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

УТВЕРЖДАЮ
Декан факультета
математики и компьютерных
наук имени профессора Н.И. Червякова
Гробова Т. А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Проектная деятельность и научно-исследовательская работа

Специальность	10.05.03 Информационная безопасность автоматизированных систем
Специализация	Анализ безопасности информационных систем
Год начала обучения	2024
Форма обучения	очная
Реализуется в семестрах	3-6

Разработано
Лапина М.А. - доцент кафедры вычислительной математики и кибернетики

Ставрополь

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Проектная деятельность и научно-исследовательская работа» является формирование у будущего специалиста по специальности 10.05.03 Информационная безопасность автоматизированных систем специализация «Анализ безопасности информационных систем» практических навыков проектной и исследовательской деятельности, включая разработку, анализ и внедрение решений в области информационной безопасности.

Задачи дисциплины:

- изучение методологии проектной и исследовательской работы в сфере информационной безопасности;
- формирование умений планирования, организации и выполнения ИБ-проектов с учетом современных технологий и стандартов;
- развитие навыков анализа угроз, уязвимостей и рисков в рамках исследовательских проектов;
- освоение методов обработки и представления результатов исследований, включая подготовку отчетов и презентаций;
- приобретение опыта командной работы и управления проектами в области информационной безопасности.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Проектная деятельность и научно-исследовательская работа» относится к части, формируемой участниками образовательных отношений дисциплинам (модулям) обязательной части. Ее освоение происходит в 3-6 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-8 Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	ИД-1ОПК-8 Знаком с перечнем сведений, относящихся к конфиденциальной информации и способы ее защиты; понятие и принцип электронной подписи (ЭП).	Обучающийся должен воспроизводить законодательно установленный перечень сведений, относящихся к конфиденциальной информации (персональные данные, коммерческая, служебная и иные тайны), а также базовое определение, виды (простая, усиленная) и принцип асимметричного шифрования электронной подписи. Обучающийся должен классифицировать конкретную информацию как конфиденциальную, выбирать адекватные организационные и технические способы её

		защиты (например, разграничение доступа, шифрование) и отличать юридически значимую электронную подпись от простой её имитации. Обучающийся должен демонстрировать навыки применения мер защиты к конфиденциальным сведениям в автоматизированных системах и использования инструментов электронной подписи для обеспечения целостности и неотказуемости документооборота.
	ИД-2ОПК-8 Проводит расчеты экономической эффективности внедрения конструкторских и технологических предложений; проводить анализ технического уровня и тенденций развития техники.	Обучающийся должен воспроизводить основные показатели экономической эффективности и методы анализа технического уровня техники; рассчитывать экономический эффект от внедрения конструкторских и технологических предложений с учётом затрат и выгод, а также проводить сопоставительный анализ разработок для выявления перспективных направлений; владеть навыками построения технико-экономического обоснования (ТЭО) и применения методик прогнозирования развития техники.
	ИД-3ОПК-8 Способен применять методы научных исследований при проведении разработок в области защиты патентной информации в автоматизированных системах.	Обучающийся должен перечислять основные эмпирические и теоретические методы научных исследований, а также виды патентной информации и типовые угрозы для неё в автоматизированных системах; применять выбранные методы (наблюдение, сравнение,

		моделирование) для анализа уязвимостей системы защиты патентных данных и оценки эффективности существующих мер; владеть навыками самостоятельной постановки исследовательской задачи, обработки результатов эксперимента и разработки предложений по усилению защиты патентной информации в автоматизированной среде.

4. Объем учебной дисциплины и формы контроля *

Объем занятий: всего: **13** з.е. 468 акад.ч.	ОФО, в акад. часах
Контактная работа:	
Лекции/из них практическая подготовка	32/0
Лабораторных работ/из них практическая подготовка	72/0 32/0 36/0 48/0
Практических занятий/из них практическая подготовка	0
Самостоятельная работа	248
Формы контроля	
Экзамен	-
Зачет	-
Зачет с оценкой	4,5,6 семестр

* 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		
	3 СЕМЕСТР						
1.	**Анализ цифровых следов в поведении пользователей онлайн-платформ** Исследование поведения пользователей и следов их активности на сайтах и в приложениях. В данной теме студентам предстоит исследовать цифровые следы, оставляемые пользователями онлайн-платформ. Особое внимание будет уделено анализу активности, поведения, истории запросов, логов и cookies. В конце изучения темы студент будет уметь выявлять закономерности и потенциальные риски, связанные с действиями пользователей.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	8.0	4.0	Собеседование
2.	**Анализ уязвимостей веб-приложения с использованием сканеров безопасности** Работа с автоматическими сканерами для поиска уязвимостей в веб-приложениях. В данной теме студентам предстоит изучить методы поиска	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	8.0	4.0	Собеседование

	уязвимостей в веб-приложениях с использованием автоматических сканеров безопасности. Особое внимание будет уделено настройке и применению инструментов типа Acunetix, OpenVAS, Nikto. В конце изучения темы студент будет уметь интерпретировать результаты сканирования и предлагать меры устранения уязвимостей.						
3.	**Разработка защищенного REST API на Node.js с авторизацией JWT** Создание API с безопасной авторизацией и передачей данных через токены. В данной теме студентам предстоит создать защищённый REST API на Node.js с применением авторизации JWT. Особое внимание будет уделено вопросам безопасной аутентификации, обработке токенов и защите маршрутов. В конце изучения темы студент будет уметь разрабатывать API, устойчивый к несанкционированному доступу.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	8.0	4.0	Собеседование
4.	**Анализ поведения вредоносного ПО в изолированной среде (sandbox)** Запуск вирусов в изоляции, изучение их действий и воздействия на систему. В данной теме студентам предстоит анализировать поведение вредоносного ПО в изолированной среде (sandbox). Особое внимание будет уделено использованию виртуализированных или контейнерных сред для безопасного запуска вредоносных программ. В конце изучения темы студент будет уметь фиксировать действия зловреда, оценивать его цели и методы воздействия на систему.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	8.0	4.0	Собеседование
5.	**Оценка стойкости паролей студентов с помощью алгоритмов перебора** Проверка сложности паролей с помощью утилит перебора и словарных атак. В данной теме студентам предстоит оценить стойкость паролей методом перебора. Особое внимание будет уделено использованию брутфорса и словарных атак с помощью таких инструментов, как Hashcat или John the	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	8.0	4.0	Собеседование

	Ripper. В конце изучения темы студент будет уметь проводить оценку надежности паролей и давать рекомендации по их усилению						
6.	**Разработка VPN-сервера и тестирование безопасности передачи данных** Настройка VPN и проверка защищенности передаваемой информации. В данной теме студентам предстоит настроить собственный VPN-сервер и протестировать безопасность передаваемых данных. Особое внимание будет уделено типам VPN-протоколов, настройке шифрования и анализу защищенности соединения. В конце изучения темы студент будет уметь организовать безопасный канал передачи данных через V	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	8.0	4.0	Собеседование
7.	**Использование SIEM-систем для мониторинга инцидентов ИБ** Анализ событий безопасности и выявление угроз через SIEM-систему. В данной теме студентам предстоит использовать SIEM-систему для мониторинга инцидентов информационной безопасности. Особое внимание будет уделено сбору логов, корреляции событий и выявлению потенциальных угроз. В конце изучения темы студент будет уметь настраивать и использовать SIEM для реагирования на инциденты.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8 ИД-3УК-6	-	-	8.0	4.0	Собеседование
8.	**Анализ сетевого трафика с использованием Wireshark** Захват и расшифровка сетевых пакетов, поиск подозрительной активности. В данной теме студентам предстоит анализировать сетевой трафик с помощью Wireshark. Особое внимание будет уделено захвату пакетов, расшифровке протоколов и поиску подозрительной активности. В конце изучения темы студент будет уметь выявлять признаки атак или нарушений в сетевом трафике.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	8.0	4.0	Собеседование
9.	**Защита от SQL-инъекций при работе с базами данных** Изучение и предотвращение SQL-инъекций в веб-приложениях.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8	-	-	8.0	4.0	Собеседование

	В данной теме студентам предстоит изучить методы защиты от SQL-инъекций при работе с базами данных. Особое внимание будет уделено использованию параметризованных запросов, ORM и валидации данных. В конце изучения темы студент будет уметь выявлять и устранять уязвимости, связанные с внедрением SQL-кода.	ИД-3 ОПК-8					
	ИТОГО за 3 семестр		-	-	**72.0**	**36.0**	
	4 СЕМЕСТР						
10.	**Создание honeypot-системы для сбора данных об атаках.** Изучение создания ловушек для фиксации активности злоумышленников. В данной теме студентам предстоит создать honeypot-систему для фиксации активности злоумышленников. Особое внимание будет уделено настройке ловушек, логированию и анализу атакующих действий. В конце изучения темы студент будет уметь разворачивать и использовать honeypot-системы для сбора информации о типах и источниках атак.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.00	10.0	Собеседование
11.	**Реализация многофакторной аутентификации для веб-приложения.** Внедрение дополнительных уровней защиты при авторизации пользователя. В данной теме студентам предстоит реализовать многофакторную аутентификацию в веб-приложении. Особое внимание будет уделено использованию одноразовых кодов, push-уведомлений, аппаратных токенов и биометрии. В конце изучения темы студент будет уметь повышать безопасность входа в систему за счёт дополнительных факторов.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.00	10.0	Собеседование
12.	**Анализ эффективности антивирусных систем на реальных примерах.** Сравнение возможностей различных антивирусных решений в условиях угроз. В данной теме студентам предстоит сравнить эффективность антивирусных решений в условиях моделируемых угроз. Особое внимание будет уделено	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.00	10.0	Собеседование

	обнаружению вредоносных файлов, реакциям в реальном времени и методам эвристического анализа. В конце изучения темы студент будет уметь выбирать подходящие средства защиты на основе их функциональности						
13.	**Оценка безопасности IoT-устройств в домашней сети.** Проверка уязвимостей умных устройств и маршрутизаторов. В данной теме студентам предстоит исследовать безопасность IoT-устройств в домашней сети. Особое внимание будет уделено обнаружению уязвимых интерфейсов, слабых паролей и отсутствию обновлений. В конце изучения темы студент будет уметь выявлять риски и предлагать меры по защите умных устройств.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.00	10.0	Собеседование
14.	**Исследование фишинговых атак: как студенты реагируют на подозрительные письма.** Оценка уровня осведомлённости и реакции на фишинговые сообщения. В данной теме студентам предстоит провести исследование фишинговых атак, оценив реакцию на подозрительные письма. Особое внимание будет уделено созданию реалистичных фишинговых сообщений и анализу поведенческих паттернов. В конце изучения темы студент будет уметь оценивать уровень фишинговой грамотности пользователей.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.00	10.0	Собеседование
15.	**Разработка собственного шифра и его криптоанализ.** Создание простого алгоритма шифрования и проверка его стойкости. В данной теме студентам предстоит разработать собственный алгоритм шифрования и провести его криптоанализ. Особое внимание будет уделено структуре алгоритма, устойчивости к перебору и атакам по выбранному открытому тексту. В конце изучения темы студент будет уметь проектировать и анализировать простые криптографические схемы.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.00	10.0	Собеседование
16.	**Анализ цифровых подписей и проверка подлинности документов.**	ОПК-8 ИД-1 ОПК-8	-	-	4.00	10.0	Собеседование

	Работа с ЭЦП и проверка достоверности передаваемых данных. В данной теме студентам предстоит проанализировать работу цифровых подписей и проверку подлинности документов. Особое внимание будет уделено механизмам ЭЦП, структуре сертификатов и алгоритмам проверки. В конце изучения темы студент будет уметь подписывать документы, проверять подписи и интерпретировать результаты верификации.	ИД-2 ОПК-8 ИД-3 ОПК-8					
17.	**Реализация системы логирования и аудита действий пользователей.** Настройка отслеживания и анализа действий в системе. В данной теме студентам предстоит реализовать систему логирования и аудита действий пользователей. Особое внимание будет уделено отслеживанию критических событий, созданию журналов и анализу активности. В конце изучения темы студент будет уметь обеспечивать прозрачность действий в системе и выявлять нарушения.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.00	6.0	Собеседование
	ИТОГО за 4 семестр		**-**	**-**	**32.0**	**76.0**	
	5 СЕМЕСТР						
18.	**Создание прототипа приложения с защищенным хранилищем данных.** Разработка системы безопасного хранения информации. В данной теме студентам предстоит создать прототип приложения с защищённым хранилищем данных. Особое внимание будет уделено выбору механизмов шифрования, защите от несанкционированного доступа и безопасному хранению ключей. В конце изучения темы студент будет уметь разрабатывать приложения, соблюдающие базовые требования к безопасности хранения информации.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.0	8.0	Собеседование
19.	**Сравнительный анализ современных алгоритмов хеширования.** Изучение алгоритмов SHA, Bcrypt, Argon2 и оценка их надёжности. В данной теме студентам предстоит провести сравнительный анализ современных алгоритмов	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.0	8.0	Собеседование

	хеширования, включая SHA-2, Bcrypt, Argon2. Особое внимание будет уделено скорости, устойчивости к атакам перебора и применимости для защиты паролей. В конце изучения темы студент будет уметь выбирать хеш-функции в зависимости от задач и рисков.						
20.	**Оценка защищенности локальной сети учебного заведения.** Проверка безопасности сети и поиск уязвимых точек. В данной теме студентам предстоит оценить защищённость локальной сети учебного заведения. Особое внимание будет уделено анализу сетевой архитектуры, настройке межсетевых экранов, наличию открытых портов и слабых точек. В конце изучения темы студент будет уметь проводить базовый аудит безопасности сетевой инфраструктуры.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.0	8.0	Собеседование
21.	**Исследование вредоносных расширений браузера.** Анализ опасных дополнений и их воздействие на систему. В данной теме студентам предстоит исследовать вредоносные расширения браузера. Особое внимание будет уделено способам обхода защиты, сбору персональных данных и внедрению вредоносного кода в веб-страницы. В конце изучения темы студент будет уметь выявлять потенциально опасные расширения и оценивать риски.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.0	8.0	Собеседование
22.	**Реализация модели RBAC (Role-Based Access Control) в веб-приложении.** Внедрение системы распределения прав доступа по ролям. В данной теме студентам предстоит реализовать модель разграничения прав доступа на основе ролей (RBAC) в веб-приложении. Особое внимание будет уделено созданию ролей, определению прав и настройке логики авторизации. В конце изучения темы студент будет уметь разрабатывать систему управления доступом на основе ролевой модели.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.0	8.0	Собеседование
23.	**Исследование атак типа Man-in-the-Middle и способов защиты.** Проведение атак перехвата и изучение методов их предотвращения.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.0	8.0	Собеседование

	В данной теме студентам предстоит провести исследование атак типа Man-in-the-Middle и изучить методы защиты от них. Особое внимание будет уделено перехвату трафика, подделке сертификатов и использованию HTTPS и VPN как средств защиты. В конце изучения темы студент будет уметь моделировать MITM-атаки и применять меры противодействия.						
24.	**Анализ поведения пользователей при установке мобильных приложений.** Исследование рисков, связанных с разрешениями и личными данными. В данной теме студентам предстоит проанализировать поведение пользователей при установке мобильных приложений. Особое внимание будет уделено анализу запрашиваемых разрешений, доступа к личным данным и уровня цифровой грамотности пользователей. В конце изучения темы студент будет уметь оценивать риски, связанные с использованием мобильного ПО.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.0	8.0	Собеседование
25.	**Обзор и тестирование инструментов для обеспечения приватности в интернете.** Изучение VPN, Tor и анти-трекеров в действии. В данной теме студентам предстоит протестировать инструменты, обеспечивающие приватность в интернете: VPN, Tor, анти-трекеры. Особое внимание будет уделено защите от слежки, сохранению анонимности и ограничению утечек данных. В конце изучения темы студент будет уметь выбирать и применять технологии приватности в различных сценариях.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.0	8.0	Собеседование
26.	**Разработка защищённого мессенджера на Python с end-to-end шифрованием.** Создание мессенджера с защитой от перехвата переписки. В данной теме студентам предстоит разработать защищённый мессенджер на Python с реализацией end-to-end шифрования. Особое внимание будет уделено защите сообщений, генерации ключей и проверке подлинности участников. В конце изучения темы студент будет уметь	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	-	-	4.0	8.0	Собеседование

	создавать приложения, защищённые от перехвата переписки.						
	ИТОГО за 5 семестр		-	-	**36.0**	**72.0**	
	6 СЕМЕСТР						
27.	**Анализ безопасности облачных хранилищ (Google Drive, Dropbox и др.).** Сравнение механизмов защиты в популярных облачных сервисах. В данной теме студентам предстоит провести анализ безопасности облачных хранилищ, таких как Google Drive, Dropbox и другие. Особое внимание будет уделено механизмам шифрования, управлению доступом, защите при передаче и хранении данных. В конце изучения темы студент будет уметь сравнивать облачные сервисы по уровню безопасности и оценивать риски их использования.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	2.0	-	6.0	8.0	Собеседование
28.	**Использование биометрической аутентификации: плюсы и риски.** Оценка надёжности биометрии и возможных угроз. В данной теме студентам предстоит изучить возможности и риски биометрической аутентификации. Особое внимание будет уделено технологиям распознавания отпечатков пальцев, лица и радужной оболочки, а также угрозам подделки и утечки биометрических данных. В конце изучения темы студент будет уметь оценивать надёжность биометрических методов и их применимость.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	4.0	-	6.0	8.0	Собеседование
29.	**Разработка расширения для браузера, блокирующего трекеры и рекламу.** Создание собственного инструмента повышения конфиденциальности. В данной теме студентам предстоит разработать расширение для браузера, блокирующее трекеры и рекламные элементы. Особое внимание будет уделено принципам работы web-трекеров, методам их обнаружения и скрытия. В конце изучения темы студент будет уметь создавать расширения, повышающие конфиденциальность пользователя в сети.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	4.0	-	6.0	8.0	Собеседование

30.	**Тестирование защищенности Wi-Fi сети с использованием Aircrack-ng.** Взлом пароля Wi-Fi и анализ методов защиты. В данной теме студентам предстоит протестировать защищённость Wi-Fi-сети с использованием инструментария Aircrack-ng. Особое внимание будет уделено методам перехвата пакетов, взлому WPA-ключей и способам усиления безопасности. В конце изучения темы студент будет уметь оценивать уязвимость беспроводных сетей и предлагать меры защиты.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	4.0	-	6.0	8.0	Собеседование
31.	**Создание keylogger'a и защита от него.** Демонстрация способа сбора вводимой информации и способов защиты. В данной теме студентам предстоит создать простейший keylogger и изучить способы защиты от подобных угроз. Особое внимание будет уделено методам скрытого отслеживания ввода и техникам обнаружения и блокировки шпионских программ. В конце изучения темы студент будет уметь выявлять вредоносные программы, собирающие пользовательскую информацию.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	4.0	-	6.0	8.0	Собеседование
32.	**Анализ цифровых следов в соцсетях: что о нас может узнать злоумышленник?** Поиск открытой информации о пользователях через соцсети В данной теме студентам предстоит проанализировать цифровые следы, оставляемые пользователями в социальных сетях. Особое внимание будет уделено открытым данным, лайкам, геометкам, контактам и другим атрибутам, позволяющим злоумышленнику получить личную информацию. В конце изучения темы студент будет уметь проводить OSINT-исследования и оценивать риски цифровой экспозиции.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	4.0	-	6.0	8.0	Собеседование
33.	**Исследование кибербуллинга и механизмов его предотвращения.** Изучение методов цифровой травли и путей противодействия.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	4.0	-	6.0	8.0	Собеседование

	В данной теме студентам предстоит исследовать феномен кибербуллинга, методы его распространения и существующие способы защиты. Особое внимание будет уделено изучению платформ, где травля наиболее активна, и мерам реагирования. В конце изучения темы студент будет уметь распознавать признаки кибербуллинга и предлагать эффективные меры противодействия.						
34.	**Анализ инцидентов с ИБ в крупнейших компаниях (например, Uber, Sony).** Разбор утечек данных, хакерских атак и их последствий. В данной теме студентам предстоит провести анализ крупных инцидентов информационной безопасности, таких как утечки в Uber, Sony, LinkedIn. Особое внимание будет уделено причинам произошедшего, уязвимостям, последствиям и принятым мерам. В конце изучения темы студент будет уметь разбирать ИБ-инциденты и формулировать рекомендации по снижению подобных рисков.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	4.0	-	4.0	8.0	Собеседование
35.	**Использование CAPTCHA и её устойчивость к ботовым атакам.** Проверка надёжности капчи как метода защиты от автоматизированных действий. В данной теме студентам предстоит изучить механизм CAPTCHA и его эффективность против ботов. Особое внимание будет уделено различным типам капчи, методам автоматического обхода и средствам повышения устойчивости. В конце изучения темы студент будет уметь оценивать надёжность CAPTCHA и подбирать подходящие решения для защиты веб-сервисов.	ОПК-8 ИД-1 ОПК-8 ИД-2 ОПК-8 ИД-3 ОПК-8	2.0	-	2.0	2.0	Собеседование
36.	**ИТОГО за 6 семестр**		**32.0**	**-**	**48.0**	**64.0**	
37.	**ИТОГО**		**32.0**	**-**	**188.0**	**248.0**	

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 «Проектная деятельность и научно-исследовательская работа» 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. Пушина Н. В. Основы проектной и исследовательской деятельности. Практикум : учебное пособие для СПО / Н. В. Пушина, Ж. В. Морозова, Г. А. Бандура. - 3-е изд., стер. - Санкт-Петербург: Лань, 2023. - 152 с. : ил. - Текст : непосредственный.
2. Хамидулин, В. С. Основы проектной деятельности / В. С. Хамидулин. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 144 с. — ISBN 978-5-507-44208-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/214844
3. *Сладкова, О. Б.* Основы научно-исследовательской работы : учебник и практикум для вузов / О. Б. Сладкова. — Москва : Издательство Юрайт, 2025. — 154 с. — (Высшее образование). — ISBN 978-5-534-15305-7.

8.1.2. Перечень дополнительной литературы:

1. Кунилова О. В. Индивидуальный проект. Проектно-исследовательская деятельность. – 2021.
2. *Зуб, А. Т.* Управление проектами : учебник и практикум для вузов / А. Т. Зуб. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 397 с. — (Высшее образование). — ISBN 978-5-534-17500-4

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

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Проектная деятельность и научно-исследовательская работа». Ставрополь : СКФУ, 2023.
2. Методические указания к практическим занятиям по дисциплине «Проектно-исследовательский практикум». Ставрополь : СКФУ, 2025.

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 «Проектно-исследовательский практикум»

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

При чтении лекций используется компьютерная техника, демонстрации презентационных мультимедийных материалов. На практических занятиях студенты защищают отчеты по работам, которые они выполняют самостоятельно или в команде с применением компьютерной техники и Интернет-технологий

Информационные справочные системы:

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

1	https://www.garant.ru/
2	http://www.consultant.ru/

Программное обеспечение:

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

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

Лабораторные занятия	Учебная аудитория для проведения учебных занятий, оснащенная мультимедийным оборудованием и техническими средствами обучения.
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 (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 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.