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
Гробова Т.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Перспективные направления защиты информации

Специальность	10.05.03 Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	А

Разработано
Бабенко М. Г. – заведующий кафедрой вычислительной математики и кибернетики

Ставрополь 2026 г.

Цель и задачи освоения дисциплины

Цель дисциплины: формирование набора универсальных и общепрофессиональных компетенций будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем

Задачи дисциплины:

- изучить методологию применения системного анализа к решению проблем повышения энергетической скрытности систем спутниковой связи и синтеза их параметров;
- изучить современные методы разработки математических моделей спутниковых каналов связи,
- изучить основы прогнозирования условий распространения радиоволн и показателей помехозащищенности систем спутниковой связи;
- привить навыки самостоятельной постановки и решения актуальных практических и научных задач в области защиты информации.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Перспективные направления защиты информации» относится к дисциплинам по выбору Б1.В.ДВ.7. Ее освоение происходит в А семестре.

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

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ПК-9 Способен формировать требования к защите информации в автоматизированных системах	ИД-1$_{ПК-9}$ Обосновывает необходимость защиты информации в автоматизированной системе.	Способен формировать требования к защите информации в автоматизированных системах, а также обосновывать необходимость защиты информации в автоматизированной системе.
	ИД-2$_{ПК-9}$ Определяет угрозы безопасности информации, обрабатываемой автоматизированной системой.	Способен формировать требования к защите информации в автоматизированных системах, а также определять угрозы безопасности информации, обрабатываемой автоматизированной системой.
	ИД-3$_{ПК-9}$ Разрабатывает архитектуру системы защиты информации автоматизированной системы.	Способен формировать требования к защите информации в автоматизированных системах, а также

		разрабатывать архитектуру системы защиты информации автоматизированной системы.
	ИД-4$_{ПК-9}$ Моделирует защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации.	Способен формировать требования к защите информации в автоматизированных системах, а также моделировать защищённые автоматизированные системы с целью анализа их уязвимостей и оценки эффективности средств и способов защиты информации.

4. Объем учебной дисциплины и формы контроля *

Объем занятий: всего: **3** з.е. **108** акад.ч.	ОФО, в акад. часах
Контактная работа:	
Лекции/из них практическая подготовка	18/0
Лабораторных работ/из них практическая подготовка	36/0
Практических занятий/из них практическая подготовка	-
Самостоятельная работа	54
Формы контроля	
Экзамен	-
Зачет А семестр	+
Зачет с оценкой	-
Курсовая работа	-

* Дисциплина предусматривает применение электронного обучения, дистанционных образовательных технологий

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

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	очная форма				Формы текущего контроля успеваемости
			Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самостоятельная работа, часов	
			Лекции	Практические занятия	Лабораторные работы		
	А СЕМЕСТР						
1	**Знакомство с современными угрозами информационной безопасности и средствами их нейтрализации.** Перспективы развития глобальных угроз и вызовов кибербезопасности Лекция представляет обзор актуальных угроз кибербезопасности и перспективных направлений их развития, включая анализ современных методов атак и обсуждение инновационных технологий защиты информации в условиях растущих киберугроз.	ПК-9 ИД-1ПК-9 ИД-2ПК-9 ИД-3ПК-9 ИД-4ПК-9	2	-	4	6	Защита лабораторной работы

2	**Анализ методов квантовой криптографии и моделирование квантовой передачи ключей.** Основы квантовой защиты информации и её потенциал. Лекция описывает основы квантовой криптографии, включая принципы суперпозиции и запутанности, а также анализирует потенциал квантовой защиты информации для создания безопасных коммуникационных систем.	ПК-9 ИД-1ПК-9 ИД-2ПК-9 ИД-3ПК-9 ИД-4ПК-9	2	-	4	6	Защита лабораторной работы
3	**Разработка схемы защиты данных на основе блокчейн-технологий.** Возможности применения блокчейна в системах ИБ. Лекция описывает процесс создания схем защиты данных на базе блокчейна, а также анализирует возможности использования этой технологии в системах информационной безопасности для обеспечения целостности и конфиденциальности информации.	ПК-9 ИД-1ПК-9 ИД-2ПК-9 ИД-3ПК-9 ИД-4ПК-9	2	-	4	6	Защита лабораторной работы
4	**Исследование применения ИИ в системах обнаружения атак.** Роль машинного обучения в автоматизации киберзащиты. Лекция описывает, как ИИ и машинное обучение применяются для автоматизации процессов обнаружения и предотвращения кибератак, а также анализирует их значимость в повышении уровня кибербезопасности и снижении времени реакции на угрозы.	ПК-9 ИД-1ПК-9 ИД-2ПК-9 ИД-3ПК-9 ИД-4ПК-9	2	-	4	6	Защита лабораторной работы

5	**Практика построения системы Zero Trust в корпоративной среде.** Концепция полного недоверия как основа новой архитектуры безопасности. Лекция описывает процесс построения системы безопасности Zero Trust, основанной на полном недоверии к любым субъектам доступа, и демонстрирует, как эта модель обеспечивает защиту корпоративных данных и приложений в современных условиях.	ПК-9 ИД-1ПК-9 ИД-2ПК-9 ИД-3ПК-9 ИД-4ПК-9	2	-	4	6	Защита лабораторной работы
6	**Моделирование защищённого обмена в среде интернета вещей (IoT).** Проблемы и решения безопасности в IoT-системах. Лекция анализирует современные угрозы безопасности в IoT-системах, включая атаки на устройства и сети, и демонстрирует методы моделирования защищённого обмена данными, направленные на минимизацию рисков компрометации информации в среде интернета вещей.	ПК-9 ИД-1ПК-9 ИД-2ПК-9 ИД-3ПК-9 ИД-4ПК-9	2	-	4	6	Защита лабораторной работы
7	**Применение гомоморфного шифрования для обработки зашифрованных данных.** Перспективы и ограничения криптографии без расшифровки. Лекция описывает принципы гомоморфного шифрования, его применение для обработки зашифрованных данных и анализирует преимущества и недостатки криптографии без расшифровки, включая проблемы производительности и управления ключами.	ПК-9 ИД-1ПК-9 ИД-2ПК-9 ИД-3ПК-9 ИД-4ПК-9	2	-	4	6	Защита лабораторной работы

8	**Анализ методов биометрической аутентификации будущего.** Новые направления в биометрии: поведенческие и нейронные признаки. Лекция исследует будущее биометрической аутентификации, акцентируя внимание на новых направлениях, таких как анализ поведенческих признаков и применение нейросетевых технологий для обработки биометрических данных, а также оценивает их потенциал и перспективы развития.	ПК-9 ИД-1ПК-9 ИД-2ПК-9 ИД-3ПК-9 ИД-4ПК-9	2	-	4	6	Защита лабораторной работы
9	**Проектирование системы защиты облачного хранилища.** Тенденции развития облачных вычислений и связанных с ними угроз. Лекция охватывает принципы построения систем защиты облачных данных и анализирует текущие тенденции в развитии облачных вычислений, включая рост числа атак и необходимость комплексного подхода к обеспечению безопасности облачных ресурсов.	ПК-9 ИД-1ПК-9 ИД-2ПК-9 ИД-3ПК-9 ИД-4ПК-9	2	-	4	6	Защита лабораторной работы
	ИТОГО за А семестр		**18**	**-**	**36**	**54**	
	ИТОГО		**18**	**-**	**36**	**54**	

6. Фонд оценочных средств по дисциплине

Фонд оценочных средств (ФОС) по дисциплине 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.

7. Методические указания для обучающихся по освоению дисциплины

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

Дисциплина «Перспективные направления защиты информации» построена по тематическому принципу, каждая тема представляет собой логически завершенный раздел.

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

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

8.1.1. Перечень основной литературы:

1. Бабаш, А. В. Актуальные вопросы защиты информации Электронный ресурс / Бабаш А. В., Баранова Е. К. : монография. – Москва : РИОР : ИНФРА-М, 2020. – 110 с. – ISBN отсутствует. – Рассматриваются современные аспекты защиты информации, включая анализ рисков и управление инцидентами в соответствии со стандартами ISO/IEC 27000, а также криптографические и теоретико-автоматные методы .
2. Шелухин, О. И. Сетевые аномалии. Обнаружение, локализация, прогнозирование Электронный ресурс / Шелухин О. И. : монография. – Москва : Горячая линия – Телеком, 2020. – 447 с. – ISBN отсутствует. – Изложены методы диагностики и защиты сетевых ресурсов от аномальных воздействий, приводящих к утечке или искажению информации .
3. Мещеряков, Р. В. Перспективные направления применения технологий искусственного интеллекта при защите информации Электронный ресурс / Мещеряков Р. В., Мельников С. Ю., Пересыпкин В. А., Хорев А. А. : статья. – Москва : Российский университет дружбы народов, 2022. – 12 с. – Рассматриваются актуальные задачи защиты информации с использованием

технологий искусственного интеллекта, включая обнаружение атак, вредоносных программ и утечек данных .

4. Ревякин, П. И. Цифровая трансформация университетов: угрозы информационной безопасности и направления снижения рисков Электронный ресурс / Ревякин П. И., Зинич А. В., и др. : статья. – Москва : Первое экономическое издательство, 2024. – 15 с. – Анализируются риски информационной безопасности в условиях цифровой трансформации образовательных организаций и предлагаются меры по их снижению .

8.1.2. Перечень дополнительной литературы:

1. Мельников, В. П. Информационная безопасность : учебник / Мельников В. П., Схиртладзе А. Г. – Москва : ТНТ, 2020. – 320 с. – ISBN 978-5-94178-403-5. – Учебник предназначен для студентов вузов, обучающихся по направлениям «Автоматизация технологических процессов и производств», «Конструкторско-технологическое обеспечение машиностроительных производств», специалистов информационных технологий и защиты информации, широкого круга пользователей компьютерных систем. Он будет полезен также магистрам и аспирантам высших учебных заведений.
2. Сухостат, В. В. Основы информационной безопасности : учебное пособие / Сухостат В. В., Васильева И. Н. – Санкт-Петербург : Изд-во СПбГЭУ, 2020. – 150 с. – ISBN отсутствует. – В пособии представлены основы информационной безопасности – базовые вопросы теории и методологии по решению проблем защиты информации.
3. Морозов, С. К. Техническая защита информации : учебное пособие. Ч. 1 / Морозов С. К., Красильникова Е. В. – Санкт-Петербург : Изд-во СПбГЭУ, 2020. – 200 с. – ISBN отсутствует. – В учебном пособии рассматриваются вопросы технической защиты информации, включая методы и средства обеспечения безопасности в компьютерных системах.

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

1. Методические указания по выполнению лабораторных работ по дисциплине "Перспективные направления защиты информации" (электронный ресурс)

2. Методические указания по организации и проведению самостоятельной работы по дисциплине " Перспективные направления защиты информации" (электронный ресурс)

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

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Нестандартные методы защиты информации»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

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

На лабораторных занятиях студенты представляют презентации, подготовленные ими в часы самостоятельной работы.

Информационные справочные системы:

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

1	КонсультантПлюс - http://www.consultant.ru/

Программное обеспечение:

1.	Альт Рабочая станция 10
2.	Альт Рабочая станция K
3.	Альт «Сервер»
4.	Пакет офисных программ - Р7-Офис

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

Лабораторные[1] занятия	Помещения для проведения лабораторных и практических работ (компьютерные классы), оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и возможностью доступа к электронной информационно-образовательной среде 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

11. Особенности освоения дисциплины 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 обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины 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 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:

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

- 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 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.