	34	0	34	40	108

14. Методические указания для обучающихся по освоению дисциплины

Для успешного освоения дисциплины в первую очередь необходима регулярная и планомерная работа на лекциях и практических занятиях. Студентам рекомендуется вести собственный конспект лекций, пересматривать и дополнять его при подготовке к очередной лекции. Следует обратить особое внимание на многочисленные определения криптографической стойкости различных примитивов и то, как они связаны между собой. Также рекомендуется запоминать англоязычные аббревиатуры и термины несмотря на то, что в курсе приводятся их русскоязычные эквиваленты и переводы. Приветствуется использование диаграмм, ментальных карт и иных способов систематизации материала.

Курс предполагает предполагает наличие у студента уверенных знаний по предыдущим дисциплинам, поэтому в случае возникновения затруднений рекомендуется в первую очередь устранить имеющиеся пробелы в знаниях, а затем, если это не помогло, обратиться к основным и дополнительным источникам. Студентам, знающим английский язык, настоятельно рекомендуется ознакомиться со стенфордским курсом прикладной криптографии Дэна Бонэ, доступном на образовательном портале «Курсера» (пункт 9 перечня литературы настоящей рабочей программы), который послужил основой для разработки данного курса, наряду с книгами Смарта и Шнайера.

Самостоятельная работа по курсу предполагает в первую очередь работу с текстами: учебниками, справочниками, дополнительной литературой. Кроме литературы из основного списка рекомендуется самостоятельно использовать дополнительную, а также самостоятельно искать релевантные материалы по изучаемым темам в интернете, книгах и журналах.

При использовании дистанционных образовательных технологий и электронного обучения студентам следует выполнять все указания преподавателей, вовремя подключаться к онлайн-занятиям, ответственно подходить к выполнению заданий для самостоятельной работы.

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

а) основная литература:

№ п/п	Источник
1.	Смарт, Н. Криптография / Н. Смарт ; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. — М. : Техносфера, 2006. — 525 с. : ил. — (Мир программирования).
2.	Шнайер, Б. Прикладная криптография: протоколы, алгоритмы, исходные тексты на языке Си : пер. с англ. / Б. Шнайер. — М.: Триумф, 2003. — 815 с. : ил. — (Знания и опыт экспертов.) — ISBN 5-89392-055-4.

б) дополнительная литература:

№ п/п	Источник
3.	Аграновский, А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. — М.: СОЛОН-Пресс, 2002. — 254. — (Аспекты защиты.) — ISBN 5-98003-002-6.
4.	Панасенко, С. П. Алгоритмы шифрования. Специальный справочник. — СПб.: БХВ-Петербург, 2009.
5.	Сингх, С. Книга шифров. Тайная история шифров и их расшифровки / С. Сингх. — М.:

	Астрель, АСТ, 2007.
6.	Словарь криптографических терминов. / Под ред. Б. А. Погорелова и В. Н. Сачкова. — М.: МЦНМО, 2006. — 94 с. — ISBN 5-94057-257-X.
7.	Доронина, А. В. Особенности перевода криптографических текстов с английского языка на немецкий и русский языки на примере рассказа Артура Конан Дойла «Пляшущие человечки» / А. В. Доронина, Е. В. Белянина, Н. А. Кандакова, Л. Ю. Курчакова. // Юный ученый. — 2020. — № 1 (31). — С. 14-19. — URL: https://moluch.ru/young/archive/31/1810.
8.	Instructions 'Testing RNGs with Diehard'. — URL: https://webspace.science.uu.nl/~sleij101/Opgaven/LabClass/site/asm_diehard.php

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

№ п/п	Ресурс
9.	Cryptography I: Coursera. — URL: https://www.coursera.org/learn/crypto
10.	Cryptography II: Coursera. — URL: https://www.coursera.org/learn/crypto2
11.	A Graduate Course in Applied Cryptography. / D. Boneh, V. Shoup. — URL: https://toc.cryptobook.us
12.	Введение в современную криптографию. Открытое образование. — URL: https://openedu.ru/course/mephi/mephi_011_crypto
13.	Cryptography: Boolean functions and related problems. — URL: https://www.coursera.org/learn/cryptography-boolean-functions

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)

№ п/п	Источник
1.	Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа : учебное пособие для студентов вузов, обучающихся по специальностям 090103 «Организация и технология защиты информации», 090104 «Комплексная защита объектов информатизации» / Л. К. Бабенко, Е. А. Ищукова. — М.: Гелиос АРВ, 2006.
2.	Мельников, В. Ю. Исследование методов защиты операционных систем и данных : Электронное учебное издание / В. Ю. Мельников, Е. К. Пугачев. — МГТУ имени Н. Э. Баумана, факультет «Информатика и системы управления», кафедра «Компьютерные системы и сети». — 2017.

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

При реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологии на базе образовательного портала «Электронный университет ВГУ» по адресу https://edu.vsu.ru, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины:

Мультимедийная аудитория (ауд. 401): специализированная мебель, компьютеры, проектор, экран, комплекс для проведения лекций, семинаров и презентаций

Microsoft Windows, Linux, Open Office, браузер Google Chrome

Помещение для самостоятельной работы обучающихся (ауд. 423): специализированная мебель, компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ВГУ
Microsoft Windows, Linux, OpenOffice, браузер Google Chrome
Помещение для самостоятельной работы обучающихся (ауд. 410): специализированная мебель, компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ВГУ

Microsoft Windows, Linux, OpenOffice, браузер Google Chrome, MatLab, NI LabView, Python
Компьютерный класс (ауд. 412) специализированная мебель, принтер, сканер, компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ВГУ
WinPro, Linux Mint, Open Office, AWR Studio, Anaconda, MicroCap Evaluation, Maxima, Octave, CoID, Cube, Lazarus
Помещение для самостоятельной работы обучающихся (ауд. 407): специализированная мебель, компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ВГУ
WinPro, OfficeSTD, Интернет-браузер Google Chrome Mozilla Firefox, MatLab, NI LabView, Python

19. Фонд оценочных средств

19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС (средства оценивания)
ОПК-3 Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ОПК-3.1 Выбирает и использует необходимые информационно-коммуникационные технологии для поиска, хранения, обработки, анализа и представления информации	1.2. Потоковые шифры 1.3. Блочные шифры 1.4. Режимы работы блочных шифров 1.5. Аутентификация сообщений 1.6. Аутентифицирующее шифрование 1.7. Типовые задачи защиты информации	Устный опрос
	ОПК-3.2 Осуществляет поиск, сбор, хранение, обработку, представление информации в требуемом формате при решении задач профессиональной деятельности	3.2. Потоковые шифры 3.3. Блочные шифры 3.4. Режимы работы блочных шифров 3.5. Аутентификация сообщений 3.6. Аутентифицирующее шифрование 3.7. Типовые задачи защиты информации	Практические задания 1–19
	ОПК-3.4 Знает и соблюдает основные требования информационной безопасности	1.1. Криптография в истории и культуре 1.2. Потоковые шифры 1.3. Блочные шифры 1.4. Режимы работы блочных шифров 1.5. Аутентификация сообщений 1.6. Аутентифицирующее шифрование 1.7. Типовые задачи защиты информации	Устный опрос
ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения	ОПК-4.1 Ориентируется в современных информационных технологиях	1.4. Режимы работы блочных шифров 1.5. Аутентификация сообщений 1.6. Аутентифицирующее шифрование	Устный опрос
	ОПК-4.2 Понимает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и	3.2. Потоковые шифры 3.3. Блочные шифры 3.4. Режимы работы блочных шифров	Практические задания 1–19

задач профессиональной деятельности	способы реализации таких процессов и методов	3.5. Аутентификация сообщений 3.6. Аутентифицирующее шифрование	
	ОПК-4.3 Выбирает и применяет современные информационные технологии и программные средства для решения задач профессиональной деятельности	3.4. Режимы работы блочных шифров 3.6. Аутентифицирующее шифрование 1.1. Криптография в истории и культуре 1.3. Блочные шифры 1.7. Типовые задачи защиты информации	Практические задания 1–19
Промежуточная аттестация			КИМ

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом информационной безопасности и криптографии, способен теоретически обосновывать стойкость криптографических систем, может обосновать ответ примерами, фактами, ссылками на научные исследования, умеет применять теоретические знания для решения практических задач, готов к практическому решению задач дисциплины с использованием современных языков программирования и операционных систем.	Повышенный уровень	Отлично
Обучающийся владеет понятийным аппаратом дисциплины, знает ограничения и область применимости распространённых криптосистем, хотя и без теоретического обоснования, но в целом готов к применению полученных знаний на практике.	Базовый уровень	Хорошо
Обучающийся частично владеет теоретическими основами дисциплины, может правильно выбрать подходящий для решения задачи криптографический алгоритм, хотя и без детальных знаний о внутреннем устройстве и условиях применимости.	Пороговый уровень	Удовле-творительно
Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки.	–	Неудовле-творительно

19.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.1 Перечень вопросов к экзамену:

1. Цели и задачи криптографии. Классификации шифросистем.
2. Краткая история шифров и криптографии. Шифры в литературе и современной культуре.
3. Одноразовый блокнот и теоретико-информационная криптостойкость, шифр Вернама.
4. Генераторы псевдослучайной чисел (ГПСЧ). Статистические тесты на ГПСЧ и криптостойкость ГПСЧ. Примеры ГПСЧ, пригодных и непригодных для криптосистем.
5. Реализация атака «встречи посередина» на примере CSS.
6. Семантическая криптостойкость.
7. Понятия псевдослучайной функции (ПСФ) и псевдослучайной перестановки (ПСФ). Криптостойкость ПСФ и ПСП.
8. Построение потокового шифра на основе блочного.

9. Краткая история стандартизации шифров DES и AES.
10. Сеть Фейстеля и её свойства. Теорема о стойкости трёхзвенной сети Фейстеля.
11. Построение блочного шифра на основе потокового.
12. Внутреннее устройство шифров DES и AES. Известные атаки на DES и AES.
13. Усовершенствованные версии DES: шифры 3DES и DESX.
14. Понятия о линейном и дифференциальном криптоанализе блочных шифров
15. Атаки по сторонним каналам. Деструктивные компиляторные оптимизации.
16. Стойкость блочных шифров для длинных сообщений.
17. Режим работы блочного шифра: «электронная кодовая книга» (ECB).
18. Режим работы блочного шифра с детерминированным счётчиком CTR.
19. Режим работы блочного шифра с обратной связью по шифротексту (CBC).
20. Рандомизированные шифры как способ предотвращения CPA-атак.
21. Инициализирующие вектора (IV) и однократно используемые числа (nonce) как способы предотвращения CPA-атак.
22. Паддинг последнего блока сообщения при блочном шифровании.
23. Пределы безопасного использования шифров в режимах CTR и CBC.
24. Контрольные суммы, коды аутентификации (MAC) и хеш-функции и их отличия друг от друга.
25. Криптографическая стойкость MAC.
26. Построение MAC на основе ПСФ.
27. Распространённые конструкции MAC на основе ПСФ: ECBC MAC.
28. Распространённые конструкции MAC на основе ПСФ: NMAC.
29. Распространённые конструкции MAC на основе ПСФ: PMAC.
30. Паддинг последнего блока как средство противодействия атакам удлинения сообщения.
31. Определение хеш-функций. Коллизии хеш-функций и их стойкость к коллизиям.
32. Парадокс дней рождения и поиск хеш-коллизии полным перебором.
33. Структура Меркла-Дамгора как способ построения хеш-функций длинных сообщений.
34. Теорема о коллизиях меркл-дамгоровых хеш-функций.
35. Структуры Дэвиса-Мейера и Миягути-Пренеля для построения односторонней функции сжатия для использования в структуре Меркла-Дамгора.
36. HMAC как способ построение MAC на основе хеш-функций.
37. Краткий обзор хеш-функций, используемых в современных шифросистемах.
38. Понятие целостности шифротекста и атаки на основе подобранного шифротекста (CCA).
39. Шифры с аутентификацией (AE-шифры) как средство противодействия CCA.
40. Примеры ситуаций, в которых необходимо использование CCA-стойких шифров.
41. Способы построение AE-шифра при помощи симметричного шифра и MAC.
42. Ассоциированные данные AE-шифротекста (AEAD). Использование AE-шифров в TLS 1.2.
43. Шифрование отдельных файлов и каталогов.
44. Полнодисковое шифрование.
45. Контроль прав пользователей в многопользовательских операционных системах.
46. Идентификация, авторизация и аутентификация пользователей в компьютерных сетях и онлайн-сервисах.
47. Защита сетевых протоколов при помощи TLS.
48. Технологии для создания VPN-сетей.
49. Инфраструктура открытых ключей (PKI).
50. Физические средства защиты информации.
51. Юридические средства защиты информации: авторское и патентное право.
52. Юридические средства защиты информации: режим коммерческой тайны.
53. Законы о криптографии в разных странах.
54. Отечественные криптографические алгоритмы.

19.3.2 Перечень практических заданий

1. Программная реализация шифра Цезаря.
2. Программная реализация шифра Виженера.
3. Взлом шифров простой замены при помощи частотного анализа.
4. Исследование статистических свойств линейного конгруэнтного генератора.
5. Использование батареи статистических тестов dieharder для тестирования ГПСЧ.
6. Шифрование файлов при помощи консольной команды openssl.
7. Использование библиотеки Crypto++.
8. Ускорение вычисления AES при помощи инструкций aesenc/aesenclast.
9. Реализация блочного шифрования в режимах AES-128-CBC и AES-128-CTR.
10. Использование инструментов командной строки Linux для вычисления хеш-функций файлов.

11. Использование модуля hashlib стандартной библиотеки Python для вычисления хеш-функций.
12. Поиск коллизии хеш-функции MD5 методом полного перебора.
13. Аутентифицирующее шифрование сообщения при помощи Chacha20+Poly1305.
14. Настройка полнодискового шифрования при помощи Veracrypt.
15. Настройка полнодискового шифрования при помощи cryptsetup/LUKS.
16. Управления правами пользователей при помощи консольных команд Linux.
17. Управление правами пользователей при помощи групповых политик Windows.
18. Настройка VPN-сети при помощи OpenVPN.
19. Настройка VPN-сети при помощи Wireguard.

19.3.4 Тестовые задания

19.3.4 Перечень заданий для контрольных работ

19.3.5 Темы курсовых работ

19.3.6 Темы рефератов

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

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 форме тестирования. Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практические задания, позволяющие оценить степень сформированности умений и навыков.

При оценивании используются качественные шкалы оценок. Критерии оценивания приведены выше.