РУКОН ЦЕЛЬ
МНОГОПРОФИЛЬНЫЙ ЦЕНТР КВАЛИФИКАЦИЙ

Автономная некоммерческая организация
дополнительного профессионального образования
«Многопрофильный центр квалификаций «Цель»

УТВЕРЖДАЮ
Директор АНО ДПО «МЦК «Цель»

_____
О. В. Самоварова

Одобрена на заседании
педагогического совета
Протокол № от «07» июля 2025 г.

Приказ № п/2025-БО
от «07» июля 2025 г.

Дополнительная общеобразовательная

общеразвивающая программа

«Этичный хакинг: миг уникальности»

(148 акад. час.)

Автор-составитель:

1. Пантелеев С.В., канд. тех. наук
2. Рыбалёва И.А., канд. пед. наук

г. Санкт-Петербург, 2025 г.

Дополнительная общеобразовательная общеразвивающая программа технической направленности

«Этичный хакинг: миг уникальности»

1. Об организации

Наименование поля	Значение поля
ИНН организации, осуществляющей образовательную деятельность	7728470220
Наименование организации	Автономная некоммерческая организация дополнительного профессионального образования «Многопрофильный центр квалификаций «Цель»
Логотип организации	
Ссылка на логотип организации	https://static.tildacdn.com/tild3234-3932-4162-b930-373132666433/tsel-logo.svg
Контакты ответственного за программу (с указанием фамилии, имени, отчества)	Рыбалёва Ирина Александровна
Контакты ответственного за программу.	

Должность	Методист
Контакты ответственного за программу. Телефон	+7 (961) 522-60-40
Контакты ответственного за программу. E-mail	Ribaleva@ya.ru

2. Пояснительная записка

Наименование поля	**Значение поля (примеры)**
Название программы (курса)	«Этичный хакинг: миг уникальности»
Уровень сложности ДОП	Продвинутый уровень. Продвинутый уровень обучения требует специализированных навыков и умений от Получателей поддержки и предполагает использование практико-ориентированного учебного материала, а также углубленное изучение содержания ДОП, ориентированной в большей части на алгоритмическое программирование, структуры данных, участие в профильных олимпиадах и соревнованиях.
Целевая аудитория/ категория обучающихся (для которого будет актуальным обучение по ДОП	Школьники 8-11 классов и обучающиеся по программам среднего профессионального образования по профессиям и (или) специальностям, включенным в Перечень профессий и специальностей среднего профессионального образования в области информационных технологий Входные требования к Получателям поддержки: уверенное владение одним из современных языков программирования и знание основ ООП; Получатель поддержки должен уметь писать

	программы начальной и средней сложности, использовать стандартные структуры данных и библиотеки, знать основы объектно-ориентированного подхода, иметь опыт решения классических задач по программированию и прикладных задач.
Описание программы	Дополнительная общеобразовательная программа «Этичный хакинг: миг уникальности» (продвинутый уровень) направлена на углубленное изучение языка программирования Python с применением технологий искусственного интеллекта и освоение продвинутых возможностей с ИИ, на освоение типовых библиотек и фреймворков, решение прикладных задач повышенной сложности, формирование базовых навыков командной разработки и использования профессиональных инструментов, а также на формирование комплексного понимания методов обеспечения информационной безопасности и противодействия различным типам атак на информационные системы с использованием технологий искусственного интеллекта. Программа состоит из 4 модулей, каждый из которых включает теоретические занятия, практические работы и самостоятельные задания: 1 модуль «Продвинутое программирование на Python с ИИ», где рассматриваются декораторы, генераторы, многопоточность, работа с базами данных (SQLite), разработка GUI (PyQt/Kivy) и совершенствуются навыки создании оптимизированных алгоритмов, интеграции ИИ для автоматизации задач; 2 модуль «Защита от сетевых атак с применением ИИ», где рассматриваются анализ трафика (Wireshark, Nmap), ARP-атаки, VPN/IPsec, защита от DDoS и на практических занятиях совершенствуются навыки разработки сканеров уязвимостей и систем мониторинга сетевой безопасности; 3 модуль Программы «Безопасность веб-приложений с применением ИИ» ориентирован на изучение и освоение методов обеспечения безопасности веб-приложений с использованием технологий искусственного интеллекта и отработку навыков по разработке и аналиуз веб-приложений на предмет уязвимостей (SQL-инъекции, XSS, CSRF) с использованием инструментов сканирования и эксплуатации, на создание систем фильтрации и санитизации пользовательского ввода для защиты от атак, реализацию безопасных механизмов работы с базами данных через параметризованные запросы и подготовленные выражения, проектирование защищенных систем аутентификации и управления сессиями с применением шифрования и подписи, а также разработку рекомендаций и отчетов по обеспечению безопасности веб-приложений на основе стандартов OWASP и других методологий. 4 модуль

	Программы «Комплексная безопасность информационных систем с применением ИИ» совершенствует навыки в освоении методов цифровой экспертизы и анализа киберинцидентов, приобретение навыков разработки мер защиты от манипулятивных атак (социальная инженерия, фишинг) с использованием ИИ, умение анализировать и обходить системы защиты для выявления уязвимостей, создание инструментов на Python для тестирования безопасности систем, разработку безопасных механизмов аутентификации и авторизации с применением шифрования данных, а также проектирование защищенных систем с учетом принципов конфиденциальности и целостности данных. Содержание Программы продвинутого уровня предполагает углубленное изучение сложных алгоритмов и структур данных, формирование навыков решения задач по оптимизации кода, освоение продвинутых подходов к проектированию и разработке больших и сложных систем. На практических занятиях, начиная с первого модуля педагогами-наставниками отрабатывается навык решения задач олимпиадного уровня сложности, материал занятий, формы, методы и приемы обучения ориентированы на подготовку учащихся к профильным олимпиадам и соревнованиям. Программа способствует ранней профориентации в сфере IT-безопасности и формирует навыки, востребованные в профессиях будущего. Обучение осуществляется очно с применением дистанционных образовательных технологий и электронного обучения. Программа рассчитана на нормативную трудоемкость обучения – 148 академических часа, включая все виды аудиторной (теоретические и практические занятия) и внеаудиторной (самостоятельной) работы учащихся. Программа состоит из 4 модулей по 36 академических часов. Прохождение каждого модуля завершается промежуточной аттестацией в форме тестирования. Программа носит практико-ориентированный характер, 56 % от общего объема Программы (84 ак.ч.) отводится на отработку практических навыков и умений на практических занятиях под руководством опытных преподавателей-наставников.
Аннотация программы	Программа «Этичный хакинг: миг уникальности» (продвинутый уровень) ориентирована на углубленное изучение кибербезопасности, программирования на Python и применения ИИ

	для защиты данных. Программа состоит из 4 модулей, каждый из которых включает теоретические и практические занятия, а также самостоятельную работу. Содержание программы направлено на изучение продвинутых методов ИИ (нейросети в кибербезопасности), разбор и анализ реальных кейсов (анализ утечек данных, защита IoT-устройств); участие в CTF-соревнованиях и хакатонах. Модули в Программе логически выстроены, взаимосвязаны, образуют единую систему, где каждый элемент усиливает и развивает предыдущий. Это позволяет учащимся не просто получать разрозненные знания, а формировать целостную экспертизу в области кибербезопасности и ИИ. Программа практико-ориентирована, так как 84 ак.ч. (56%) отводится на отработку практических навыков и умений через практические занятия и 24 ак.ч. (16%) отводится на самостоятельную работу учащихся, где также совершенствуются навыки продвинутых возможностей Python с применением ИИ, идет углубленное изучение кибербезопасности, программирования на Python и используются профессиональные инструменты.
Цель программы	углубленное изучение кибербезопасности, программирования на Python и применения ИИ для защиты данных, освоение типовых библиотек и фреймворков, решение прикладных задач повышенной сложности, формирование базовых навыков командной разработки и использования профессиональных инструментов
Задачи программы	*Обучающие:* ➢ изучение и освоение продвинутых возможностей языка программирования Python с применением технологий искусственного интеллекта; ➢ изучение методов анализа и защиты сетевых протоколов, предотвращения сетевых атак и обеспечения безопасности сетевых ресурсов с использованием технологий искусственного интеллекта; ➢ изучение и освоение методов обеспечения безопасности веб-приложений с использованием технологий искусственного интеллекта; ➢ формирование комплексного понимания методов обеспечения информационной безопасности и противодействия различным типам атак на информационные системы с использованием технологий искусственного интеллекта.

	Развивающие: ➢ развитие критического мышления, аналитических способностей и креативности: разбор реальных кейсов утечек данных; оценка рисков и уязвимостей; разбор реальных кейсов утечек данных; создание собственных инструментов для пентеста; ➢ развитие алгоритмического мышления: проектирование решений для защиты систем; оптимизация кода для анализа данных; ➢ развитие познавательной активности школьников: поиск и выделение необходимой информации, структурирование знаний, самостоятельное создание алгоритмов деятельности при решении проблем творческого и поискового характера; ➢ развитие регулятивных умений: ставить цели, планировать собственную деятельность и способы достижения результата, осуществлять контроль и коррекцию деятельности); ➢ развитие коммуникативных умений: планирование учебного сотрудничества, умение полно и точно выражать свои мысли в соответствии с задачами коммуникации и прочее; ➢ развитие технических способностей обучающегося, логики, внимания, памяти, воображения, мотивации к дальнейшему изучению программирования. *Воспитательные:* ➢ привитие этических норм работы в IT-сфере: понимание границ этичного хакинга; ответственность за использование знаний; ➢ формирование практических навыков цифровой гигиены: безопасное поведение в сети; защита персональных данных; ➢ создание условий ранней профориентации в сфере IT- технологий для профессионального самоопределения учащихся; ➢ формирование у учащихся самостоятельности, ответственности, социальной активности.
Актуальность	Актуальность ДОП. Программа «Этичный хакинг: миг уникальности» не только соответствует актуальным запросам времени, но и опережает стандартные школьные курсы, готовит учащихся к профильным олимпиадам и соревнованиям, способствует ранней профориентации в сфере IT-безопасности и формирует навыки, востребованные в профессиях будущего, то новое поколение IT-специалистов, способных обеспечивать безопасность цифрового пространства России. Спрос

	на специалистов по кибербезопасности растет с каждым годом. Даже базовые навыки этичного хакинга открывают двери в перспективные профессии: пентестер (тестирует системы на взлом); кибербезопасник (защищает компании от атак); разработчик защищенных систем. Цифровой мир — это реальность, в которой мы живем. Соцсети, онлайн-платежи, умные устройства — всё это требует защиты. Хакерские атаки, утечки данных и мошенничество в интернете происходят каждый день. Ребенок с раннего возраста уже активно пользуется технологиями — значит, ему жизненно важно понимать, как защитить себя и свои данные. Уникальность программы заключается в синтезе программирования, кибербезопасности и ИИ в рамках одного курса с акцентом на этичное применение знаний. Программа разработана в соответствии с требованиями ФЗ «Об образовании в РФ» и профессиональными стандартами IT-отрасли. Отличительные особенности ДОП заключаются в том, что работа с реальными кейсами утечек данных и атак дает глубокое погружение в реальные задачи кибербезопасности; программирование + ИИ + Безопасность — уникальная комбинация: автоматизация взлома и защиты с помощью Python и нейросетей; разработка собственных сканеров уязвимостей; акцент на легальный хакинг и этику: только «белые» методы взлом –как находить уязвимости и закрывать их, а не использовать во вред, а также **разбор** реальных судебных дел о хакерах — почему важно оставаться в правовом поле. Также практико-ориентированные занятия, командная работа, исследование и работа над проектом, развивают, формируют и совершенствуют надпрофессиональные компетенции учащихся (Soft skills + Future skills): системное мышление (анализ киберугроз как сложных систем (связь техники, психологии, экономики); креативность (CTF-соревнования с нестандартными задачами (например, взлом IoT-чайника); эмоциональный интеллект (ролевые игры: «Жертва хакерской атаки» → обучение эмпатии); управление проектами (Agile-подход в разработке защитных систем (Scrum-доски в GitHub); когнитивная гибкость (экспресс-адаптация к новым угрозам (например, генерация защиты против Zero-day уязвимости); цифровая этика (дебаты: «Границы этичного хакинга» с юристами). Надпрофессиональные компетенции, формируемые в рамках данного Комплекта ДОП, востребованы в 2025+ гг. согласно Атласу новых профессий: киберпсихолог → эмоциональный интеллект + цифровая этика; архитектор цифровых платформ → системное мышление + управление проектами,

	дизайнер кибербезопасности → креативность + когнитивная гибкость. Новизна ДОП заключается в синтезе современных технологий (Python + ИИ). Программа объединяет три актуальных направления в одном курсе: ➢ этичный хакинг (безопасность вместо взлома); ➢ программирование на Python (доступный язык для начинающих); ➢ искусственный интеллект. Также в Программе в рамках образовательного процесса предполагается система наставничества «Ученик → Ученик». Формат: учащиеся продвинутого уровня Программы становятся менторами для учащихся Программы начального уровня: проводят ежемесячные разборы задач (например, помощь в написании первого сканера портов); организуют Q&A-сессии по основам Python, а учащиеся базового уровня участвует в роли ассистентов. Так, к примеру, команда из 3 уровней Программы совместно разрабатывает «этичный вирус» (продвинутые пишут код, базовые тестируют, начинающие документируют уязвимости). Эффекты от такого взаимодействия очевидны: для учащихся начального уровня: получают поддержку и видят перспективы роста; учащиеся базового уровня развивают лидерские навыки, а учащиеся продвинутого уровня учатся управлять проектами. Также предполагается наставничество в подготовке к внутреннему Хакатону, а также к иным образовательным активностям, к примеру «Созданию сквозных кейсов», где выходные данные одного уровня становятся входными для другого: начальный уровень: собирает статистику утечек паролей; базовый уровень: пишет скрипт для проверки их сложности, а продвинутый уровень: обучает нейросеть предсказывать уязвимые комбинации. Итог: единый отчет с рекомендациями для школы. Инструменты поддержки взаимодействия: цифровая платформа: общий чат в Telegram с каналами по уровням и GitHub-организация с репозиториями проектов. Таким образом, реализуется комплексный подход с упором на практическое применение ИИ в этичном хакинге. Это не просто курс по программированию, а первый шаг в профессию будущего с акцентом на этику.
Дополнительная информация	Дополнительная общеобразовательная программа разработана с учетом требований актуальных нормативных правовых актов и иных документов: ➢ Федерального закона от 29 декабря 2012 г. № 273 «Об образовании в Российской

	Федерации»; ➢ Постановления Правительства Российской Федерации от 11 октября 2023 г. № 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»; ➢ Приказа Министерства просвещения Российской Федерации от 27 июля 2022 г. № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»; ➢ Постановления Главного государственного санитарного врача Российской Федерации от 28 сентября 2020 г. № 28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодёжи»; ➢ Постановления Главного государственного санитарного врача Российской Федерации от 28 января 2021 г. № 2 «Об утверждении санитарных правил и норм СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания»; ➢ Приказа Министерства просвещения Российской Федерации от 28 ноября 2024 г. № 838 «Об утверждении перечня средств обучения и воспитания, соответствующих современным условиям обучения, необходимых при оснащении общеобразовательных организаций в целях реализации мероприятий государственной программы Российской Федерации «Развитие образования», направленных на содействие созданию (создание) в субъектах Российской Федерации новых (дополнительных) мест в общеобразовательных организациях, модернизацию инфраструктуры общего образования, школьных систем образования, критериев его формирования и требований к функциональному оснащению общеобразовательных организаций».
Формат обучения	Очная форма с применением дистанционных образовательных технологий, в том числе с применением средств электронного обучения

Уровень сложности	Продвинутый
Срок освоения образовательной программы	148 ак. ч.
Объем каждого модуля в ак.ч.	36
Объем часов в неделю в ак.ч.	4-6
Количество занятий	84
Направленность программы	Современные языки программирования
Язык программирования	Python
Дополнительная общеобразовательная программа не представлена для участия в иных федеральных проектах, направленных на дополнительное образование граждан, кроме федерального проекта «Развитие кадрового потенциала ИТ- отрасли»	Не представлена

Дополнительная общеобразовательная программа не была реализована до начала отбора и/или не реализовывается в период отбора на безвозмездной основе	Не реализована
Категория обучающихся по программе	Школьники 8-11 классов и обучающиеся по программам среднего профессионального образования по профессиям и (или) специальностям, включенным в Перечень профессий и специальностей среднего профессионального образования в области информационных технологий
Описание планируемых результатов обучения	<u>В результате освоения программы выпускники будут знать:</u> ➢ продвинутые возможности Python с применением ИИ; ➢ методы анализа и защиты сетевых протоколов; ➢ технологии искусственного интеллекта для автоматизации процессов обнаружения уязвимостей, анализа сетевого трафика и защиты сетевых ресурсов; ➢ методы обнаружения и защиты от основных уязвимостей веб-приложений (SQL-инъекции, XSS, CSRF); ➢ стандарты безопасности (OWASP Top 10) и методы противодействия атакам через валидацию данных, фильтрацию входных параметров, использование токенов CSRF и HTTP-заголовков; ➢ методы цифровой экспертизы и анализа киберинцидентов; <u>Выпускники будут уметь:</u> ➢ работать с файлами и базами данных SQLite, включая использование контекстного менеджера и выполнение SQL-запросов; ➢ освоят принципов многопоточного и параллельного программирования с использованием модулей threading и multiprocessing; ➢ разрабатывать графические интерфейсы с помощью библиотек PyQt и Kivy и применения технологий искусственного интеллекта для создания программного обеспечения; ➢ работать с инструментами для сканирования портов и анализа трафика (Nmap,

	Wireshark; ➢ выявлять и предотвращать сетевые атаки (ARP-атаки, сниффинг, DoS/DDoS); ➢ разрабатывать программы на Python для мониторинга сетевой безопасности, настройки брандмауэров и управления VPN-соединениями с использованием IPsec; ➢ разрабатывать скрипты на Python для поиска и эксплуатации уязвимостей с использованием ИИ; ➢ создавать системы фильтрации и санитизации пользовательского ввода, разрабатывать защищенные базы данных через параметризацию запросов и подготовленные выражения, проектировать безопасные системы аутентификации и управления сессиями с применением шифрования и подписи; ➢ разрабатывать меры защиты от манипулятивных атак (социальная инженерия, фишинг) с использованием ИИ; ➢ анализировать и обходить системы защиты для выявления уязвимостей, создавать инструменты на Python для тестирования безопасности систем, разрабатывать безопасные механизмы аутентификации и авторизации с применением шифрования данных; ➢ проектировать защищенные системы с учетом принципов конфиденциальности и целостности данных.
Ссылка на лендинг Образовательной программы	
Ссылка на LMS	
Страница обучения на курсе	
Дополнительная информация о ДОП	Перечень обязательных для выполнения каждым Получателем поддержки работ/контрольных точек по каждому модулю Программы и по Программе в целом:

	➢ в рамках текущего контроля обязательные к выполнению задания самостоятельной работы (4 по каждому модулю), т.е. 16 контрольных точек являются обязательными активностями; ➢ в рамках промежуточного контроля обязательные к выполнению тестовые задания (1 тест по каждому модулю), т.е. 4 контрольных точек являются обязательными активностями; ➢ в рамках итогового контроля обязательные к выполнению проект, т.е. 1 контрольная точка является обязательной активностью. Таким образом, по Программе 21 образовательные активности являются контрольными точками, т.е. обязательными к выполнению каждым Получателем поддержки.

Цели, задачи, планируемые результаты обучения и типы задач по каждому модулю Программы

Название модуля	Общая цель модуля	Планируемые результаты обучения по модулю	Типы задач/деятельности (примеры)
Модуль 1. Продвинутое программирование на Python с ИИ	Изучение и освоение продвинутых возможностей языка программирования Python с применением технологий искусственного интеллекта.	Освоение продвинутых возможностей Python, таких как работа с декораторами, генераторами, метаклассами, множественным наследованием и дескрипторами, приобретение навыков работы с файлами и базами данных SQLite, включая использование контекстного менеджера и выполнение SQL-запросов, освоение принципов многопоточного и параллельного программирования с использованием модулей threading и multiprocessing, а также получение практических	Программные решения с использованием продвинутых возможностей Python, включая создание декораторов и генераторов для оптимизации работы функций, реализацию паттернов проектирования через множественное наследование и дескрипторы, решение задач многопоточности и параллельных вычислений для повышения производительности приложений, разработка графических интерфейсов с применением библиотек PyQt и

		навыков разработки графических интерфейсов с помощью библиотек PyQt и Kivy и применения технологий искусственного интеллекта для создания программного обеспечения.	Kivy для создания пользовательских приложений, а также интеграция технологий искусственного интеллекта для автоматизации процессов разработки и тестирования программного обеспечения.
Модуль 2. Защита от сетевых атак с применением ИИ	Изучение методов анализа и защиты сетевых протоколов, предотвращения сетевых атак и обеспечения безопасности сетевых ресурсов с использованием технологий искусственного интеллекта.	Освоение методов анализа и защиты сетевых протоколов, приобретение навыков работы с инструментами для сканирования портов и анализа трафика (Nmap, Wireshark), умение выявлять и предотвращать сетевые атаки (ARP-атаки, сниффинг, DoS/DDoS), разработку программ на Python для мониторинга сетевой безопасности, настройки брандмауэров и управления VPN-соединениями с использованием IPsec, а также применение технологий искусственного интеллекта для автоматизации процессов обнаружения уязвимостей, анализа сетевого трафика и защиты сетевых ресурсов.	Анализ сетевых уязвимостей и протоколов с использованием инструментов сканирования, задачи на перехват и анализ сетевого трафика, практическое применение методов защиты от сетевых атак (настройка брандмауэров, фильтрация трафика), реализация программ для обнаружения ARP-атак и сниффинга, разработка решений для безопасной передачи данных через VPN и IPsec, а также автоматизация процессов анализа и защиты сетевых ресурсов с применением технологий искусственного интеллекта.

Модуль 3. Безопасность веб-приложений с применением ИИ	Изучение и освоение методов обеспечения безопасности веб-приложений с использованием технологий искусственного интеллекта.	Освоение методов обнаружения и защиты от основных уязвимостей веб-приложений (SQL-инъекции, XSS, CSRF), приобретение навыков разработки скриптов на Python для поиска и эксплуатации уязвимостей с использованием ИИ, создание систем фильтрации и санитизации пользовательского ввода, разработку защищенных баз данных через параметризацию запросов и подготовленные выражения, проектирование безопасных систем аутентификации и управления сессиями с применением шифрования и подписи, а также освоение стандартов безопасности (OWASP Top 10) и методов противодействия атакам через валидацию данных, фильтрацию входных параметров, использование токенов CSRF и HTTP-заголовков.	Разработка и анализ веб-приложений на предмет уязвимостей (SQL-инъекции, XSS, CSRF) с использованием инструментов сканирования и эксплуатации, создание систем фильтрации и санитизации пользовательского ввода для защиты от атак, реализация безопасных механизмов работы с базами данных через параметризованные запросы и подготовленные выражения, проектирование защищенных систем аутентификации и управления сессиями с применением шифрования и подписи, а также разработка рекомендаций и отчетов по обеспечению безопасности веб-приложений на основе стандартов OWASP и других методологий.
Модуль 4. Комплексная безопасность информационных систем с	Формирование комплексного понимания методов обеспечения информационной безопасности и противодействия различным	Освоение методов цифровой экспертизы и анализа киберинцидентов, приобретение навыков разработки мер защиты	Анализ и сбор цифровых доказательств для расследования киберинцидентов, разработка

применением ИИ	типам атак на информационные системы с использованием технологий искусственного интеллекта.	от манипулятивных атак (социальная инженерия, фишинг) с использованием ИИ, умение анализировать и обходить системы защиты для выявления уязвимостей, создание инструментов на Python для тестирования безопасности систем, разработку безопасных механизмов аутентификации и авторизации с применением шифрования данных, а также проектирование защищенных систем с учетом принципов конфиденциальности и целостности данных.	мер защиты от атак социальной инженерии и фишинга с использованием ИИ, создание инструментов на Python для тестирования безопасности систем и обхода аутентификации, проектирование защищенных механизмов аутентификации и авторизации, реализация шифрования данных и обеспечение конфиденциальности, а также составление отчетов по анализу уязвимостей и рекомендаций по повышению уровня защищенности информационных систем.

3. Промежуточная аттестация

Количество академических часов	4
Формы контроля	Тестирование
Диагностические инструменты	Форма промежуточной аттестации – зачет, который проводится в форме тестирования, состоящего из 20 вопросов, 15 вопросов – закрытого типа с выбором варианта ответа, где один вариант правильный и 5 вопросов – открытого типа, где необходимо вписать правильный ответ. Перечень вопросов составляется на основе изученного в процессе обучения материала по

	модулю. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения промежуточной аттестации выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 50% и более правильных ответов; отметка «не зачтено» – менее 50% правильных ответов.

Примеры заданий	Промежуточная аттестация по модулю 1.
	
	1. Что вернет «decorator(my_function)»?
	def decorator(func):
	def wrapper(*args, **kwargs):
	# Добавляет логику до/после вызова func
	return func(*args, **kwargs)
	return wrapper
	a) Результат my_function
	b) Функцию wrapper
	c) Ошибку
	d) None
	
	2. Какой оператор используется для получения значения из генератора?
	a) return
	b) yield
	c) next()
	d) field
	
	3. Для чего используется __metaclass__?
	a) Изменение создания классов
	b) Обработка исключений
	c) Оптимизация памяти
	d) Множественного наследования

	4. Какой метод закрывает соединение с БД? a) commit() b) close() c) cursor() d) replace() 5. Что предотвращает «Lock» в модуле threading? a) Race condition b) Утечку памяти c) Deadlock d) Семафор 6. Какой виджет используется для ввода текста в PyQt? a) QLabel b) QLineEdit c) QPushButton d) QText 7. Что означает «GPT»? Ответ: Generative Pre-trained Transformer 8. Какой метод дескриптора вызывается при присвоении значения? a) __get__ b) `__set__` c) __delete__ d) __upload__ 9. Как добавить обработчик нажатия кнопки в Kivy? a) on_press: callback() b) on_click: callback()

	c) signal: callback()
	d) on_press: click()
	
	10. Какое ключевое слово обозначает асинхронную функцию?
	Ответ: async
	
	11. Как создать генераторное выражение?
	a) [x for x in range(10)]
	b) (x for x in range(10))
	c) {x for x in range(10)}
	d) [[x for x in range(10)]]
	
	12. Как применить декоратор к функции?
	a) @decorator
	b) apply(decorator, func)
	c) decorator(func)
	d) func(decorator)
	
	13. Что гарантирует «with open(...)»?
	a) Автоматическое закрытие файла
	b) Шифрование данных
	c) Кэширование записи
	d) Освобождение буфера
	
	14. Что вернет «list(gen())»?
	def gen():
	for i in range(3):
	yield i * 2
	a) [0, 1, 2]
	b) [0, 2, 4]
	c) [2, 4, 6]

	d) [0, 2, 8] 15. Как выполнить SQL-запрос в SQLite? a) db.run("SELECT * FROM table") b) db.execute("SELECT * FROM table") c) conn.query("SELECT * FROM table") d) cursor.execute("SELECT * FROM table") 16. С помощью какой функции достигается синхронизация доступа к общим ресурсам? Ответ: Lock() 17. Какой виджет в PyQt отображает текст? Ответ: QLabel 18. Как объявить метакласс? a) class MyClass(metaclass=Meta) b) class MyClass(Meta) c) class MyClass with Meta d) class MyClass(Meta=metaclass) 19. Как создать бесконечный генератор? a) while True: yield b) for i in infinity: yield c) yield from endless() d) while None: yield 20. Для чего используется «multiprocessing.Pool()»? a) Создание потоков b) Параллельное выполнение функций c) Синхронизация процессов d) Блокировка общего ресурса

	Промежуточная аттестация по 2 модулю: 1. Выберите уязвимость протокола DNS: a) Отравление кэша b) XSS-инъекция c) SQL-инъекция d) ARP-spoofing 2. Инструмент для анализа трафика с графическим интерфейсом: Ответ: Wireshark 3. Цель DoS-атаки: a) Похищение данных b) Нарушение доступности сервиса c) Установка backdoor d) Шифрование данных 4. Для защиты от перехвата трафика используется протокол: a) FTP b) **SSL/TLS** c) HTTP d) SMTP 5. ARP-отравление возможно из-за: a) Отсутствия аутентификации в ARP b) Шифрования пакетов c) Использования порта 443 d) Фильтрации MAC-адресов 6. Порт по умолчанию для HTTPS:

	Ответ: 443 7. Инструмент для эксплуатации уязвимостей: a) Wireshark b) Metasploit c) tcpdump d) Nessus 8. Как называется атака которая имитирует легитимный сервер для перехвата трафика? (напишите аббревиатуру) *Ответ: MITM 9. IDS предназначена для: a) Блокировки трафика b) Обнаружения вторжений c) Шифрования данных d) Сканирования портов 10. Фильтрация трафика по IP-адресам реализуется через: a) DNS-сервер b) Брандмауэр c) DHCP d) ARP-таблицу 11. На каком уровне модели OSI работает Ipsec? (одним прилагательным) Ответ: сетевой 12. Протокол для безопасной передачи файлов: a) HTTP b) FTPS c) DNS

	d) SNMP
	Ответ: b
	
	13. Что вернет функция для порта 80 на 127.0.0.1, если HTTP-сервер запущен?
	import socket
	def scan_port(ip, port):
	try:
	sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
	sock.settimeout(0.5)
	result = sock.connect_ex((ip, port))
	sock.close()
	return result == 0
	except:
	return False
	Ответ: True
	
	14. Какой протокол может предотвратить перехват трафика в веб?
	Ответ: HTTPS
	
	15. Будет что вернет функция в качестве реакции на пакет с «src="10.0.0.5", dport=23»?
	def firewall_rule(packet, allowed_ips=["192.168.1.1"], blocked_ports=[23]):
	if packet.src not in allowed_ips or packet.dport in blocked_ports:
	return "BLOCK"
	return "ALLOW"
	Ответ: BLOCK
	
	16. Атаки на какой протокол обнаруживает эта функция?
	from scapy.all import arpcache
	def check_arp(ip, expected_mac):
	return arpcache[ip] == expected_mac
	Ответ: ARP

	17. Для защиты от ARP-спуфинга используется: a) DHCP Snooping b) HTTP-прокси c) Открытый релей SMTP d) DNS-кеширование 18. SSLstrip атакует путём: a) Понижения HTTPS до HTTP b) Шифрования DNS-запросов c) Блокировки порта 443 d) Подмены сертификатов CA 19. Инструмент для пассивного анализа трафика: a) Nmap b) tcpdump c) Netcat d) SQLmap 20. IPS отличается от IDS тем, что: a) Только обнаруживает атаки b) Может автоматически блокировать трафик c) Анализирует только DNS d) Работает на уровне приложений Промежуточная аттестация по 3 модулю: 1.Какой тип атаки используется? SELECT * FROM users WHERE id = 25 OR 1=1; a) Слепая инъекция b) Синтаксическая ошибка

	c) Временная задержка
	d) Бандл-инъекция
	
	2. Какой метод безопасно выводит пользовательские данные?
	a) {{ user_input }}
	b) {% autoescape off %}{{ user_input }}{% endautoescape %}
	c) {{ user_input|safe }}
	d) {{ user_input|escape }}
	
	3. Какое условие обязательно для успешной CSRF-атаки?
	a) XSS на целевом сайте
	b) Пользователь авторизован на уязвимом сайте
	c) SQL-инъекция в форме
	d) Отсутствие HTTPS
	
	4. Какой код защищен от SQL-инъекций?
	# A
	cursor.execute(f"SELECT * FROM users WHERE name = '{input}'")
	# B
	cursor.execute("SELECT * FROM users WHERE name = ?", (input,))
	a) Только A
	b) Только B
	c) Оба варианта
	d) Ни один
	
	5. Как подписать сессионные куки в Flask?
	a) app.secret_key = 'secret'
	b) app.config['SESSION_COOKIE_SECURE'] = True
	c) app.config['SESSION_COOKIE_HTTPONLY'] = True
	d) Использовать JWT

	6. Выберите прокси-сервер для перехвата HTTP(S): a) Nmap b) Wireshark c) Burp Suite d) sqlmap 7. Какой HTTP-заголовок блокирует встраивание страницы в <iframe>? a) X-XSS-Protection b) Content-Security-Policy c) X-Frame-Options d) Strict-Transport-Security 8. Какой метод используется для подтверждения уязвимости слепой SQL-инъекции? a) Анализ кода ошибки b) Измерение времени ответа c) Сравнение HTTP-статусов d) Изменение Content-Type 9. Какая функция Python преобразует <script> в безопасную строку? a) str.replace() b) html.escape() c) re.sub() d) json.dumps() 10. Какая библиотека Python используется для обработки естественного языка в санитизации? a) TensorFlow b) Scikit-learn c) spaCy d) NLTK 11. Какой оператор позволяет объединить результаты двух запросов в SQL?

	Ответ: UNION
	
	12. Что такое «фиксация сессии»?
	a) Перехват sessionID через XSS
	b) Принуждение пользователя использовать известный злоумышленнику sessionID
	c) Подмена sessionID Ответ:Ответ:в базе данных
	d) Брутфорс sessionID
	
	13. Какой метод безопасен для фильтрации данных в Django?
	# A
	User.objects.raw(f"SELECT * FROM users WHERE name = '{name}'")
	# B
	User.objects.filter(name=name)
	a) Только A
	b) Только B
	c) Оба варианта
	d) Ни один
	
	14. Какой параметр SameSite блокирует CSRF?
	a) None
	b) Lax
	c) Strict
	d) Secure
	
	15. Какая функция Python опасна для выполнения пользовательского ввода?
	a) subprocess.check_output()
	b) os.system()
	c) shlex.quote()
	d) requests.get()
	
	16. Какой инструмент OWASP интегрирует ИИ для сканирования?

	a) ZAP b) SQLMap c) Nikto d) W3af 17. Какой метод хеширования паролей соответствует стандартам OWASP? Ответ: bcrypt 18. Где происходит выполнение вредоносного кода в DOM-based XSS? a) На сервере b) В базе данных c) В браузере жертвы d) На прокси-сервере 19. Какая СУБД может работать без сервера? Ответ: SQLite 20. Ниболее популярный фреймвор для разработки сайтов на Python? Ответ: Django Промежуточная аттестация по 4 модулю: 1. Цель цифровой форензики: a) Прогнозирование атак b) Сбор доказательств для суда c) Разработка ИИ-моделей d) Обучение сотрудников 2. **МС** (Multiple Choice): Методы извлечения данных: a) Анализ метаданных b) Восстановление ОЗУ c) Фишинг

	d) Брутфорс 3. Цепочка расследования должна фиксировать всех, кто имел доступ к доказательствам? (да/нет) Ответ: да 4. Этапы анализа доказательств: 1. Сбор данных 2. Извлечение артефактов 3. Составление отчета 4. Всё перечисленное 5. Ключевой элемент отчета об инциденте? a) Биография хакера b) Рекомендации по предотвращению c) Реклама ИИ-инструментов d) Следы взлома 6.ИИ может автоматически генерировать юридически значимые отчеты? (да/нет) Ответ: нет 7. Пример фишинга: a) SSL-сертификат b) Письмо "Ваш аккаунт заблокирован" c) VPN-соединение d) «Письмо счастья» 8. Уязвимость при обходе аутентификации: a) SQL-injection b) XSS c) Broken Authentication

	d) Перехват домена 9. Этапы атаки брутфорс: a) Сбор логинов b) Подбор паролей c) Эксплуатация d) Всё перечисленное 10. Функция хэширования пароля: import hashlib def hash_password(password, salt): return hashlib.____(salt.encode() + password.encode()).hexdigest() a) md5() b) sha256() c) aes() d) hash() 11. SSH использует асимметричное шифрование для установки соединения? (да/нет) Ответ: да 12. Инструмент анализа метаданных: Ответ: ExifTool 13. Самый опасный тип фишинга: a) Целевой b) Массовый c) Смс-фишинг d) Подмена домена 14. Признаки уязвимости Broken Authentication: a) Отсутствие 2FA

	b) Сильные требования к паролям
	c) Открытый порт 80
	в) Закрытый порт 443
	
	15. Брутфорс-атака на форму логина:
	import requests
	def brute_force(url, logins):
	for login in logins:
	r = requests.post(url, data={"login":_____, "pass":"test"})
	if "Welcome" in r.text: return login
	a) login
	b) "admin"
	c) logins[0]
	d) chain
	
	16. Лучшая защита от MITM-атак:
	a) SSL Pinning
	b) Хеширование паролей
	c) WAF
	d) Брендмауэр
	
	17. Обнаружение фишинговых URL:
	def is_phishing(url):
	import re
	return bool(re.search(r'(?:http://|www\.)(?!trusted-domain)', _____))
	a) url
	b) url.lower()
	c) str(url)
	d) url[0]
	
	18. Какой метод НЕ используется для обхода аутентификации?

	a) SQL-инъекции b) Подбор сессионных куки c) Физический доступ к серверу d) Межсайтовый скриптинг 19. Лучшая практика хранения паролей: a) Симметричное шифрование b) Хеширование с солью c) Открытое хранение d) Кодирование Base64 20. Генерация безопасного пароля: def generate_password(length=12): import secrets, string alphabet = string.ascii_letters + string.digits + _____ return ''.join(secrets.choice(alphabet) for _ in range(length)) a) "!@#$%" b) string.punctuation c) "_-." d) len(string)
Шкала оценивания, нижнее значение	0
Шкала оценивания, верхнее значение	20
Шкала оценивания, минимальный проходной балл	10

ИТОГОВАЯ АТТЕСТАЦИЯ	
Количество академических часов	4
Формы контроля	Представление итогового проекта. Темы итогового проекта (по выбору учащегося): 1. «Автоматизированная система защиты веб-приложений на Python» (для анализа уязвимостей и предотвращения атак.) 2. «NeuroPentest: Интеллектуальный сканер уязвимостей» (Использование нейросетей для поиска и эксплуатации уязвимостей.) 3. «Ethical Hawk» (Игра слов: «Hawk» (ястреб) + "Hack". Проект по мониторингу сетевых угроз в реальном времени.) 4. «CipherMind: Квантово-устойчивая криптография с применением ИИ» (Защита данных от будущих квантовых атак.) 5. «SOC AI: Система реагирования на инциденты с ИИ-аналитикой» (Автоматизация Security Operations Center.) 6. «PhishBuster: Детектор фишинга» (Анализ почты и веб-страниц на признаки мошенничества.) 7. «ZeroDay Shield: Прогнозирование Zero-Day уязвимостей с помощью ИИ» (Предсказание неизвестных угроз на основе паттернов.) 8. «DarkTrace Light: Открытый аналог системы обнаружения аномалий в сети» 9. «HackNet Simulator: VR-тренажер для отработки кибератак и защиты» (Имитация реальных сценариев взлома и защиты в виртуальной среде.) 10. «SentinelX: Автономный бот для Bug Bounty с GPT-интеграцией» (Автоматический поиск багов с генерацией отчетов через ИИ.)
Диагностические инструменты	Оценка итогового проекта осуществляется в соответствии с системой критериев. Каждый критерий оценивается по следующим рубрикаторам: • не соответствует критерию (0 баллов)

	• скорее соответствует, чем не соответствует критерию (1 балл) • скорее соответствует, чем не соответствует критерию (2 балла) • полностью соответствует критерию (3 балла) Максимально возможное количество баллов за итоговый проект: 30 баллов В рамках процедуры оценивания технические баллы переводятся в следующую шкалу оценки: от 0% до 50% (0-15 баллов) – не зачтено от 51% до 100% (16-30 баллов) - зачтено
Показатели и критерии оценивания	1. Владение технологиями показано на уровне реализаций проектов подобных типов 2. Проект выполнен в соответствии с современными подходами в заявленной тематической области 3. Проект выполнен самостоятельно, без содержательной помощи преподавателя 4. В проекте корректно используется язык программирования Python 5. Требования к стилю кода соблюдены 6. Графические элементы интерфейса отображаются корректно, текстовые элементы не содержат языковых ошибок 7. Используются оптимальные алгоритмы и структура базы данных, а также оптимальные запросы к базе данных 8. Терминология соответствует решаемой проблеме и используется правильно 9. Интерфейс интуитивно понятен пользователям, удобен в использовании 10. Проект выполнен и предоставлен на проверку с соблюдением дедлайна.

4. Преподаватели

ФИО	Наименование основного места работы	Должность	Высшее образование или среднее профессиональ ное образование по направлению «Образование и педагогические науки»	Высшее образование или среднее профессиональное образование по иному направлению соответствующим направленности ДОП	Ссылка на веб-страницы с портфолио	Информация о курсах повышения квалификац ии по профилю преподаваем ой дисциплины (за последние 3 года)	Пройдена промежуточная аттестация не менее чем за два года обучения по образовательным программам высшего образования по специальностям и направлениям подготовки, соответствующим направленности ДОП	Отметка о полученном согласии на обработку персональных данных
Бердашкевич Артём Эдуардович	АО «Диалог»	Руководитель направления информационной безопасности	нет	да	https://xn----btbkcarrtg5c1as4d.xn--p1ai/experts/berdashkevich	Программирование Python. Продвинутый уровень, 36 час., ООО Институт Повышения Квалификации Дополнительного профессионального образования, 2023 г.	нет	да
Лукьянцев Игорь Сергеевич	АО «Диалог»	Специалист по информационной	нет	да	https://xn----btbkcarrtg5c1as4d.xn--	Программирование Python. Продвинутый уровень, 36 час.,	нет	да

		безопасности			p1ai/experts/lukiantzev	ООО Институт Повышения Квалификации Дополнительного профессионального образования, 2023 г.		
Яицкий Антон Андреевич	ООО «Зенит-Арена»	Специалист по информационной безопасности	нет	да	https://xn----btbkcarrtg5c1as4d.xn--p1ai/experts/yaitsky	Программирование Python. Продвинутый уровень, 36 час., ООО Институт Повышения Квалификации Дополнительного профессионального образования, 2023 г.	нет	да
Почаевец Андрей Андреевич	АНО ДПО МЦК «Цель»	Программный директор АНО ДПО МЦК "Цель"; преподаватель	нет	да	https://xn----btbkcarrtg5c1as4d.xn--p1ai/experts/pochaevets	-	нет	да

5. Комплект организационно-педагогических условий реализации дополнительной общеобразовательной общеразвивающей программе начального уровня «Этичный хакинг: миг уникальности» (далее –ДОП)

5.1. Учебный план

№ п/п	Модули, итоговый контроль/аттестация	Элементы модуля (темы, промежуточная аттестация)	Общее кол-во часов элемента модуля, ак.час	Из них:				Кол-во видео в теме, ед. (при наличии)
				теоретическая подготовка, ак.час	практическая работа, ак.час	самостоятельная работа и самоконтроль, ак.час	контроль/ аттестация, ак.час	
1.	Модуль 1. Продвинутое программирование на Python с ИИ	Тема 1.1. Инструменты Python для решения сложных задач	8	2	5		1	1
2.		Тема 1.2. Базы данных и обработка файлов на Python	8	2	5		1	1
3.		Тема 1.3. Основы параллельных вычислений и многопоточного программирования	9	2	5	1	1	1
4.		Тема 1.4. Создание графических интерфейсов на Python и применению ИИ для разработки программ	10	2	6	1	1	1
5.		Промежуточная аттестация по 1 модулю	1				1	
6.	Модуль 2.	Тема 2.1. Уязвимости сетевых протоколов и их анализ с помощью ИИ	8	2	5		1	1

7.	Защита от сетевых атак с применением ИИ	Тема 2.2. Анализ и перехват трафика с применением ИИ	8	2	5		1	1
8.		Тема 2.3. ARP-атаки и сниффинг	9	2	5	1	1	1
9.		Тема 2.4. Защита сетевых ресурсов с применением ИИ	10	2	6	1	1	1
10.		Промежуточная аттестация по 2 модулю	1				1	
11.	Модуль 3. Безопасность веб-приложений с применением ИИ	Тема 3.1. Эксплуатация уязвимостей веб-приложений с помощью ИИ	8	2	5		1	1
12.		Тема 3.2. Защита баз данных с применением ИИ	8	2	5		1	1
13.		Тема 3.3. Аутентификация и атаки на сессии с применением ИИ	9	2	5	1	1	1
14.		Тема 3.4. Защита и и противодействие атакам на веб-приложения с помощью ИИ	10	2	6	1	1	1
15.		Промежуточная аттестация по 3 модулю	1				1	
16.	Модуль 4. Комплексная безопасность информационных систем с применением ИИ	Тема 4.1. Цифровая экспертиза с применением ИИ	8	2	5		1	1
17.		Тема 4.2. Манипулятивные атаки с применением ИИ	8	2	5		1	1
18.		Тема 4.3.	9	2	5	1	1	1

		Обход системы защиты и противодействие этому с помощью ИИ						
19.		Тема 4.4. Безопасные системы с применением ИИ	10	2	6	1	1	1
20.		Промежуточная аттестация по 4 модулю	1				1	
21.	Итоговый контроль/аттестация по ДОП		4			4		
22.	Итого по ДОП:		**148**	**32**	**84**	**12**	**20**	
23.	ИТиСИ		Часы ИТиСИ не входят в общую трудоемкость ДОП, но участие в ИТиСИ обязательно для всех успешно прошедших итоговый контроль/аттестацию по ДОП					

5.2. Рабочая программа с описанием каждого модуля дополнительной общеобразовательной общеразвивающей программе начального уровня «Этичный хакинг: миг уникальности» (далее –ДОП)

Элементы ДОП (модули и итоговый контроль ДОП)	Элементы модуля (темы, промежуточная аттестация)	Содержание (единицы содержания теоретической подготовки, практической работы, самостоятельной работы, контроля по теме и промежуточной аттестации (вопросы, задания, задачи и пр.)	Виды образовательных мероприятий /деятельности (теоретическая подготовка, практическая работа, самостоятельная работа, аттестация/контроль)	Объем в ак.ч.
Модуль 1. Продвинутое программирование на Python с ИИ Описание модуля: *Модуль посвящен изучению продвинутых возможностей Python, включая декораторы, множественное наследование, дескрипторы, работу*	Тема 1.1. Инструменты Python для решения сложных задач	Изучение продвинутых возможностей Python: генераторов, декораторов, метаклассов, множественного наследования и дескрипторов, включая их создание, использование и применение для управления данными и атрибутами классов.	теоретические занятия	2
		Реализация декоратора timer для измерения времени выполнения функции и создание генератора, выводящего последовательность чисел Фибоначчи до заданного предела.	практические занятия	5
		Создание генератора, выводящего последовательность простых чисел до заданного предела.	текущий контроль	1

с потоками, параллельные вычисления, основы GUI и графических библиотек. Практические навыки включают использование декораторов, генераторов, работу с файлами, контекстный менеджер, управление базами данных SQLite, многопоточность и разработку графических приложений с помощью ИИ. Цель модуля: *Изучение и освоение продвинутых возможностей языка программирования Python с применением технологий искусственного интеллекта.* Планируемые результаты: *Освоение продвинутых возможностей Python, таких как работа с декораторами, генераторами, метаклассами, множественным наследованием и дескрипторами, приобретение навыков работы с файлами и базами данных SQLite, включая использование контекстного менеджера и выполнение SQL-запросов, освоение принципов многопоточного и параллельного программирования с использованием модулей threading и multiprocessing, а также получение практических навыков разработки графических интерфейсов с помощью библиотек PyQt и Kivy и применения технологий искусственного интеллекта для создания программного обеспечения.*	Тема 1.2. Базы данных и обработка файлов на Python	Работа с файлами (открытие, чтение, запись, использование контекстного менеджера with) и базами данных (подключение, выполнение SQL-запросов, управление данными, закрытие соединения).	теоретические занятия	2
		Создание и работа с файлом (запись и чтение данных) и базой данных SQLite (создание таблицы users, добавление записей).	практические занятия	5
		Создание таблицы products в базе данных с полями id, name, price, quantity и заполнение её данными о товарах.	текущий контроль	1
	Тема 1.3. Основы параллельных вычислений и многопоточного программирования	Изучение многопоточного и параллельного программирования: создание и управление потоками с помощью модуля threading, синхронизации данных (Lock, Condition, Semaphore, Queue), а также использование модуля multiprocessing для работы с процессами, обмена данными и распределенных вычислений.	теоретические занятия	2
		Разработка программы для создания потоков: один поток выводит числа от 1 до 10 с задержкой в 1 секунду, а также реализуется программа, где три потока выводят свои имена по 5 раз.	практические занятия	5
		Реализации программ: параллельное вычисление суммы элементов двух списков и использование пула процессов для параллельного расчета факториалов чисел от 1 до 10.	самостоятельная работа текущий контроль	1 1
	Тема 1.4. Создание графических интерфейсов на Python и применению ИИ для разработки программ	Основы GUI (окна, виджеты, события), разработка графических приложений с использованием библиотек (PyQt, Kivy), интеграции функциональности (базы данных, файлы, сети), оптимизация интерфейса (многопоточность, асинхронность). Виды ИИ. GPT-модели. Способы взаимодействия с ИИ. Примеры генерации кода с помощью ИИ. Объяснение кода с помощью ИИ.	теоретические занятия	2

Типы задач/деятельности: *Программные решения с использованием продвинутых возможностей Python, включая создание декораторов и генераторов для оптимизации работы функций, реализацию паттернов проектирования через множественное наследование и дескрипторы, решение задач многопоточности и параллельных вычислений для повышения производительности приложений, разработка графических интерфейсов с применением библиотек PyQt и Kivy для создания пользовательских приложений, а также интеграция технологий искусственного интеллекта для автоматизации процессов разработки и тестирования программного обеспечения.*		Основы GUI (окна, виджеты, события), разработка графических приложений с использованием библиотек (PyQt, Kivy), интеграции функциональности (базы данных, файлы, сети), оптимизация интерфейса (многопоточность, асинхронность). Виды ИИ. GPT-модели. Способы взаимодействия с ИИ. Примеры генерации кода с помощью ИИ. Объяснение кода с помощью ИИ.	практические занятия	6
		Разработка с помощью ИИ графического приложения на выбранной библиотеке, позволяющего пользователю создавать, сохранять и открывать файлы.	самостоятельная работа текущий контроль	1 1
	Промежуточная аттестация по 1 модулю	Тестирование		1
Модуль 2. Защита от сетевых атак с применением ИИ Описание модуля: *Модуль посвящен изучению уязвимостей сетевых протоколов, методов их анализа и защиты, работы с ARP-атаками, сниффингом и сетевыми атаками, а также освоению навыков анализа трафика, разработки программ для атак и защиты, настройки брандмауэра и*	Тема 2.1. Уязвимости сетевых протоколов и их анализ с помощью ИИ	Изучение уязвимостей сетевых протоколов, их классификация, методы анализа (сканирование портов, анализ трафика) с использованием инструментов (Nmap, Wireshark, Nessus, Metasploit), способы эксплуатации (DoS, переполнение буфера) и методы защиты (обновления, брандмауэр, шифрование, протоколы безопасности).	теоретические занятия	2
		Использование Nmap для сканирования портов в локальной сети, перехват и анализ HTTP-трафика с извлечением данных (заголовки запросов и ответов) с помощью ИИ, а также автоматизации этих действий на Python.	практические занятия	5
		Написание программы на Python с использованием ИИ для сканирования диапазона IP-адресов, определения	текущий контроль	1

управления VPN-соединениями через Ipsec, в том числе с помощью ИИ. Цель модуля: *Изучение методов анализа и защиты сетевых протоколов, предотвращения сетевых атак и обеспечения безопасности сетевых ресурсов с использованием технологий искусственного интеллекта.* Планируемые результаты: *Освоение методов анализа и защиты сетевых протоколов, приобретение навыков работы с инструментами для сканирования портов и анализа трафика (Nmap, Wireshark), умение выявлять и предотвращать сетевые атаки (ARP-атаки, сниффинг, DoS/DDoS), разработку программ на Python для мониторинга сетевой безопасности, настройки брандмауэров и управления VPN-соединениями с использованием IPsec, а также применение технологий искусственного интеллекта для автоматизации процессов обнаружения уязвимостей, анализа сетевого трафика и защиты сетевых ресурсов.* Типы задач/деятельности:		открытых портов и доступных сервисов на каждом узле.		
	Тема 2.2. Анализ и перехват трафика с применением ИИ	Рассматриваются расширенные методы перехвата и анализа сетевого трафика, использование снифферов, изучение протоколов (HTTP, FTP, DNS, SMTP), фильтрация трафика с помощью Wireshark/tcpdump, анализ зашифрованного трафика (SSL/TLS) и выявление атак (Man-in-the-Middle, ARP-отравление, DNS-отравление).	теоретические занятия	2
		Реализация программы для перехвата сетевого трафика на локальной машине, выявления подозрительной активности (например, аномалий в запросах или размерах пакетов), а также анализа зашифрованного HTTPS-трафика с помощью sslstrip и ИИ для изучения данных в открытом виде.	практические занятия	5
		Изучается протокол DNS и его уязвимости, а также реализация программы с помощью ИИ для перехвата и анализа DNS-запросов с целью выявления подозрительных запросов или изменений в DNS-ответах.о найденной информации и её применимости.	текущий контроль	1
	Тема 2.3. ARP-атаки и сниффинг	Рассматриваются сниффинг и его роль в сетевых атаках, принципы работы ARP, уязвимости протокола, методы проведения ARP-атак (отравление, перехват), использование инструментов для сниффинга и защиты, а также способы обнаружения подмененных ARP-записей.	теоретические занятия	2
		Разработка программы для ARP-отравления в локальной сети с подменой MAC-адресов и анализом перехваченных пакетов, а также создание решения с использованием ИИ и scapy для перехвата трафика, идентификации ARP-пакетов и отслеживания изменений в ARP-таблице.	практические занятия	5

Анализ сетевых уязвимостей и протоколов с использованием инструментов сканирования, задачи на перехват и анализ сетевого трафика, практическое применение методов защиты от сетевых атак (настройка брандмауэров, фильтрация трафика), реализация программ для обнаружения ARP-атак и сниффинга, разработка решений для безопасной передачи данных через VPN и IPsec, а также автоматизация процессов анализа и защиты сетевых ресурсов с применением технологий искусственного интеллекта.		Разработка инструмента с использованием ИИ для мониторинга ARP-таблицы и обнаружения подмененных записей, который регулярно сканирует таблицу и оповещает администратора о возможной подмене MAC-адресов.	самостоятельная работа текущий контроль	1 1
	Тема 2.4. Защита сетевых ресурсов с применением ИИ	Рассматриваются основы защиты сетевых ресурсов, включая брандмауэры, IDS/IPS, методы противодействия DoS/DDoS-атакам, использование сетевых политик и фильтров, а также применение протоколов безопасности (IPsec, SSL/TLS) для защиты коммуникаций.	теоретические занятия	2
		Разработка программы с помощью ИИ для настройки брандмауэра с возможностью блокировки трафика по заданным правилам, а также для установки VPN-соединения через IPsec с запросом параметров и аутентификационных данных.	практические занятия	6
		Разработка программы с использованием ИИ для фильтрации сетевого трафика, позволяющую настраивать правила доступа по IP-адресам, портам и протоколам.	самостоятельная работа текущий контроль	1 1
	Промежуточная аттестация по 2 модулю	Тестирование		1
Модуль 3. Безопасность веб-приложений с применением ИИ Описание модуля:	Тема 3.1. Эксплуатация уязвимостей веб-приложений с помощью ИИ	Рассматриваются основные уязвимости веб-приложений (SQL-инъекции, XSS, CSRF), механизмы их эксплуатации, методы анализа (белый и черный ящик), а также инструменты для обнаружения уязвимостей и перехвата трафика (сканеры, прокси-серверы).	теоретические занятия	2
		Разработка скрипта на Python с использованием ИИ для автоматизированного поиска уязвимостей XSS путем отправки вредоносных данных и анализа ответов, а также программы для эксплуатации SQL-инъекций с	практические занятия	5

В данном модуле в фокусе внимания - веб-приложения. Изучаются основные уязвимости веб-приложений; инструменты и методы обнаружения и эксплуатации уязвимостей веб-приложений; SQL-инъекции; методы защиты от SQL-инъекций; принципы сессий и механизмов аутентификации; виды атак на сессии; методы безопасной аутентификации; стандарты безопасности, связанные с сессиями и аутентификацией; основные методы защиты от атак. *Осваиваются навыки разрабатывать скрипты на Python для поиска и эксплуатации уязвимостей; разрабатывать систему фильтрации и санитизации пользовательского ввода; разрабатывать программы на Python для работы с базой данных; анализировать код веб-приложений на предмет уязвимостей SQL-инъекций; разрабатывать системы аутентификации на основе сессий; разрабатывать безопасные веб-приложения с использованием фреймворка Django; исследователь стандарты и формулировать рекомендации по безопасности веб-приложений; составлять отчет о мерах по защите веб-приложений. Показываются возможности ИИ для решения таких задач.* <u>Цель модуля:</u>		целью несанкционированного доступа или изменения данных.		
		Разработка системы фильтрации и санитизации пользовательского ввода с помощью ИИ для защиты от XSS, включающая создание модуля проверки и очистки данных от опасных символов и скриптов перед выводом на веб-страницу.	текущий контроль	1
	<u>Тема 3.2.</u> Защита баз данных с применением ИИ	Рассматриваются SQL-инъекции, их принципы работы и типы (синтаксические ошибки, временные задержки, бандл-инъекции), а также методы защиты: параметризация запросов, подготовленные выражения, ограничение прав доступа и санитизация ввода.	теоретические занятия	2
		Создание базы данных на SQLite и программы на Python с использованием ИИ для выполнения запросов, защищенных от SQL-инъекций через параметризацию и подготовленные выражения, а также применение sqlmap для автоматизированных атак на SQL-базы.	практические занятия	5
		Анализ кода веб-приложения с помощью ИИ для выявления уязвимостей SQL-инъекций, и их эксплуатация путем внедрения злонамеренных запросов и предложение мер по устранению обнаруженных проблем.	текущий контроль	1
	<u>Тема 3.3.</u> Аутентификация и атаки на сессии с применением ИИ	Рассматриваются принципы работы сессий и аутентификации в веб-приложениях, виды атак на сессии (перехват, подмена, фиксация) и методы безопасной аутентификации, такие как использование сильных паролей, двухфакторная аутентификация и ограничение попыток входа.	теоретические занятия	2
		Разработка с помощью ИИ системы аутентификации на основе сессий в Flask, обеспечивающей защиту данных через шифрование и подпись сессий, а также изучение методов безопасной аутентификации, включая	практические занятия	5

Изучение и освоение методов обеспечения безопасности веб-приложений с использованием технологий искусственного интеллекта Планируемые результаты: *Освоение методов обнаружения и защиты от основных уязвимостей веб-приложений (SQL-инъекции, XSS, CSRF), приобретение навыков разработки скриптов на Python для поиска и эксплуатации уязвимостей с использованием ИИ, создание систем фильтрации и санитизации пользовательского ввода, разработку защищенных баз данных через параметризацию запросов и подготовленные выражения, проектирование безопасных систем аутентификации и управления сессиями с применением шифрования и подписи, а также освоение стандартов безопасности (OWASP Top 10) и методов противодействия атакам через валидацию данных, фильтрацию входных параметров, использование токенов CSRF и HTTP-заголовков.* Типы задач/деятельности: *Разработка и анализ веб-приложений на предмет уязвимостей (SQL-инъекции, XSS, CSRF) с использованием инструментов сканирования и эксплуатации, создание систем фильтрации и санитизации пользовательского ввода для защиты от атак, реализация безопасных меха-*		двухфакторную авторизацию с одноразовыми паролями или мобильными приложениями.		
		Рассмотрение стандартов безопасности сессий и аутентификации в веб-приложениях, включая OWASP Top 10, и применение возможностей ИИ для проведения аудита безопасности.	самостоятельная работа текущий контроль	1 1
	Тема 3.4. Защита и и противодействие атакам на веб-приложения с помощью ИИ	Рассматриваются методы защиты веб-приложений от инъекций, XSS, CSRF и других уязвимостей через валидацию данных, фильтрацию входных параметров, использование токенов CSRF, HTTP-заголовков (SameSite, X-Frame-Options), а также эскейпинг и санитизацию для предотвращения XSS-атак.	теоретические занятия	2
		Разработка с помощью ИИ веб-приложение на Django, включая меры защиты от инъекций и XSS-атак через валидацию, фильтрацию данных, ORM-запросы, эскейпинг и санитизацию пользовательского ввода.	практические занятия	6
		Изучение стандартов безопасности веб-приложений, такие как OWASP Top 10 и CWE/SANS Top 25, и составление с помощью ИИ отчета о ключевых мерах защиты и противодействия распространенным атакам.	самостоятельная работа текущий контроль	1 1
	Промежуточная аттестация по 3 модулю	Тестирование		1

низмов работы с базами данных через параметризованные запросы и подготовленные выражения, проектирование защищенных систем аутентификации и управления сессиями с применением шифрования и подписи, а также разработка рекомендаций и отчетов по обеспечению безопасности веб-приложений на основе стандартов OWASP и других методологий.и усиления сетевой безопасности.				
Модуль 4. Комплексная безопасность информационных систем с применением ИИ Описание модуля: *В данном модуле рассматриваются методы и инструменты форензики, правовые и этические аспекты, социальная инженерия, фишинг, анализ и обход защиты систем, безопасное проектирование систем, а также практические навыки: создание отчетов по цифровым доказательствам, разработка мер защиты от атак, создание инструментов на Python и проектирование механизмов аутентификации.* Цель модуля: *Формирование комплексного понимания методов обеспечения информационной безопасности и противодействия различным типам атак*	Тема 4.1. Цифровая экспертиза с применением ИИ	Рассматриваются определение и отличия форензики и судебной экспертизы, роль форензики в сборе и анализе цифровых доказательств, методы извлечения данных, восстановления файлов и анализа метаданных, а также правовые и этические аспекты использования доказательств в суде.	теоретические занятия	2
		Разработка с помощью ИИ отчета об анализе цифровых доказательств для конкретного случая компьютерного преступления, включающий методы анализа, найденные следы и рекомендации по предотвращению подобных инцидентов.	практические занятия	5
		Составление с помощью ИИ плана действий для анализа инцидентов информационной безопасности, включающий шаги по сбору и анализу цифровых доказательств, а также восстановлению работоспособности системы после взлома или утечки данных.	текущий контроль	1
	Тема 4.2. Манипулятивные атаки с применением ИИ	Рассматриваются социальная инженерия и фишинг, их принципы, методы и типичные сценарии, включая манипуляции и создание чрезвычайных ситуаций, виды фишинга (письма, сайты, звонки) и разрабатываются методы защиты через обучение, технические меры и мониторинг активности.	теоретические занятия	2
		Разработка с помощью ИИ скрипта на Python для создания фишингового письма, включающего элементы	практические занятия	5

на информационные системы с использованием технологий искусственного интеллекта. Планируемые результаты: *Освоение методов цифровой экспертизы и анализа киберинцидентов, приобретение навыков разработки мер защиты от манипулятивных атак (социальная инженерия, фишинг) с использованием ИИ, умение анализировать и обходить системы защиты для выявления уязвимостей, создание инструментов на Python для тестирования безопасности систем, разработку безопасных механизмов аутентификации и авторизации с применением шифрования данных, а также проектирование защищенных систем с учетом принципов конфиденциальности и целостности данных.* Типы задач/деятельности: *Анализ и сбор цифровых доказательств для расследования киберинцидентов, разработка мер защиты от атак социальной инженерии и фишинга с использованием ИИ, создание инструментов на Python для тестирования безопасности систем и обхода аутентификации, проектирование защищенных механизмов аутентификации и авторизации, реализация шифрова-*		социальной инженерии, такие как маскировка под известную организацию или создание срочной ситуации, с последующим сохранением письма в HTML-формате и отправкой его себе или сокурснику.		
		Разработка с помощью ИИ обучающих материалов для сотрудников, включающих презентации, тесты и задания, направленные на проверку знаний и обучение методам противодействия атакам социальной инженерии.	текущий контроль	1
	Тема 4.3. Обход системы защиты и противодействие этому с помощью ИИ	Рассматриваются методы анализа и обхода защиты системы для выявления уязвимостей, включая атаки (брутфорс, словарные, обход аутентификации) и инструменты для их проведения, а также рассмотрение мер защиты и повышения безопасности системы.	теоретические занятия	2
		Разработка с помощью ИИ инструмента на Python для автоматического поиска и эксплуатации уязвимостей через библиотеку Metasploit, а также создание скрипта для обхода аутентификации на веб-сайте методом перебора логинов и паролей с использованием библиотеки requests.	практические занятия	5
		Разработка с помощью ИИ уязвимой системы для тестирования её безопасности с применением изученных методов и инструментов.	самостоятельная работа текущий контроль	1 1
	Тема 4.4. Безопасные системы с применением ИИ	Рассматриваются принципы безопасного проектирования систем, включая защиту от атак, разработку безопасных приложений, проектирование механизмов аутентификации и авторизации, а также реализацию шифрования и обеспечения конфиденциальности данных.	теоретические занятия	2
		Разработка с помощью ИИ системы управления пользователями с хранением паролей в хэшированном виде и приложения для обмена зашифрованными сообщениями через асимметричное шифрование.	практические занятия	6

ния данных и обеспечение конфиденциальности, а также составление отчетов по анализу уязвимостей и рекомендаций по повышению уровня защищенности информационных систем.		Разработка с помощью ИИ механизма безопасной передачи файлов по сети с использованием протокола SSH и симметричного шифрования.	самостоятельная работа текущий контроль	1 1
	Промежуточная аттестация по 4 модулю	Тестирование		1
Итоговый контроль/аттестация	Итоговая аттестация по ДОП			**4**
ИТОГО ПО ПРОГРАММЕ:				Объем в ак.ч. / Объем в %
			теоретическая подготовка	**32** / **22**
			практическая работа	**84** / **56**
			самостоятельная работа	**8** / **5**
			текущий контроль	**16** / **11**
			промежуточная аттестация	**4** / **3**
			итоговый контроль/аттестация	**4** / **3**
			Всего, ак.ч.	**148**
ИТиСИ	*Часы ИТиСИ не входят в общую трудоемкость ДОП, но участие в ИТиСИ обязательно для всех успешно прошедших итоговый контроль/аттестацию по ДОП*			

5.3. Календарный учебный график

№ п/п	Название ДОП	№ потока	Дата начала обучения по ДОП	№ модуля ДОП	Начало обучения по модулю ДОП	Календарный период (количество дней) длительности модуля	Дата окончания обучения по ДОП
1	«Этичный хакинг: миг уникальности»	1	22.09.2025	1	22.09.2025	22.09.2025 – 29.11.2025 69 к.д.	29.05.2026
				2	01.12.2025	01.12.2025 – 02.02.2026 64 к.д.	

				3	03.02.2026	03.02.2026 – 29.03.2026 56 к.д.	
				4	30.03.2026	30.03.2026 – 29.05.2026 61 к.д.	

5.4. Календарно-тематическое планирование

№ п/п	Модули, итоговый контроль/ аттестация	Элементы модуля (темы, промежуточная аттестация)	Кол-во занятий*	Кол-во часов	Дата
1.	Модуль 1. Продвинутое программирование на Python с ИИ	Тема 1.1. Инструменты Python для решения сложных задач	7	2 2 2 2	24.09.2025 26.09.2025 01.10.2025 03.10.2025
2.		Тема 1.2. Базы данных и обработка файлов на Python	7	2 2 2 2	08.10.2025 10.10.2025 15.10.2025 17.10.2025
3.		Тема 1.3. Основы параллельных вычислений и многопоточного программирования	7	2 2 2 3	22.10.2025 24.10.2025 29.10.2025 31.10.2025
4.		Тема 1.4. Создание графических интерфейсов на Python и применению ИИ для разработки программ	8	2 2 2 2 2	05.11.2025 07.11.2025 12.11.2025 14.11.2025 19.11.2025
5.		Промежуточная аттестация по 1 модулю			21.11.2025

6.	Модуль 2. Защита от сетевых атак с применением ИИ	Тема 2.1. Уязвимости сетевых протоколов и их анализ с помощью ИИ	7	2 2 2 2	02.12.2025 03.12.2025 05.12.2025 10.12.2025
7.		Тема 2.2. Анализ и перехват трафика с применением ИИ	7	2 2 2 2	12.12.2025 17.12.2025 19.12.2025 24.12.2025
8.		Тема 2.3. ARP-атаки и сниффинг	7	2 2 2 3	26.12.2025 14.01.2026 16.01.2026 17.01.2026
9.		Тема 2.4. Защита сетевых ресурсов с применением ИИ	8	2 2 2 2 2	20.01.2026 21.01.2026 23.01.2026 28.01.2026 29.01.2026
10.		Промежуточная аттестация по 2 модулю			30.01.2026
11.	Модуль 3. Безопасность веб-приложений с применением ИИ	Тема 3.1. Эксплуатация уязвимостей веб-приложений с помощью ИИ	7	2 2 2 2	04.02.2026 06.02.2026 11.02.2026 13.02.2026
12.		Тема 3.2. Защита баз данных с применением ИИ	7	2 2 2 2	18.02.2026 20.02.2026 25.02.2026 27.02.2026
13.		Тема 3.3. Аутентификация и атаки на сессии с применением ИИ	7	2 2 2 3	04.03.2026 06.03.2026 11.03.2026 13.03.2026

14.		Тема 3.4. Защита и и противодействие атакам на веб-приложения с помощью ИИ	8	2 2 2 2 2	18.03.2026 20.03.2026 24.03.2026 25.03.2026 26.03.2026
15.		Промежуточная аттестация по 3 модулю			27.03.2026
16.	Модуль 4. Комплексная безопасность информационных систем с применением ИИ	Тема 4.1. Цифровая экспертиза с применением ИИ	7	2 2 2 2	30.03.2026 01.04.2026 03.04.2026 08.04.2026
17.		Тема 4.2. Манипулятивные атаки с применением ИИ	7	2 2 2 2	10.04.2026 15.04.2026 17.04.2026 22.04.2026
18.		Тема 4.3. Обход системы защиты и противодействие этому с помощью ИИ	7	2 2 2 3	24.04.2026 29.04.2026 06.05.2026 08.05.2026
19.		Тема 4.4. Безопасные системы с применением ИИ	8	2 2 2 2 2	13.05.2026 15.05.2026 20.05.2026 22.05.2026 23.05.2026
20.		Промежуточная аттестация по 4 модулю			25.05.2026
21.	Итоговый контроль/аттестация по ДОП			4	27.05.2026
22.	Итого по ДОП:			148	
23.	ИТиСИ				

***количество занятий не включают часы, отведенные на самостоятельное изучение, и часы, отведенные на прохождение аттестации**

6. Учебно-методические материалы

Наименование поля	**Значение полей**	**Значение полей**	**Значение полей**	**Значение полей**
Порядковый номер модуля	**1**	**2**	**3**	**4**
Методы, формы и технологии	освоение содержания модуля предполагает использование -объяснительно-иллюстративных, наглядных, проблемных, практических и проектных методов обучения. - синхронных и асинхронных форматов обучения с использованием дистанционных технологий, - лекций, практических занятий, самостоятельной работы, - индивидуальной. групповой и фронтальной форм организации обучения - технологий «перевернутого класса»,	освоение содержания модуля предполагает использование -объяснительно-иллюстративных, наглядных, проблемных, практических и проектных методов обучения. - синхронных и асинхронных форматов обучения с использованием дистанционных технологий, - лекций, практических занятий, самостоятельной работы, - индивидуальной. групповой и фронтальной форм организации обучения - технологий «перевернутого класса», геймификация, кейс-	освоение содержания модуля предполагает использование -объяснительно-иллюстративных, наглядных, проблемных, практических и проектных методов обучения. - синхронных и асинхронных форматов обучения с использованием дистанционных технологий, - лекций, практических занятий, самостоятельной работы, - индивидуальной. групповой и фронтальной форм организации обучения - технологий	освоение содержания модуля предполагает использование -объяснительно-иллюстративных, наглядных, проблемных, практических и проектных методов обучения. - синхронных и асинхронных форматов обучения с использованием дистанционных технологий, - лекций, практических занятий, самостоятельной работы, - индивидуальной. групповой и фронтальной форм организации обучения

	геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного обучения	технология, онлайн-конференция, технология проектного обучения, технология проблемного обучения	«перевернутого класса», геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного обучения	- технологий «перевернутого класса», геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного обучения
Методические разработки	реализация модуля предусматривает авторские разработки лекционных материалов (рабочих листов, презентаций, конспектов); заданий, видеоинструкций, скринкастов, гайдов для организации и реализации практических занятий и самостоятельной работы.	реализация модуля предусматривает авторские разработки лекционных материалов (рабочих листов, презентаций, конспектов); заданий, видеоинструкций, скринкастов, гайдов для организации и реализации практических занятий и самостоятельной работы.	реализация модуля предусматривает авторские разработки лекционных материалов (рабочих листов, презентаций, конспектов); заданий, видеоинструкций, скринкастов, гайдов для организации и реализации практических занятий и самостоятельной работы.	реализация модуля предусматривает авторские разработки лекционных материалов (рабочих листов, презентаций, конспектов); заданий, видеоинструкций, скринкастов, гайдов для организации и реализации практических занятий и самостоятельной работы.
Материалы модуля	материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, видеоролики, задания для	материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, видеоролики, задания для практикумов с	материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий,	материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий,

	практикумов с пошаговыми инструкциями, видеоинструкциями и скринкастами, критериями для формирующего оценивания; задания, инструкции, видеоинструкции для самостоятельной работы учащихся, критерии качества работы, тестовые задания для промежуточного контроля и итоговой аттестации, список основной и дополнительной литературы, электронных информационных и образовательных ресурсов по теме модуля	пошаговыми инструкциями, видеоинструкциями и скринкастами, критериями для формирующего оценивания; задания, инструкции, видеоинструкции для самостоятельной работы учащихся, критерии качества работы, тестовые задания для промежуточного контроля и итоговой аттестации, список основной и дополнительной литературы, электронных информационных и образовательных ресурсов по теме модуля	видеоролики, задания для практикумов с пошаговыми инструкциями, видеоинструкциями и скринкастами, критериями для формирующего оценивания; задания, инструкции, видеоинструкции для самостоятельной работы учащихся, критерии качества работы, тестовые задания для промежуточного контроля и итоговой аттестации, список основной и дополнительной литературы, электронных информационных и образовательных ресурсов по теме модуля	видеоролики, задания для практикумов с пошаговыми инструкциями, видеоинструкциями и скринкастами, критериями для формирующего оценивания; задания, инструкции, видеоинструкции для самостоятельной работы учащихся, критерии качества работы, тестовые задания для промежуточного контроля и итоговой аттестации, список основной и дополнительной литературы, электронных информационных и образовательных ресурсов по теме модуля
Учебная литература	Изучаем Python. 3-е издание, Марк Лутц. - 830 с.- ISBN:9785932861387. Программируем на Python, Майкл Доусон,	Black Hat Python: программирование для хакеров и пентестеров. 2-е изд. — СПб.:Питер, 2022. — 256 с.: ил. — (Серия	Python. Разработка на основе тестирования. / пер. с англ. Логунов А. В. – М.: ДМК Пресс, 2018. – 622 с.: ил.	Искусство тестирования на проникновение в сеть / пер. с анг. В. С. Яценкова. – М.: ДМК Пресс, 2021. – 310 с.: ил.

	Издательство: Питер,2014. - 416 с. - ISBN 978-5-4461-1386-6. МакГрат, М. Программирование на Python для начинающих / М. МакГрат. - М.: Эксмо, 2015. - 192 с. Саммерфилд, М. Программирование на Python 3. Подробное руководство / М. Саммерфилд. - СПб.: Символ-плюс, 2015. - 608 с. Вордерман, К. Программирование на Python. Иллюстрированное руководство для детей / К. Вордерман, К. Стили, К. Квигли. - М.: Манн, Иванов и Фербер, 2017. - 346 с. Банкрашков, А.В. Программирование для детей на языке Python / А.В. Банкрашков. - М.: АСТ, 2018. - 288 с.	«Библиотека программиста»). Python: быстрый старт. — СПб.: Питер, 2021. — 224 с.: ил. — (Серия «Библиотека программиста»). Python глазами хакера. - СПб.: БХВ-Петербург, 2022. - 176 с.: ил. - (Библиотека журнала «Хакер») Python и анализ данных / пер. с анг. А. А. Слинкина. – М.: ДМК Пресс, 2020. – 540 с.: ил. Python. Лучшие практики и инструменты. — СПб.: Питер, 2021. — 560 с.: ил. — (Серия «Библиотека программиста»).	Python на практике. / Пер. с англ. Слинкин А. А. – М.: ДМК Пресс, 2016. – 338 с.: ил. Python на примерах. Практический курс по программированию. Наука и Техника, 2016. 432 с.: ил. Python. Справочник. Полное описание языка, 3-е издание. : Пер. с англ. СПб.: ООО "Диалектика", 2019. - 896 с.: ил. - Парал. тит. англ. Большая книга проектов Python. — СПб.: Питер, 2022. — 432 с.: ил. — (Серия «Библиотека программиста»). Как устроен Python. Гид для разработчиков, программистов и интересующихся. — СПб.: Питер, 2019. — 272 с.: ил. — (Серия «Библиотека программиста»).	Внутреннее устройство Linux. — 2-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2021. — 400 с.: ил. Восстановление данных. Практическое руководство / К. Касперски, В. А. Холмогоров, К. С. Кирилова. - 2-е изд., перераб. и доп. - СПб.: БХВ-Петербург, 2021. - 288 с.: ил. Вскрытие покажет! Практический анализ вредоносного ПО. — СПб.: Питер, 2018. — 768 с.: ил. — (Серия «Для профессионалов»). Как стать хакером: Сборник практических сценариев, позволяющих понять, как рассуждает злоумышленник / пер. с англ. Д. А. Беликова – М.: ДМК Пресс, 2020. – 380 с.: ил. Командная строка Linux. Полное

				руководство. — СПб.: Питер, 2017. — 480 с.: ил. - (Серия «Для профессионалов»).

7. Материально-технические условия реализации программы

Наименование поля	**Значение полей**	**Значение полей**	**Значение полей**	**Значение полей**
Порядковый номер модуля	**1**	**2**	**3**	**4**
Наименование требуемого оборудования	Компьютер или ноутбук со свободным объемом на жестком диске 30+ Гб. CPU: от 2,2 Мгц, Оперативная память: от 4Гб; Выход в интернет со скоростью 2+ мбит/сек	Компьютер или ноутбук со свободным объемом на жестком диске 30+ Гб. CPU: от 2,2 Мгц, Оперативная память: от 4Гб; Выход в интернет со скоростью 2+ мбит/сек	Компьютер или ноутбук со свободным объемом на жестком диске 30+ Гб. CPU: от 2,2 Мгц, Оперативная память: от 4Гб; Выход в интернет со скоростью 2+ мбит/сек	Компьютер или ноутбук со свободным объемом на жестком диске 30+ Гб. CPU: от 2,2 Мгц, Оперативная память: от 4Гб; Выход в интернет со скоростью 2+ мбит/сек

Наименование требуемого программного обеспечения	Операционная система Windows/MacOS Интерпретатор Python, интегрированная среда разработки (IDE), библиотеки Python, браузер для работы с веб-приложениями, ПО Oracle Virtualbox или VMware Workstation для работы с виртуальными машинами, дистрибутивы Linux (bWAPP, DVWA, Kali Linux) Любой браузер	Операционная система Windows/MacOS Интерпретатор Python, интегрированная среда разработки (IDE), библиотеки Python, браузер для работы с веб-приложениями, ПО Oracle Virtualbox или VMware Workstation для работы с виртуальными машинами, дистрибутивы Linux (bWAPP, DVWA, Kali Linux) Любой браузер	Операционная система Windows/MacOS Интерпретатор Python, интегрированная среда разработки (IDE), библиотеки Python, браузер для работы с веб-приложениями, ПО Oracle Virtualbox или VMware Workstation для работы с виртуальными машинами, дистрибутивы Linux (bWAPP, DVWA, Kali Linux) Любой браузер	Операционная система Windows/MacOS Интерпретатор Python, интегрированная среда разработки (IDE), библиотеки Python, браузер для работы с веб-приложениями, ПО Oracle Virtualbox или VMware Workstation для работы с виртуальными машинами, дистрибутивы Linux (bWAPP, DVWA, Kali Linux) Любой браузер
Электронные информационные ресурсы	Selectel — ведущий в России провайдер облачной инфраструктуры и услуг дата-центров. Общество с ограниченной ответственностью «Сеть дата-центров «Селектел» Официальный сайт - URL: https://selectel.ru Санкт-Петербург, (дата обращения: 06.07.2025) - Текст: электронный. 7 полезных книг по Python для старта и	Selectel — ведущий в России провайдер облачной инфраструктуры и услуг дата-центров. Общество с ограниченной ответственностью «Сеть дата-центров «Селектел» Официальный сайт - URL: https://selectel.ru Санкт-Петербург, (дата обращения: 06.07.2025) - Текст: электронный. Отмена пользовательских	Перехват и анализ сетевого трафика. Общество с ограниченной ответственностью "Аудит-Новые Технологии" Официальный сайт - URL: https://newtechaudit.ru/ Санкт-Петербург, (дата обращения: 06.07.2025) - Текст: электронный. Перехват и анализ сетевого трафика с	Лучшие дистрибутивы для тестирования на проникновение. АО “Синклит" Официальный сайт - URL: https://owasp.org/www-chapter-moscow/.- Москва, (дата обращения: 06.07.2025) - Текст: электронный. Лучшие дистрибутивы для проведения тестирования на проникновение. Блог о

	развития навыков: выбор сотрудников Selectel.Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/companies/selectel/articles/693800/ (дата обращения: 06.07.2025) - Текст: электронный. Сбер — крупнейший банк в России. Сбертех, АО Официальный сайт - URL: https://sbertech.ru/ Санкт-Петербург, (дата обращения: 06.07.2025) - Текст: электронный. Лучшие книги по Python 2021-2022 года: для новичков и профи. Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/companies/sberbank/articles/679852/(дата обращения:	паролей. Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/companies/selectel/articles/112794/ (дата обращения: 06.07.2025) - Текст: электронный. Selectel — ведущий в России провайдер облачной инфраструктуры и услуг дата-центров. Общество с ограниченной ответственностью «Сеть дата-центров «Селектел» Официальный сайт - URL: https://selectel.ru Санкт-Петербург, (дата обращения: 06.07.2025) - Текст: электронный. Селектел и открытое программное обеспечение. Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. -	помощью библиотеки pcap. Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/articles/550148/ (дата обращения: 06.07.2025) - Текст: электронный.	кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/articles/276477/ (дата обращения: 06.07.2025) - Текст: электронный.

	06.07.2025) - Текст: электронный.	Москва. - URL: https://habr.com/ru/companies/selectel/articles/197814/ (дата обращения: 06.07.2025) - Текст: электронный. Selectel — ведущий в России провайдер облачной инфраструктуры и услуг дата-центров. Общество с ограниченной ответственностью «Сеть дата-центров «Селектел» Официальный сайт - URL: https://selectel.ru Санкт-Петербург, (дата обращения: 06.07.2025) - Текст: электронный. Отмена пользовательских паролей. Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/companies/selectel/articles/112794/ (дата обращения: 06.07.2025) - Текст:		

		электронный.		
Электронные образовательные ресурсы	Сайт pythonchik.ru — обучение основам Python - Москва. - URL: https://pythonchik.ru/osnovy/___(дата обращения: 06.07.2025) - Текст: электронный. Простым языком об HTTP. Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/post/215117/(дата обращения: 06.07.2025) - Текст: электронный.	Лабораторная работа в Packet Tracer. Блог о кибербезопасности"Habr". Positive Technologies: официальный сайт.- Москва. - URL: https://habr.com/ru/post/350720/ (дата обращения: 06.07.2025) - Текст: электронный. Практическое задание в Cisco Packet Tracer. http://ncti.ru/files/studentu/Olimpiada/zadanie_II_.pdf (дата обращения: 06.07.2025) - Текст: электронный. Easy-Network - обучающий курс по сетевым технологиям. Лабораторные работы по Cisco CCNA. URL: https://easy-network.ru/zadaniya.html (дата обращения: 06.07.2025) - Текст: электронный. Форум информационной	PortSwigger: официальный сайт. - URL: https://portswigger.net/web-security (дата обращения: 06.07.2025) - Текст: электронный. TryHackMe - тренинг по кибербезопасности: официальный сайт. - Лондон. - URL: https://tryhackme.com/(дата обращения: 06.07.2025) - Текст: электронный. HACKTHEBOX URL: https://www.hackthebox.com/__(дата обращения: 06.07.2025) - Текст: электронный.	TryHackMe - тренинг по кибербезопасности: официальный сайт. - Лондон. - URL: https://tryhackme.com/(дата обращения: 06.07.2025) - Текст: электронный. Блог “NetSkills” URL: http://blog.netskills.ru/ (дата обращения: 06.07.2025) - Текст: электронный.

		безопасности - CODEBY.NET.____URL: https://codeby.net/threads/cisco-ccna-1-2019-zadanija-v-cisco-packet-tracer.69507/_____(дата обращения: 06.07.2025) - Текст: электронный.		