

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)
ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ
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

6

Разработано

Доцент кафедры

(должность разработчика)

Рачков В.Е.

Ф.И.О.

Ставрополь 2026 г.

1. Цель и задачи освоения дисциплины (модуля)

Целью изучения дисциплины «Защита информации от утечки по техническим каналам» является формирование набора общекультурных и профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

Формируемые в рамках дисциплины компетенции способствуют решению профессиональных задач по защите информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях, а также приобретение набора общекультурных и общепрофессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Защита информации от утечки по техническим каналам» 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;
	ИД-3 _{ОПК-6} Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	Осуществляет тщательный подбор, изучение и подробное обобщение научно-технической литературы, нормативных и методических материалов, составлять полный обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности
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: 5 з.е. 180 акад.ч.	ОФО, в акад. часах
Контактная работа:	
Лекции/из них практическая подготовка	32
Лабораторных работ/из них практическая подготовка	32
Практических занятий/из них практическая подготовка	32
Самостоятельная работа	48
Формы контроля	
Экзамен	36
Курсовая работа	+

* 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	Тема 1. Социальная психология как наука Социальная психология конфликта. Информационные и технические показатели технического контроля. Цели и задачи технического контроля эффективности мер защиты информации. Содержание технического контроля.	ОПК-6 ОПК-9	2	2	2	2.00
2	Тема 2. История возникновения и развития социально-психологических идей Контроль защищенности объекта. Содержание аттестационного контроля. Содержание эксплуатационного контроля.	ОПК-6 ОПК-9	2	2	2	2.00
3	Тема 3. Основные теоретические ориентации современной социальной психологии Порядок реализации организационной и инструментальной частей аттестационного контроля. Проведение контроля защищенности.	ОПК-6 ОПК-9	2	2	2	2.00
4	Тема 4. Основные теоретические ориентации современной социальной психологии Порядок реализации эксплуатационного контроля. Оценка защитных мероприятий. Технический контроль выполнения норм защиты информации от утечки за счет ПЭМИН.	ОПК-6 ОПК-9	2	2	2	2.00
5	Тема 5. Методология и методы социально-психологического исследования Порядок измерения напряжения ПЭМИН. Провести разработку алгоритма измерения напряженности поля.	ОПК-6 ОПК-9	2	2	2	2.00

6	Тема 6. Проблема группы в социальной психологии Порядок измерения напряженности поля. Измерительные площадки.	ОПК-6 ОПК-9	2	2	2	2.00
7	Тема 7. Особенности больших социальных групп Измерительные площадки. Порядок реализации эксплуатационного контроля. Проведение контроля защищенности.	ОПК-6 ОПК-9	2	2	2	2.00
8	Тема 8. Массовидные явления в больших социальных группах Контроль защищенности выделенных помещений от утечки акустической речевой информации. Оценка мероприятий по информационной защите помещений. Инструментальный контроль акустической защищенности.	ОПК-6 ОПК-9	2	2	2	2.00
9	Тема 9. Психология малых групп Калибровка передающего измерительного комплекса. Размещение акустического излучателя передающего измерительного комплекса. Измерение отношений «сигнал/шум» в контрольных точках при инструментальном контроле рабочих помещений, не оборудованных системой звукоусиления.	ОПК-6 ОПК-9	2	2	2	2.00
10	Тема 10. Концепция коллектива в социальной психологии Реализация инструментально-расчетного метода определения отношений «речевой сигнал / акустический (вибрационный) шум».	ОПК-6 ОПК-9	2	2	2	2.00
11	Тема 11. Динамические процессы в малой группе Моделирование и исследование процесса паразитной (несанкционированной) модуляции (интермодуляции). Моделирование и исследование принципов действия средств высокочастотного навязывания.	ОПК-6 ОПК-9	2	2	2	4.00
12	Тема 12. Социально-психологические аспекты социализации личности Акустоэлектрический преобразователь телефонного аппарата. Конденсаторный микрофон. Принцип реализации ВЧ. Процесс высокочастотного навязывания.	ОПК-6 ОПК-9	2	2	2	4.00
13	Тема 13. Психологические механизмы регуляции социального поведения личности Моделирование и исследование принципов работы средств экранирования ПЭМИН.	ОПК-6 ОПК-9	2	2	2	4.00
14	Тема 14. Социальная психология общения Эффективность экранирования. Отдельные виды экранирования. Подавление емкостных паразитных связей.	ОПК-6 ОПК-9	2	2	2	4.00
15	Тема 15. Психология межличностных отношений Подавление индуктивных паразитных связей. Магнитостатическое экранирование. Экранирование проводов и катушек индуктивности.	ОПК-6 ОПК-9	2	2	2	4.00
16	Тема 16. Социальная психология конфликта Методика расчета параметров пассивных НЧ и ВЧ фильтров. Методика расчета параметров пассивных полосовых и режекторных фильтров.	ОПК-6 ОПК-9	2	2	2	4.00

17	Тема 17. Оценка защищенности помещений от утечки речевой информации по акустическим и виброакустическим каналам. Моделирование и исследование принципов построения и работы средств генерации шума для энергетического скрывтия ПЭМИН. Технические характеристики. Генератор шума ГШ-1000М.	ОПК-6 ОПК-9	-	-	-	2.00
18	Тема 18. Аттестация объекта информатизации по требованиям безопасности информации Исследование звукопоглощающих и звукоизоляционных характеристик материалов, применяемых для звукоизоляции выделенных помещений. Энергетическое скрывтие акустических сигналов. Звукоизолирующие ограждения.	ОПК-6 ОПК-9	-	-	-	2.00
	ИТОГО за 6 семестр		32	32	32	48
	ИТОГО		32	32	32	48

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 *(включается при наличии 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. Технические средства и методы защиты информации: учеб. пособие / под ред. А.П. Зайцева, А.А. Шелупанова. – [4-е изд., испр. и доп.]. – Москва : Горячая линия-Телеком, 2016. – 616 с.

2. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. – М.: НПЦ «Аналитика», 2018.

8.1.2. Перечень дополнительной литературы:

Иванов, А. В. Защита речевой информации от утечки по акустоэлектрическим каналам / А.В. Иванов; В.А. Трушин. - Новосибирск : НГТУ, 2012. - 43 с. - ISBN 978-5-7782-1888-8

2 Титов, А. А. Инженерно-техническая защита информации : Учебное пособие / Титов А. А. - Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. - 197 с. - Книга находится в базовой версии ЭБС IPRbooks.

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 информации от утечки по техническим каналам».
2. Методические рекомендации по выполнению лабораторных работ по учебной дисциплине «Защита информации от утечки по техническим каналам»
3. Методические рекомендации по выполнению практических работ по учебной дисциплине «Защита информации от утечки по техническим каналам».
4. Методические рекомендации по выполнению курсовых работ (проектов) по учебной дисциплине «Защита информации от утечки по техническим каналам».

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 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 занятия ¹	Лаборатория в области электротехники, электроники и схемотехники, оснащенная учебно-лабораторными стендами и контрольно-измерительной аппаратурой для измерения частотных свойств, форм и временных характеристик сигналов, средствами для измерения параметров электрических цепей, средствами генерирования сигналов.
Практические занятия	Учебная аудитория для проведения учебных занятий, оснащенная современной вычислительной техникой, мультимедийным оборудованием и техническими средствами обучения обеспечивающая практическую подготовку в соответствии с направленностью (профилем) программы бакалавриата «Организация и технологии

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

	защиты информации (по отрасли или в сфере профессиональной деятельности)». Специально оборудованная аудитория защищенного документооборота, оснащенный рабочими местами на базе офисной техники, обучающими стендами и материалами
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. Комплекс средств защиты информации от несанкционированного доступа пакета прикладных программ интегрированной системы технических средств охраны АССаД 32.
3. Межсетевой экран серии Cisco ASA 55xx.
4. Операционная система MS Windows Server 2008 Standard Edition (SP2).
5. Операционная система Аврора.
6. Операционная система специального назначения «Astra Linux Special Edition».
7. Подсистема безопасности программного обеспечения «Инструментальная система разработки распределенных приложений «Sitex» 4.2».
8. Программа анализа защищенности TCP/IP «Ревизор Сети» версии 1.2.1.0.
9. Программа контроля полномочий доступа к информационным ресурсам «Ревизор-2 XP».
10. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
11. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
12. Программа поиска и измерения опасных сигналов ПЭМИН СВТ «Легенда-05Упс».
13. Программа расчета зон безопасности средств вычислительной техники «Легенда-05Рс».
14. Программа фиксации и контроля исходного состояния программного комплекса «ФИКС».
15. Программное изделие «Kaspersky Endpoint Security 10 для Linux.
16. Программное изделие «Kaspersky Endpoint Security 10 для Windows».
17. Программное изделие «Kaspersky Endpoint Security for Aurora».
18. Программное изделие Антивирус Касперского 8.0 для Windows Servers Enterprise Edition.
19. Программное комплекс Acronis Backup & Recovery.
20. Программное обеспечение Cisco IOS AES версии 12.4(5b) для маршрутизаторов Cisco 3825.
21. Программное обеспечение Oracle Identity Access Management Suite.
22. Программное обеспечение SafeNet Authentication Service.
23. Программное обеспечение усиления функций безопасности операционных систем Microsoft Windows – eToken Network Logon 5.
24. Программное средство расчета показателей защищенности информации от утечки за счет побочных электромагнитных излучений и наводок по результатам специальных исследований и оценки защищенности (эффективности защиты) информации, обрабатываемой средствами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок «ПЭМИН-2018».
25. Программный комплекс «InfoWatch Traffic Monitor».

26. Программный комплекс для создания и управления виртуальной инфраструктурой VMware vSphere.
27. Программный комплекс защиты информации от НСД «Страж 1.1.
28. Программный комплекс Межсетевой экран с системой обнаружения вторжений Iidesco UTM.
29. Программный комплекс обнаружения вторжений «Ребус-СОВ».
30. Система защиты информации от несанкционированного доступа «Доверенная операционная система «Циркон 10С.p2»
31. Специальное программное обеспечение «АС «ГРИФ».
32. Специальное программное обеспечение межсетевого экрана «Z-2», версия 2.6.

Программно-аппаратное обеспечение

1. Аппаратно-программный комплекс обнаружения компьютерных атак «Аргус», версия 1.5».
2. Аппаратно-программный комплекс шифрования «Континент».
3. Аппаратный модуль обнаружения вторжений Cisco IDSM-2 FOR CISCO 6500 SERIES с версией программного обеспечения Cisco Intrusion Prevention System.
4. Коммутатор Cisco 2XXX/38XX.
5. Комплекс системы защиты информации от несанкционированного доступа «Аккорд-1.95.
6. Комплекс средств защиты информации от несанкционированного доступа «Аккорд-NT/2000».
7. Маршрутизатор Cisco 2911 с установленным программным обеспечением Cisco IOS Software.
8. Маршрутизатор Cisco 3825/3845.
9. Маршрутизатор Cisco 3925 с установленным программным обеспечением Cisco IOS.
10. Межсетевой экран Cisco ASA 5580-20.
11. Межсетевой экран Cisco PIX Firewall 515E.
12. Программа контроля состояния сертифицированных программных средств защиты информации» «ФИКС 3.0».
13. Программа поиска и гарантированного уничтожения на дисках «TERRIER».
14. Программно-аппаратный комплекс «Сервер безопасности DioNIS Security Server» с встроенным межсетевым экраном «DioNIS Firewall».
15. Программно-аппаратный комплекс межсетевого экрана «WatchGuard Firebox» с программным обеспечением «Fireware OS».
16. Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ».
17. Программный комплекс защиты информации от НСД «Страж 1.1.
18. Система защиты информации «Secret Net».
19. Система защиты информации от несанкционированного доступа «Dallas Lock 7.0».
20. Система защиты информации от несанкционированного доступа «Страж NT».
21. Система оценки защищенности выделенных помещений по виброакустическому каналу «ШЕПОТ».
22. Средство создания модели системы разграничения доступа «Ревизор-1 XP».

Технические средства защиты информации

1. Виброакустический генератор «БАРОН»
2. Генератор акустического шума «ЛГШ-301»
3. Генератор шума «Гром-ЗИ-4»

4. Генератор шума ГШ-1000М
5. Система акустической и вибрационной защиты «Кабинет»
6. Система акустической и вибрационной защиты «Кабинет».
7. Система виброакустической и акустической защиты «Соната-АВ».
8. Система постановки виброакустических и акустических помех «Шорох-2М».
9. Система постановки виброакустических помех «Шторм»
10. Устройство защиты объектов информатизации от утечки по техническим каналам «Соната-Р2».
11. 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, 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.