Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гробова 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. Гробова
Ф.И.О.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита персональных данных в информационных системах
название дисциплины (модуля)

| | |
|---|---|
| Направление подготовки | 10.03.01 «Информационная безопасность» |
| Направленность (профиль) | Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности) |
| Год начала обучения | 2026 |
| Форма обучения | очная |
| Реализуется в семестре | 6 |

**Разработано**
Заведующий кафедрой
(должность разработчика)
Петренко В.И.
Ф.И.О.

Ставрополь 2026 г.

**1. Цель и задачи освоения дисциплины (модуля)**

Цель освоения дисциплины «Защита персональных данных в информационных системах» является теоретическая и практическая подготовка бакалавра для проведения работ по обеспечению безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) в соответствии с современными требованиями, а также приобретение набора компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Задачи освоения дисциплины

– формирование знаний нормативно-правовой документации в области персональных данных и умений работы с ней с использованием современных информационных технологий;

– формирование умений выявления угроз и уязвимостей безопасности персональных данных с подготовкой отчетов в цифровом или бумажном формате;

– формирование умений по разработке организационных и технических мер по обеспечению безопасности персональных данных;

– формирование навыков разработки организационно-распорядительных документов в области защиты персональных данных с использованием офисных приложений;

– формирование навыков самостоятельного изучения литературы в области обеспечения безопасности персональных данных с использованием инструментария электронных библиотечных систем, а также порталов регуляторов в области защиты информации.

**2. Место дисциплины (модуля) в структуре образовательной программы**

Дисциплина «Защита персональных данных в информационных системах» 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-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности | ИД-2 ОПК-5 Определяет рациональные меры по обеспечению организационной защиты на объекте; организует работу персонала с конфиденциальной информацией; разрабатывает проекты нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов. | – организует работу персонала с персональными данными<br>– разрабатывает проекты нормативных документов, регламентирующих работу по защите персональных данных в информационных системах персональных данных, а также положений, инструкций и других организационно-распорядительных документов |
| | ИД-3 ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации | – оценивает угрозы безопасности персональным данным в информационных системах персональных данных на основе нормативных и |

| | | |
|---|---|---|
| | | методических документов, регламентирующих деятельность по защите персональных данных |
| ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности | ИД-1 ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности защите персональных данных в информационных системах | – разрабатывает, внедряет и сопровождает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных<br>– разрабатывает внедряет и сопровождает комплекс мер по построению системы защиты персональных данных |

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

| Объем занятий: всего: 3 з.е. 108 акад.ч. | ОФО, в акад. часах |
|---|---|
| **Контактная работа:** | |
| Лекции/из них практическая подготовка | 32 |
| Лабораторных работ/из них практическая подготовка | 32 |
| **Самостоятельная работа** | 44 |
| **Формы контроля** | |
| Зачет с оценкой | + |

* Дисциплина (модуль) предусматривает применение электронного обучения, дистанционных образовательных технологий *(если иное не установлено образовательным стандартом)*

**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 | |
| 1. | Основные понятия и определения<br>1. Актуальность проблемы защиты персональных данных в информационных системах<br>2. Основные понятия в области защиты персональных данных | ИД-2 ОПК-5 | 2 | | 2 | 2,00 |
| 2. | Международное и национальное право в области защиты персональных данных<br>1. Международное право в области защиты персональных данных<br>2. Федеральное законодательство Российской Федерации в области защиты персональных данных | ИД-2 ОПК-5 | 2 | | 2 | 2,00 |
| 3. | Содержание и основные положения Федерального закона Российской Федерации № 152-ФЗ «О персональных данных»<br>1. Общие положения закона<br>2. Принципы и условия обработки персональных данных<br>3. Категории персональных данных<br>4. Права субъекта персональных данных<br>5. Обязанности оператора | ИД-2 ОПК-5 | 2 | | 2 | 2,00 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4. | Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах<br>1. Основные принципы моделирования угроз с использованием методических документов ФСТЭК и ФСБ<br>2. Угрозы информационной безопасности<br>3. Общая характеристика уязвимостей информационной системы персональных данных | ИД-3 ОПК-5 | 2 | | 2 | 2,00 |
| 5. | Особенности обработки биометрических персональных данных<br>1. Порядок обработки параметров биометрических персональных данных<br>2. Порядок размещения и обновления биометрических персональных данных в единой биометрической системе<br>3. Требования к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации<br>4. Перечень угроз безопасности, актуальных при обработке биометрических персональных данных | ИД-3 ОПК-5 | 2 | | 2 | 2,00 |
| 6. | Методика оценки угроз безопасности персональным данным<br>1. Порядок оценки угроз безопасности персональным данным<br>2. Определение негативных последствий от реализации угроз безопасности персональным данным<br>3. Определение возможных объектов воздействия угроз безопасности персональным данным | ИД-3 ОПК-5, ИД-1ОПК-2.3. | 2 | | 2 | 2,00 |
| 7. | Оценка возможности реализации угроз безопасности персональным данным и определение их актуальности<br>1. Определение источников угроз безопасности персональным данным<br>2. Оценка способов реализации угроз безопасности персональным данным<br>3. Оценка актуальности угроз безопасности персональным данным | ИД-3 ОПК-5 | 2 | | 2 | 2,00 |
| 8. | База знаний о поведениях компьютерных злоумышленников<br>1. Аналитика угроз<br>2. Обнаружение и аналитика<br>3. Эмуляция противника и Red Teaming<br>4. Оценки и инжиниринг | ИД-3 ОПК-5 | 2 | | 2 | 2,00 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 9. | Построение системы защиты персональных данных<br>1. Основные этапы при построении системы защиты персональных данных<br>2. Комплекс организационных и технических мероприятий в рамках СЗПДн | ИД-1 ОПК-2.3 | 2 | | 2 | 2,00 |
| 10. | Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных<br>1. Организационные и технические меры по обеспечению безопасности персональных данных<br>2. Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных | ИД-1 ОПК-2.3 | 2 | | 2 | 2,00 |
| 11. | Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий<br>1. Общие требования по безопасности информации в информационных системах персональных данных<br>2. Требования к разработке и производству средства<br>3. Требования к проведению испытаний средства<br>4. Требования к поддержке безопасности средства | ИД-1 ОПК-2.3 | 2 | | 2 | 4,00 |
| 12. | Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных с использованием средств криптографической защиты информации<br>1. Определение актуальности использования средств криптографической защиты информации для обеспечения безопасности персональных данных<br>2. Определение актуальных угроз<br>3. Состав и содержание организационных и технических мер | ИД-1 ОПК-2.3 | 2 | | 2 | 4,00 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 13. | Аттестация, сертификация и лицензирование в области защиты персональных данных<br>1. Сертификация средств защиты персональных данных<br>2. Аттестации информационных систем персональных данных по требованиям безопасности информации<br>3. Лицензирование деятельности по защите персональных данных | ИД-1 ОПК-2.3 | 2 | | 2 | 4,00 |
| 14. | Контроль в области защиты персональных данных<br>1. Регуляторы в области защиты персональных данных<br>2. Проверки Роскомнадзора<br>3. Проверки ФСБ РФ<br>4. Проверки ФСТЭК РФ | ИД-1 ОПК-2.3 | 2 | | 2 | 4,00 |
| 15. | Регламент по защите данных General Data Protection Regulation 2016/679 (GDPR)<br>1. Критерии применимости GDPR<br>2. Принципы GDPR<br>3. Правовые основания передачи персональных данных<br>4. Обеспечение прозрачности при обработке персональных данных в онлайн-сервисах | ИД-2 ОПК-5 | 2 | | 2 | 4,00 |
| 16. | Ответственность за нарушение законодательства в области персональных данных<br>1. Административная ответственность<br>2. Уголовная ответственность<br>3. Ответственность согласно Трудовому кодексу РФ<br>4. Ответственность согласно Федеральному закону «О персональных данных» | ИД-2 ОПК-5 | 2 | | 2 | 4,00 |
| | ИТОГО за 6 семестр | | 32 | | 32 | 44 |
| | ИТОГО | | 32 | | 32 | 44 |

**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 завершенный раздел.

Лекционный материал посвящен рассмотрению ключевых, базовых положений курсов и разъяснению учебных заданий, выносимых на самостоятельную работу студентов *(включается при наличие соответствующих занятий)*.

Практические занятия проводятся с целью закрепления усвоенной информации, приобретения навыков ее применения при решении практических задач в соответствующей предметной области *(включается при наличие соответствующих занятий).*

Лабораторные работы направлены на приобретение опыта практической работы в соответствующей предметной области *(включается при наличие соответствующих занятий)*.

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. Петренко, В. И. Защита персональных данных в информационных системах: учебное пособие / В. И. Петренко. — Ставрополь : Северо-Кавказский федеральный университет, 2016. — 201 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/66023.html (дата обращения: 04.03.2023). — Режим доступа: для авторизир. пользователей

2. Петренко, В. И. Защита персональных данных в информационных системах: лабораторный практикум / В. И. Петренко, И. В. Мандрица. — Ставрополь : Северо-Кавказский федеральный университет, 2018. — 118 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/83198.html (дата обращения: 04.03.2023). — Режим доступа: для авторизир. пользователей

3. Технические средства и методы защиты информации: учебное пособие / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков, И. В. Голубятников. — Москва: Горячая линия-Телеком, 2012. — 616 с. — ISBN 978-5-9912-0084-4. — Текст: электронный // Лань:

электронно-библиотечная система. — URL: https://e.lanbook.com/book/5154 (дата обращения: 18.10.2022).

8.1.2. Перечень дополнительной литературы:

1. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко. — Ставрополь : Северо-Кавказский федеральный университет, 2015. — 222 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/63138.html (дата обращения: 04.03.2023). — Режим доступа: для авторизир. пользователей

2. Петренко, В. И. Защита персональных данных в информационных системах. Практикум / В. И. Петренко, И. В. Мандрица. — 4-е изд., стер. — Санкт-Петербург : Лань, 2022. — 108 с. — ISBN 978-5-507-45301-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/264242 (дата обращения: 04.03.2023). — Режим доступа: для авториз. пользователей.

3. Воробьев, Е. Г. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных : учебное пособие / Е. Г. Воробьев. — Санкт-Петербург : Интермедия, 2017. — 432 с. — ISBN 978-5-4383-0120-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/66796.html (дата обращения: 04.03.2023). — Режим доступа: для авторизир. пользователей

4. Скрипник, Д. А. Обеспечение безопасности персональных данных : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 121 с. — ISBN 978-5-4497-0334-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89449.html (дата обращения: 04.03.2023). — Режим доступа: для авторизир. пользователей

5. Голембиовская, О. М. Формализация подходов к обеспечению защиты персональных данных : монография / О. М. Голембиовская, М. Ю. Рытов, К. Е. Шинаков. — Саратов : Ай Пи Эр Медиа, 2019. — 198 с. — ISBN 978-5-4486-0726-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/81851.html (дата обращения: 04.03.2023). — Режим доступа: для авторизир. пользователей

6. Шинаков, К. Е. Анализ рисков безопасности информационных систем персональных данных : монография / К. Е. Шинаков, М. Ю. Рытов, О. М. Голембиовская. — Москва : Ай Пи Ар Медиа, 2020. — 236 с. — ISBN 978-5-4497-0535-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/95150.html (дата обращения: 04.03.2023). — Режим доступа: для авторизир. пользователей

7. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. - 436 с.: ил

8.1.3. Перечень нормативных документов:

1. Приказ Роскомнадзора от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения».

2. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению

безопасности персональных данных при их обработке в информационных системах персональных данных».

4. Положение о федеральном государственном контроле (надзоре) за обработкой персональных данных, утв. Постановлением Правительства РФ от 29.06.2021 № 1046 (ред. от 16.12.2021) – содержит описание видов и приемом контроля.

5. Приказ Роскомнадзора от 24.12.2021 № 253 «Об утверждении формы проверочного листа (списка контрольных вопросов, ответы на которые свидетельствуют о соблюдении или несоблюдении контролируемым лицом обязательных требований), применяемого при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальными органами».

6. Выписка из Требований по безопасности информации, утвержденных приказом ФСТЭК России от 2 июня 2020 г. N 76.

7. Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

8. Постановление Правительства Российской Федерации от 23.10.2021 г. № 1815 «Об утверждении перечня случаев осуществления сбора и обработки используемых для идентификации либо идентификации и аутентификации биометрических персональных данных в информационных системах организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также случаев использования организациями, за исключением кредитных организаций, некредитных финансовых организаций, которые осуществляют указанные в части первой статьи 761 Федерального закона "О Центральном банке Российской Федерации (Банке России)" виды деятельности, субъектами национальной платежной системы, индивидуальными предпринимателями указанных информационных систем для идентификации либо идентификации и аутентификации физического лица, выразившего согласие на их проведение».

9. Постановление Правительства Российской Федерации от 20.10.2021 г. № 1799 «Об аккредитации организаций, владеющих информационными системами, обеспечивающими идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, и (или) оказывающих услуги по идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц».

10. Приказ Минцифры России № 930 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации».

11. Приказ Минцифры России № 902 «Об утверждении перечня угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица в информационных системах организаций, осуществляющих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, за исключением единой

информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, а также актуальных при взаимодействии государственных органов, органов местного самоуправления, индивидуальных предпринимателей, нотариусов и организаций, за исключением организаций финансового рынка, с указанными информационными системами, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных, и учетом вида аккредитации организации из числа организаций, указанных в частях 18.28 и 18.31 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации"».

12. Приказ Минцифры России № 896 «Об утверждении требований к деловой репутации единоличного исполнительного органа или членов коллегиального исполнительного органа организации, владеющей информационной системой, обеспечивающей идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, и (или) оказывающей услуги по идентификации и (или) аутентификации с использованием биометрических персональных данных физических лиц».

13. Приказ Минцифры РФ от 06.08.2021 № 816 «Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных, а также об определении степени взаимного соответствия указанных биометрических персональных данных, достаточной для проведения идентификации, предусмотренной Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

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

1. Методические рекомендации по организации и проведению самостоятельной работы студентов по учебной дисциплине «Защита персональных данных в информационных системах».
2. Методические рекомендации по выполнению лабораторных работ по учебной дисциплине «Защита персональных данных в информационных системах».

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. Цифровой образовательный ресурс IPR SMART // ЭБС IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/ (дата обращения: 04.02.2023).

7. Znanium.com. // ЭБС Znanium: [сайт]. — URL: https://znanium.com/ (дата обращения: 04.02.2023).

8. ЭБС «Юрайт». // Юрайт. Образовательная платформа: [сайт]. — URL: http://www.biblio-online.ru (дата обращения: 04.02.2023).

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 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 | Лаборатория в области технической защиты информации, оснащенная специализированным оборудованием по защите информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок, техническими средствами контроля эффективности защиты информации от утечки по указанным каналам.<br><br>Лаборатория в области программно-аппаратных средств защиты информации, оснащенную антивирусными программными комплексами, аппаратными средствами аутентификации пользователя, программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации, средствами контроля и управления доступом в помещения, средствами охранной и пожарной сигнализации. |
| 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. Межсетевой экран серии Cisco ASA 55xx.
2. Операционная система MS Windows Server 2008 Standard Edition (SP2).
3. Операционная система Аврора.
4. Операционная система специального назначения «Astra Linux Special Edition».
5. Программное изделие «Kaspersky Endpoint Security 10 для Linux.
6. Программное изделие «Kaspersky Endpoint Security 10 для Windows».
7. Программное изделие Антивирус Касперского 8.0 для Windows Servers Enterprise Edition.

***Программно-аппаратное обеспечение***

1. Аппаратно-программный комплекс шифрования «Континент».
2. Коммутатор Cisco 2XXX/38XX.
3. Маршрутизатор Cisco 3825/3845.
4. Межсетевой экран Cisco ASA 5580-20.

***Технические средства защиты информации***

1. Генератор шума ГШ-1000М.
2. Система виброакустической и акустической защиты «Соната-АВ».
3. Система постановки виброакустических и акустических помех «Шорох-2М».
4. Система постановки виброакустических помех «Шторм».

[1] Перечень лабораторий используемых в учебном процессе представлен https://www.ncfu.ru/sveden/objects/

5. Устройство защиты объектов информатизации от утечки по техническим каналам «Соната-Р2».

6. Фильтр сетевой помехоподавляющий ФСП-1Ф-7А

**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, прочитать 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, прочитать 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 Минобрнаки 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.