

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Анатольевна

Должность: и.о. декана факультета математики и компьютерных наук имени

профессора Н.И. Червякова

Дата подписания: 17.06.2026 15:38:47

Уникальный программный ключ:

bd39d4208aa94cf4422feb787c81619d42de79a7

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего
образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

И.о. декана факультета математики
и компьютерных наук имени
профессора Н.И. Червякова
Т.А. Грובה
Ф.И.О.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Методы и средства криптографической защиты информации
название дисциплины (модуля)

Направление подготовки
Направленность (профиль)

10.03.01 «Информационная безопасность»
Организация и технологии защиты
информации (по отрасли или в сфере
профессиональной деятельности)

Год начала обучения

2026

Форма обучения

очная

Реализуется в семестре

5,6

Разработано

Профессор кафедры
информационной безопасности
автоматизированных систем
(должность разработчика)

И.А. Калмыков
Ф.И.О.

Ставрополь 2026 г.

1. Цель и задачи освоения дисциплины (модуля)

Целью освоения дисциплины «Методы и средства криптографической защиты информации» является формирование у будущего бакалавра 10.03.01 «Информационная безопасность фундаментальных знаний основных положений теории криптографической защиты информации, принципов построения симметричных и асимметричных шифров, схем цифровой подписи и функции хеширования, инфраструктуры систем управления ключами, оценки криптостойкости, имитостойкости и помехоустойчивости шифров,, криптографических протоколов,

Задачи дисциплины:

- - изучить математические основы криптографических методов защиты информации;
- - изучить основные алгоритмы симметричного и асимметричного шифрования данных;
- - изучить основы организации структуры криптосистем.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Методы и средства криптографической защиты информации» относится к дисциплинам обязательной части.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИД-2 ОПК-6 Эффективно применяет знания теории и методики курса при раскрытии компьютерных преступлений, при работе с конфиденциальной информацией и государственной тайной, при работе с организационно-правовым обеспечением, при работе с ЭП, при защите авторского и международного права, при проведении экспертизы преступлений в сфере компьютерной информации; применять нормативно-правовые акты при защите информации; оценивать состояние организационной защиты информации на объекте.	-осуществляет организацию защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; -выбирает мероприятия защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; -участвует в организации защиты информации ограниченного доступа в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной

		службы по техническому и экспортному контролю;
ОПК-9 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ИД-1 ОПК-9 Понимает базовые принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности.	- оперирует знаниями средств криптографической и технической защиты информации по техническим каналам; - оценивает средства криптографической и технической защиты информации по техническим каналам; - анализирует средства криптографической и технической защиты информации по техническим каналам;
	ИД-2 ОПК-9 Использует средства криптографической и технической защиты информации для решения задач профессиональной деятельности.	- осуществляет выбор средств криптографической и технической защиты информации для решения задач профессиональной деятельности; - выделяет средства криптографической и технической защиты информации для решения задач профессиональной деятельности; - использует средства криптографической и технической защиты информации для решения задач профессиональной деятельности.
	ИД-3 ОПК-9 Выбирает оптимальный вариант использования навыков и методик применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности	- демонстрирует знания устройства и принципов работы криптографических средств защиты информации, применяемых в компьютерных системах и сетях; - устанавливает, настраивает и интегрирует криптографические средства защиты информации в компьютерных системах и сетях

4. Объем учебной дисциплины (модуля) и формы контроля *

Объем занятий: всего: 8 з.е. 288 акад.ч.	ОФО, в акад. часах
Контактная работа:	
Лекции/из них практическая подготовка	68
Лабораторных работ/из них практическая подготовка	50
Практических занятий/из них практическая подготовка	50
Самостоятельная работа	84
Формы контроля	

Экзамен	36
Зачет с оценкой	+

* Дисциплина (модуль) предусматривает применение электронного обучения, дистанционных образовательных технологий.

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием количества часов и видов занятий

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	очная форма			
			Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	
1	Основные понятия криптографии	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2			2
1	Модели шифров	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9			2	2
2	Классификация методов криптографической защиты информации	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9			2	2
3	Простейшие шифры подстановки и их свойства	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2			2

3	Алгоритм шифрования таблицей Виженера	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9			2	2
4	Шифры перестановки их свойства	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2		2	2
5	Американский стандарт шифрования DES	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9				2
5	Шифрование алгоритмом S-DES	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2	2		2
6	Практическое применение американского стандарта	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9				2
6	Расшифрование алгоритмом S-DES	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2	2		2
7	Блочные шифры	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9				2
7	Блочный шифр. Ключевая система	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2	2		2

8	Стандарт криптографической защиты AES	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9				2
8	Шифрование алгоритмом S-AES	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2	2		2
9	Принципы работы алгоритма шифрования AES	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9				2
9	Расшифрованное алгоритмом S-AES	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2	2		2
10	Стандарт шифрования данных Магма	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9				2
10	Шифрование и расшифрование алгоритмом S-Магма	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2	2		2
11	Отечественный стандарт шифрования Кузнечик	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9				2
11	Шифрование на основе генератора Фибоначчи	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2	2		2

12	Синхронные поточные системы шифрования	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9				2
12	Расшифрование на основе генератора Фибоначчи	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2	2		2
13	Самосинхронизирующиеся поточные системы шифрования	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9				2
13	Шифрование на основе генераторов много тактовых кодовых фильтров	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2	2		2
14	Программная реализация шифров	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9				2
14	Расшифрование на основе генераторов много тактовых кодовых фильтров	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2		2	2
15	Режимы использования блочных шифров	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9				2
15	Шифрование с помощью самосинхронизирующихся поточных шифров	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2		2	2

16	Режимы шифрования с обратной связью	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9				2
16	Расшифрование с помощью самосинхронизирующихся поточных шифров	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2		2	2
17	Надежность шифров	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9				2
17	Основы построения поточного шифра S-A5	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2		2	2
18	Стойкость шифров	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9				2
18	Расшифрование с помощью поточного шифра S-A5	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2		2	2
	ИТОГО за 5 семестр		36	18	18	72
19	Арифметика целых чисел	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2	2	2	4
20	Модульная арифметика	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2	2	2	4

21	Алгебраические структуры	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2	2	2	4
22	Расширение полей Галуа GF(2 ^m)	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2	2	2	
23	Математические модели расширенных полей Галуа	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2	2	2	
24	Асимметричные системы шифрования	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2			
24	Алгоритм шифрования без передачи ключа	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9		2	2	
25	Практическая реализация асимметричных систем шифрования	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2			
25	Алгоритм шифрования Эль-Гамала	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9		2	2	
26	Электронная цифровая подпись	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2			

26	Построение электронной цифровой подписи RSA	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9		2	2	
27	Практическая реализация электронных цифровых подписей	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2			
27	Построение электронной цифровой подписи Эль-Гамала	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9		2	2	
28	Управление ключами	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2			
28	Ключевой обмен на основе алгоритма Диффи-Хеллмана	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9		2	2	
29	Протоколы распределения ключей	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2			
29	Модифицированный метод ключевого обмена на основе алгоритма Диффи-Хеллмана	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9		2	2	
30	Криптографические схемы разделения секрета	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2			

30	Схема разделения секрета Шамира	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9		2	2	
31	Протоколы аутентификации	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2			
31	Протокол аутентификации Шнорра	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9		2	2	
32	Протоколы аутентификации с нулевым разглашением знаний и их применение	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2			
32	Протокол аутентификации для систем электронных платежей	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9		2	2	
33	Криптографические хеш-функции	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2			
33	Отечественная криптографическая хеш-функция	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9		2	2	
34	Скрытый канал	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9	2			

34	Скрытый канал Эль-Гамалы	ИД-2 ОПК-6 ИД-1 ОПК-9 ИД-2 ОПК-9 ИД-3 ОПК-9		2	2	
	ИТОГО за 6 семестр		32.00	32.00	32.00	12.00
	ИТОГО		68	60	60	84.00

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств (ФОС) по дисциплине (модулю) базируется на перечне осваиваемых компетенций с указанием индикаторов. ФОС обеспечивает объективный контроль достижения запланированных результатов обучения. ФОС включает в себя:

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций (включаются в методические указания по тем видам работ, которые предусмотрены учебным планом и предусматривают оценку сформированности компетенций);
- типовые оценочные средства, необходимые для оценки знаний, умений и уровня сформированности компетенций.

ФОС является приложением к данной программе дисциплины (модуля).

7. Методические указания для обучающихся по освоению дисциплины

Приступая к работе, каждый студент должен принимать во внимание следующие положения.

Дисциплина (модуль) построена по тематическому принципу, каждая тема представляет собой логически заверченный раздел.

Лекционный материал посвящен рассмотрению ключевых, базовых положений курсов и разъяснению учебных заданий, выносимых на самостоятельную работу студентов.

Практические занятия проводятся с целью закрепления усвоенной информации, приобретения навыков ее применения при решении практических задач в соответствующей предметной области.

Лабораторные работы направлены на приобретение опыта практической работы в соответствующей предметной области.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к практическим и лабораторным занятиям, а также выполнения всех видов самостоятельной работы.

Для успешного освоения дисциплины, необходимо выполнить все виды самостоятельной работы, используя рекомендуемые источники информации.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

8.1.1. Перечень основной литературы:

1. Бутакова, Н. Г. Криптографические методы и средства защиты информации : учебное пособие / Н. Г. Бутакова, Н. В. Федоров. — Санкт-Петербург : Интермедия, 2020. — 380 с. — ISBN 978-5-4383-0210-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/161347>

2. Костин, В. Н. Методы и средства защиты компьютерной информации: Криптографические методы для защиты информации : учебное пособие / В. Н. Костин. — Москва : МИСИС, 2018. — 40 с. — ISBN 978-5-90695-334-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/115270>

8.1.2. Перечень дополнительной литературы:

1. Применение искусственных нейронных сетей и системы остаточных классов в криптографии / [авт. кол.: Червяков Н.И., Евдокимов А.А., и др.]. - Москва : ФИЗМАТЛИТ, 2012. - 280 с. : ил. - Прил.: с. 269-279. - Библиогр.: с. 269-279 (191 назв.) и в конце гл. - ISBN 978-5-9221-1386-1.

8.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине (модулю)

1. Криптографические методы защиты информации : Лабораторный практикум : Направление подготовки 10.05.03 (090303.65) - Информационная безопасность автоматизированных систем / сост. И. А. Калмыков, Д. О. Науменко, Т. А. Гиш. - Ставрополь : СКФУ, 2015. - 109 с.

2. Я. Рябко, А. Н. Фионов. - М. : Горячая линия - Телеком, 2014. - 229 с. : ил., табл. - Гриф: Рек. УМО. - Библиогр.: с. 218-221. - Предм. указ.: с. 222-226. - ISBN 978-5-9912-0286-2.

3. Методические рекомендации к самостоятельной работе по дисциплине «Теория информации». Ставрополь : СКФУ, 2021

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Сайт ФСТЭК России // Федеральная служба по техническому и экспортному контролю: [сайт]. — URL: <https://fstec.ru/> (дата обращения: 04.02.2023).

2. Сайт Роскомнадзора // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: [сайт]. — URL: <https://rkn.gov.ru/> (дата обращения: 04.02.2023).

3. Сайт ФСБ России // Федеральная служба безопасности Российской Федерации: [сайт]. — URL: <http://fsb.ru/> (дата обращения: 04.02.2023).

4. «Лань». Электронно-библиотечная система // Консорциум сетевых электронных библиотек ЭБС «Лань»: [сайт]. — URL: <https://e.lanbook.com/> (дата обращения: 04.02.2023).

5. Библиоклуб.РУ // ЭБС «Университетская библиотека ОНЛАЙН»: [сайт]. — URL: <https://www.biblioclub.ru/> (дата обращения: 04.02.2023).

6. http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=5170 Малюк А.А., Теория защиты информации, издательство "Горячая линия-Телеком", 2012"

7. 2. <http://siblec.ru/index.php?dn=html&way=> - банк лекций

8. 3. http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=4427 Панин.В.В., Основы теории информации, издательство "Бином. Лаборатория знаний", 2012

9. Поисковые интернет-системы Яндекс, Rambler, Google и др.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

При чтении лекций используется компьютерная техника, демонстрация презентационных мультимедийных материалов, программное обеспечение для проведения веб-конференции.

При проведении практических занятий и лабораторных работ используются информационно-справочные системы, интерактивная доска для совместной работы команд и сервис для совместной работы.

При реализации дисциплины с применением электронного обучения и дистанционных образовательных технологий материал может размещаться в системе электронного обучения.

Для обеспечения удаленного доступа, в том числе в случае применения электронного обучения, дистанционных образовательных технологий, используется программное обеспечение для проведения веб-конференции, виртуализации рабочих столов и система электронного обучения.

Информационные справочные системы

Информационно-справочные и информационно-правовые системы, используемые при изучении дисциплины:

1. Государственный реестр сертифицированных средств защиты информации // Федеральная служба по техническому и экспортному контролю: [сайт]. — URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153->

sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00

2. Реестр аккредитованных ФСТЭК России органов по сертификации и испытательных лабораторий // Федеральная служба по техническому и экспортному контролю: [сайт]. — URL: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/588-perechen-ispytatelnykh-laboratorij-n-ross-ru-0001-01bi00>

3. Реестр операторов, осуществляющих обработку персональных данных // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: [сайт]. — URL: <https://pd.rkn.gov.ru/operators-registry/operators-list/>

4. Банк данных угроз безопасности информации. // Федеральная служба по техническому и экспортному контролю: [сайт]. — URL: <https://bdu.fstec.ru/threat>

5. База данных общеизвестных уязвимостей информационной безопасности // Common Vulnerabilities and Exposures: [сайт]. — URL: <https://cve.mitre.org/>

6. MITRE ATT&CK® - База знаний о тактике и методах противника // Common Vulnerabilities and Exposures : [сайт]. — URL: <https://attack.mitre.org/>

7. Государственная система распространения правовых актов в электронном виде // Официальный интернет-портал правовой информации: [сайт]. — URL: <http://www.pravo.gov.ru/>

8. «КонсультантПлюс» (перечень информационных систем). // «КонсультантПлюс»: [сайт]. — URL: <http://www.consultant.ru/>

9. «ГАРАНТ» (комплект «ГАРАНТ-Максимум»). // ГАРАНТ.РУ Информационно-правовой портал: [сайт]. — URL: <https://www.garant.ru/>

Программное обеспечение:

1	Операционная система: Альт образование 11.1
2	Российский пакет офисных приложений Р7-Офис

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия	Учебная аудитория для проведения учебных занятий, оснащенная мультимедийным оборудованием и техническими средствами обучения: доска магнитно-маркерная, проектор, компьютер с необходимым комплектом лицензионного программного обеспечения
Лабораторные ¹ занятия	Учебная аудитория для проведения занятий семинарского типа укомплектована специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации: проектор, интерактивная доска. Есть подключение к сети «Интернет», выход в образовательную сеть университета.
Практические занятия	Учебная аудитория для проведения занятий семинарского типа укомплектована специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации: проектор, интерактивная доска. Есть подключение к сети «Интернет», выход в образовательную сеть университета.
Самостоятельная работа	Помещение для самостоятельной работы обучающихся оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и возможностью доступа к электронной информационно-образовательной среде университета

Программное обеспечение

1. Защищенная операционная система реального времени «QNX».
2. Операционная система MS Windows Server 2008 Standard Edition (SP2).
3. Операционная система Аврора.
4. Операционная система специального назначения «Astra Linux Special Edition».
5. Программа анализа защищенности TCP/IP «Ревизор Сети» версии 1.2.1.0.
6. Программа контроля полномочий доступа к информационным ресурсам «Ревизор-2 XP».
7. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
8. Программное изделие «Kaspersky Endpoint Security 10 для Linux».
9. Программное изделие «Kaspersky Endpoint Security 10 для Windows».
10. Программное изделие «Kaspersky Endpoint Security for Aurora».

Программно-аппаратное обеспечение

1. Аппаратно-программный комплекс шифрования «Континент».

11. Особенности освоения дисциплины (модуля) лицами с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины (модуля) обеспечивается:

- 1) для лиц с ограниченными возможностями здоровья по зрению:
 - присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочесть и оформить задание, в том числе, записывая под диктовку),
 - письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,
 - специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),
 - индивидуальное равномерное освещение не менее 300 люкс,
 - при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;
- 2) для лиц с ограниченными возможностями здоровья по слуху:
 - присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочесть и оформить задание, в том числе, записывая под диктовку),
 - обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;
 - обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата (в том числе с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента задания могут выполняться в устной форме.

12. Особенности реализации дисциплины с применением дистанционных образовательных технологий и электронного обучения

Согласно части 1 статьи 16 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» под *электронным обучением* понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников. Под *дистанционными образовательными технологиями* понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Реализация дисциплины может быть осуществлена с применением дистанционных образовательных технологий и электронного обучения полностью или частично. Компоненты УМК дисциплины (рабочая программа дисциплины, оценочные и методические материалы, формы аттестации), реализуемой с применением дистанционных образовательных технологий и электронного обучения, содержат указание на их использование.

При организации образовательной деятельности с применением дистанционных образовательных технологий и электронного обучения могут предусматриваться асинхронный и синхронный способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет».

При применении дистанционных образовательных технологий и электронного обучения в расписании по дисциплине указываются: способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет» (ВКС-видеоконференцсвязь, ЭТ – электронное тестирование); ссылки на электронную информационно-образовательную среду СКФУ, на образовательные платформы и ресурсы иных организаций, к которым предоставляется открытый доступ через информационно-телекоммуникационную сеть «Интернет»; для синхронного обучения - время проведения онлайн-занятий и преподаватели; для асинхронного обучения - авторы онлайн-курсов.

При организации промежуточной аттестации с применением дистанционных образовательных технологий и электронного обучения используются Методические рекомендации по применению технических средств, обеспечивающих объективность результатов при проведении промежуточной и государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры с применением дистанционных образовательных технологий (Письмо Минобрнауки России от 07.12.2020 г. № МН-19/1573-АН "О направлении методических рекомендаций").

Реализация дисциплины с применением электронного обучения и дистанционных образовательных технологий осуществляется с использованием электронной информационно-образовательной среды СКФУ, к которой обеспечен доступ обучающихся через информационно-телекоммуникационную сеть «Интернет», или с использованием ресурсов иных организаций, в том числе платформ, предоставляющих сервисы для

проведения видеоконференций, онлайн-встреч и дистанционного обучения МТС Линк, а также с использованием возможностей социальных сетей для осуществления коммуникации обучающихся и преподавателей.

Учебно-методическое обеспечение дисциплины, реализуемой с применением электронного обучения и дистанционных образовательных технологий, включает представленные в электронном виде рабочую программу, учебно-методические пособия или курс лекций, методические указания к выполнению различных видов учебной деятельности обучающихся, предусмотренных дисциплиной, и прочие учебно-методические материалы, размещенные в информационно-образовательной среде СКФУ.