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
Программно-аппаратные средства 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	8

Разработано
Орёл Д.В., - доцент кафедры организации и технологии защиты информации

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:

- Формирование требований к системе управления информационной безопасности конкретного объекта;
- Проектирование системы управления информационной безопасности конкретного объекта.
- Эффективное управление информационной безопасности конкретного объекта

2. Место дисциплины в структуре образовательной программы

Дисциплина «Программно-аппаратные средства защиты информации» относится к дисциплинам обязательной части. Ее освоение происходит в 8 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
ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	ИД-1ОПК-2 Осуществляет поиск системного программного обеспечения, понимает структуру операционной системы, предназначение основных параметров и компонентов операционной системы семейства Windows; использует методы инсталляции системного программного обеспечения, а также режимы его взаимодействия с операционной системой; выбирает методы мониторинга компонентов операционной системы Windows, а также режимы отказоустойчивой конфигурации.	Предоставляет отчёт с детальным анализом назначения системного программного обеспечения, а также структуры операционной системы, предназначения основных параметров и компонентов операционной системы семейства Windows; методов инсталляции системного программного обеспечения, а также режимов его взаимодействия с операционной системой; методов мониторинга компонентов операционной системы Windows, а также режимов отказоустойчивой конфигурации
	ИД-2ОПК-2 Устанавливает и удаляет операционную систему семейства Windows, развертывает службу каталогов Windows, а также настраивает роли сервера; устанавливает и удаляет системное программное обеспечение, запускает, останавливает и настраивает службы Windows, а также использует программный маршрутизатор на базе ОС Windows; диагностирует причины сбоев работоспособности операционной системы Windows с помощью системного программного	Предоставляет детальный отчёт с результатами установки и удаления операционной системы семейства Windows, развертывания службы каталогов Windows, а также настройки роли сервера; установки и удаления системного программного обеспечения, запуска, остановки и настройки службы Windows. А также результатами использования программного маршрутизатора на базе

	обеспечения.	ОС Windows; диагностики причин сбоев работоспособности операционной системы Windows с помощью системного программного обеспечения
	ИД-3ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.	Предоставляет детальный отчёт с демонстрацией способности применять программные средства системного и прикладного назначений, в том числе Отечественного производства, для решения задач профессиональной деятельности.
ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации, автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ИД-1ОПК-15 Выделяет этапы разработки политики информационной безопасности для организации; осуществляет поиск особенностей подсистем защиты ОС Windows и Linux; осуществляет систематизацию стандартных средств организации виртуальных частных сетей; определяет различия в особенностях применения хост-ориентированных и сеть-ориентированных систем обнаружения вторжений; выбирает стандартные схемы использования межсетевых экранов; выделяет особенности подсистем защиты, распространенных СУБД.	Предоставляет детальный отчет с полным пояснением, в котором демонстрирует этапы разработки политики информационной безопасности для организации, описывает особенности подсистем защиты ОС Windows и Linux; стандартные средства организации виртуальных частных сетей, показывает различия в особенностях применения хост-ориентированных и сеть-ориентированных систем обнаружения вторжений и демонстрирует стандартные схемы использования межсетевых экранов; особенности подсистем защиты распространенных СУБД.
	ИД-2ОПК-15 Оценивает эффективность и надежность защиты ОС, ВС и СУБД; планирует политику безопасности организации; выявляет слабости защиты ОС, ВС и СУБД использовать их для вскрытия защиты; организовывать защиту сегмента, подключаемого к открытым телекоммуникационным системам.	Предоставляет детальный отчет, в котором демонстрирует способность оценивать эффективность и надежность защиты ОС, ВС и СУБД; планировать политику безопасности организации, а также выявлять слабости защиты ОС, ВС и СУБД и использовать их для вскрытия защиты и организовывать защиту сегмента, подключаемого к открытым телекоммуникационным системам.
	ИД-3ОПК-15 Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации, автоматизированных систем, инструментальный мониторинг	Предоставляет детальный отчет с полным пояснением, в котором демонстрирует способность осуществлять администрирование и контроль функционирования средств

	защищенности автоматизированных систем.	и систем защиты информации, автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем
ОПК-7.1. Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем	ИД-1ОПК-7.1 Способен оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защите.	Предоставляет детальный отчет с полной оценкой информационных рисков в автоматизированных системах и определяет информационную инфраструктуру и информационные ресурсы, подлежащие защите.
	ИД-2ОПК-7.1 Формулирует угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в информационных системах.	Предоставляет детальный отчет с полной формулировкой угрозы безопасности, информационных воздействий, критериев оценки защищенности и методов защиты информации в информационных системах.
	ИД-3ОПК-7.1 Осуществляет навыки разработки и исследования аналитических и компьютерных моделей информационных систем и подсистем безопасности информационных систем.	Предоставляет детальный отчет в котором демонстрирует навыки разработки и исследования аналитических и компьютерных моделей информационных систем и подсистем безопасности информационных систем.

4. Объем учебной дисциплины и формы контроля *

Объем занятий: всего: 4 з.е. 144 акад.ч.	ОФО, в акад. часах
Контактная работа:	
Лекции/из них практическая подготовка	32/0
Лабораторных работ/из них практическая подготовка	48/0
Практических занятий/из них практическая подготовка	0
Самостоятельная работа	28
Формы контроля	
Экзамен **8 семестр**	36
Зачет	-
Зачет с оценкой	-
Курсовая работа	нет

* 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		
	8 СЕМЕСТР						
1.	**Исследование методов криптографической защиты данных (шифрование AES, RSA).** Практическое использование OpenSSL для шифрования/дешифрования. В рамках дисциплины «Исследование методов криптографической защиты данных» изучаются принципы и алгоритмы симметричного и асимметричного шифрования, такие как AES (Advanced Encryption Standard) и RSA (Rivest–Shamir–Adleman). Рассматриваются криптографические протоколы, методы генерации ключей, а также обеспечение целостности и аутентичности данных.	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	4.00	2.00	Защита лабораторной работы

2.	**Анализ стойкости парольной защиты (перебор хешей с помощью John the Ripper).** Исследование методов атак на хеши MD5, SHA-1, bcrypt. В рамках дисциплины «Анализ стойкости парольной защиты и методов атак на хеши» изучаются методы оценки надежности паролей и уязвимостей хеш-функций. Особое внимание уделяется использованию инструментов, таких как John the Ripper, для проведения атак методом перебора и взлома хешированных паролей.	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	4.00	2.00	Защита лабораторной работы
3.	**Настройка и тестирование межсетевого экрана (iptables/firewalld).** Создание правил фильтрации трафика, защита от DDoS. В рамках дисциплины «Настройка и тестирование межсетевого экрана (iptables/firewalld)» изучаются методы защиты сети путём настройки правил фильтрации входящего и исходящего трафика. Студенты обучаются созданию правил для разрешения или блокировки конкретных видов трафика, управлению доступом к сервисам и обеспечению безопасности сети.	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	4.00	2.00	Защита лабораторной работы

4.	**Исследование работы VPN (OpenVPN, WireGuar**d). Настройка защищенного туннеля, анализ трафика. В рамках курса «Исследование работы VPN (OpenVPN, WireGuard)» студенты изучают принципы работы виртуальных частных сетей, их преимущества и особенности реализации. Основное внимание уделяется настройке защищенных туннелей для безопасного обмена данными через публичные сети.	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	4.00	2.00	Защита лабораторной работы
5.	**Защита от сниффинга (анализ сетевого трафика в Wireshark, защита с помощью SSL/TLS).** Перехват и анализ незашифрованных данных. В рамках курса «Защита от сниффинга (анализ сетевого трафика в Wireshark, защита с помощью SSL/TLS)» студенты изучают методы обнаружения и предотвращения перехвата данных в сети. Основное внимание уделяется анализу сетевого трафика с помощью инструмента Wireshark, который позволяет выявлять незашифрованные и подозрительные передачи данных. .	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	4.00	2.00	Защита лабораторной работы

6.	**Изучение механизмов защиты от вредоносного ПО (антивирусы, песочницы).** Анализ поведения вирусов в изолированной среде. В рамках курса «Изучение механизмов защиты от вредоносного ПО (антивирусы, песочницы)» студенты осваивают основные принципы обнаружения и нейтрализации вредоносных программ. Особое внимание уделяется использованию антивирусных решений, их типам (сканеры, эвристические системы, базы данных сигнатур), а также технологиям изоляции и анализа подозрительных файлов.	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	4.00	2.00	Защита лабораторной работы
7.	**Исследование методов аутентификации (двухфакторная аутентификация, OTP, биометрия).** Настройка 2FA на примере Google Authenticator. В рамках курса «Исследование методов аутентификации (двухфакторная аутентификация, OTP, биометрия)» студенты изучают современные подходы к обеспечению безопасности при входе в системы и приложения	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	2.00	2.00	Защита лабораторной работы

8.	**Анализ уязвимостей веб-приложений (SQL-инъекции, XSS, CSRF).** Практическое тестирование с использованием Burp Suite. В рамках курса «Анализ уязвимостей веб-приложений» студенты изучают основные виды уязвимостей, такие как SQL-инъекции, XSS (Cross-Site Scripting) и CSRF (Cross-Site Request Forgery). Они осваивают методы обнаружения и эксплуатации этих уязвимостей, а также учатся использовать инструмент Burp Suite для практического тестирования веб-приложений: перехвата и анализа HTTP-запросов, выявления слабых мест и моделирования атак.	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	2.00	2.00	Защита лабораторной работы
9.	**Изучение систем обнаружения вторжений (Snort, Suricata).** Настройка IDS и анализ атакующих пакетов. В рамках курса «Изучение систем обнаружения вторжений» студенты знакомятся с такими инструментами, как Snort и Suricata, которые используются для мониторинга сетевого трафика и выявления возможных атак. Они изучают принципы работы систем IDS (систем обнаружения вторжений), их настройку и конфигурирование для эффективного обнаружения злоумышленнических действий.	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	2.00	2.00	Защита лабораторной работы

10.	**Защита данных на уровне жесткого диска (шифрование BitLocker, VeraCrypt).** Создание зашифрованных контейнеров и анализ устойчивости к взлому. В рамках курса «Защита данных на уровне жесткого диска» студенты изучают методы шифрования информации с помощью инструментов BitLocker и VeraCrypt, что позволяет обеспечить безопасность данных в случае утери или кражи устройства. Они осваивают процедуры включения шифрования, создание зашифрованных контейнеров и разделов для хранения конфиденциальной информации.	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	4.00	2.00	Защита лабораторной работы
11.	**Исследование методов защиты от фишинга (анализ поддельных писем, обучение пользователей).** Разработка тестового фишингового письма и его детекция. В рамках курса «Исследование методов защиты от фишинга» студенты изучают способы выявления и предотвращения фишинговых атак. Они анализируют признаки поддельных писем, такие как фальшивые ссылки, необычные отправители и подозрительный контент, а также обучают пользователей распознавать фишинговые сообщения для повышения общей информационной безопасности.	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	2.00	2.00	Защита лабораторной работы

12.	**Настройка и тестирование систем контроля доступа (SELinux, AppArmor).** Ограничение прав процессов, предотвращение эксплуатации уязвимостей. В рамках дисциплины «Настройка и тестирование систем контроля доступа» студенты изучают принципы работы систем безопасности на уровне операционной системы, такие как SELinux и AppArmor.	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	2.00	2.00	Защита лабораторной работы
13.	**Изучение аппаратных средств защиты (HSM, TPM-модули, смарт-карты).** Работа с аппаратными токенами для безопасного хранения ключей. В рамках дисциплины «Изучение аппаратных средств защиты» студенты знакомятся с различными аппаратными технологиями обеспечения безопасности, такими как аппаратные защищённые модули (HSM), TPM-модули и смарт-карты. Они осваивают принципы работы и области применения этих устройств для защиты криптографических ключей и других секретных данных.	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	2.00	2.00	Защита лабораторной работы

14.	**Анализ безопасности беспроводных сетей (взлом WPA2, защита WPA3).** В рамках курса по анализу безопасности беспроводных сетей студенты изучают уязвимости протоколов WPA2 и методы их эксплуатации, включая атаки типа "брютфорс", перехват и расшифровку трафика, а также методы взлома паролей. Особое внимание уделяется современным стандартам WPA3, их технологиям защиты и возможным уязвимостям, а также способам их устранения.	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	4.00	2.00	Защита лабораторной работы
15.	**Исследование методов защиты от атак типа "Человек посередине" (MITM).** Перехват трафика в локальной сети и защита с помощью сертификатов. В рамках дисциплины «Исследование методов защиты от атак типа "Человек посередине" (MITM)» студенты изучают техники осуществления атак типа «man-in-the-middle», а также методы их обнаружения и предотвращения. Они знакомятся с способами перехвата трафика в локальной сети, анализируют уязвимости протоколов и способов внедрения злоумышленников.	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	2.00	-	Защита лабораторной работы

16.	**Разработка и тестирование политик информационной безопасности (на основе ISO 27001, ГОСТ Р 57580).** Создание регламентов доступа, аудит защищенности системы. В рамках курса по разработке и тестированию политик информационной безопасности студенты изучают методы формирования эффективных документов на основе международного стандарта ISO 27001 и национальных нормативных актов, таких как ГОСТ Р 57580. Они создают политики безопасности, регламенты доступа, процедуры управления рисками и планы реагирования на инциденты, обеспечивающие комплексную защиту информационных ресурсов организации.	ОПК-2 ИД-1ОПК-2 ИД-2ОПК-2 ИД-3ОПК-2 ОПК-15 ИД-1ОПК-15 ИД-2ОПК-15 ИД-3ОПК-15 ОПК-7.1 ИД-1ОПК-7.1 ИД-2ОПК-7.1 ИД-3ОПК-7.1	2.00	-	2.00	-	Защита лабораторной работы
	ИТОГО за 8 семестр		**32.00**	**-**	**48.00**	**28.00**	
	ИТОГО		**32.00**	-	**48.00**	**28.00**	

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 «Программно-аппаратные средства 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. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2026. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0.
2. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8.
3. Программно-аппаратные средства защиты информации. В 3 частях. Ч. 1 : учебное пособие / Гриднев В. А., Губсков Ю. А., Дерябин А. С. [и др.]. - Тамбовский государственный технический университет, ЭБС АСВ, 2022. - ISBN 978-5-8265-2464-0, 978-5-8265-2467-1 (ч. 1).
4. Программно-аппаратные средства защиты информации. В 3 частях. Ч. 2 : учебное пособие / Гриднев В. А., Губсков Ю. А., Дерябин А. С. [и др.]. - Тамбовский государственный технический университет, ЭБС АСВ, 2023. - ISBN 978-5-8265-2464-0, 978-5-8265-2609-5 (ч. 2).
5. Программно-аппаратные средства защиты информации. В 3 частях. Ч. 3 : учебное пособие / Гриднев В. А., Губсков Ю. А., Дерябин А. С. [и др.]. - Тамбовский

государственный технический университет, ЭБС АСВ, 2024. - ISBN 978-5-8265-2795-5.
6. Казарин О. В., Забабурин А. С. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / Казарин О. В., Забабурин А. С. - М. : Юрайт, 2024. - 311 с. - (Высшее образование). - Библиогр. в конце глав. - ISBN 978-5-9916-9043-0.

8.1.2. Перечень дополнительной литературы:

1. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов ; под редакцией А. В. Душкина. — Москва : Горячая линия-Телеком, 2018. — 248 с. — ISBN 978-5-9912-0470-5.
2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2026. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2.
3. Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации / сост. Денисов И. А. - Московский технический университет связи и информатики, 2016.
4. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие для вузов / Душкин А. В., Барсуков О. М., Кравцов Е. В., Славнов К. В. ; ред. Душкин А. В. - М. : Горячая линия - Теклеком, 2016. - 247 с. : ил. - (Учебное пособие для вузов. Специальность). - ISBN 978-5-9912-0470-5.
5. Фомин Д. В. Защита информации: специализированные аттестованные программные и программно-аппаратные средства : практикум / Фомин Д. В. - Вузовское образование, 2021. - ISBN 978-5-4487-0795-7.

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

1. Методические указания по выполнению лабораторных работ по дисциплине "Программно-аппаратные средства защиты информации" (электронный ресурс) – Ставрополь, СКФУ, 2026.

2. Методические указания по организации и проведению самостоятельной работы по дисциплине "Программно-аппаратные средства защиты информации" (электронный ресурс) – Ставрополь, СКФУ, 2026.

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 «Программно-аппаратные средства 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

Лекционные занятия	Учебная аудитория для проведения занятий лекционного типа укомплектована специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: ноутбук, проектор. Учебно-наглядные пособия в виде тематических презентаций, соответствующих рабочим программам дисциплин.
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,

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

- 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 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.