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: первые шаги с Python и ИИ»

(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: первые шаги с Python и ИИ»

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

2. Пояснительная записка

Наименование поля	**Значение поля (примеры)**
Название программы (курса)	«Этичный хакинг: первые шаги с Python и ИИ»
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: не требуются специфические знания и навыки в программировании; предполагается наличие знаний школьной программы по математике и информатике на уровне не ниже 8 класса, логическое мышление на базовом уровне, общая цифровая грамотность.
Описание программы	Использование одного из самых популярных языков программирования Python для обеспечения информационной безопасности является перспективным IT направлением в условиях современных реалий цифровой экономики. Этичный хакинг – это выстраивание эффективной защиты на основе глубинного понимания методов и инструментов действиям злоумышленников. Специалисты по кибербезопасности (этичные хакеры) моделируют взломы систем безопасности, проводят тесты на уязвимость, придумывают новые способы проверки, используя для этого язык программирования Python и системы искусственного интеллекта. Данная программа поможет школьникам попробовать себя в роли этичного хакера, а также позволит научиться использовать язык программирования Python для решения различных задач обеспечения информационной безопасности. 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: первые шаги с Python и ИИ» (начальный уровень) Программа «Этичный хакинг: первые шаги с Python и ИИ» (начальный уровень) формирует базовые компетенций в области этичного хакинга, программирования на Python и применения искусственного интеллекта для защиты данных через практико-ориентированное обучение, развитие цифровой грамотности и осознанного подхода к кибербезопасности. В рамках обучения по Программе учащиеся познакомятся: с основами кибербезопасности; с принципами и инструментами программирования, несложными алгоритмами, с ролью ИИ в кибербезопасности; освоят элементы выбранного языка программирования и способы организации данных на соответствующем уровне сложности; применят полученных знания и умения для решения комплексных задач на соответствующем уровне сложности, используя библиотеки и внешние данные. У учащихся будет сформирован навык применения всех полученных знаний и умений для создания простых приложений в выбранной прикладной области. Учащиеся будут уметь: писать простые программы с использованием основных синтаксических конструкций языка Python; создавать собственные функции, импортировать модули и использовать стандартные функции Python; разрабатывать программы для решения простых задач на Python; использовать условные операторы (if, elif, else) для принятия решений в программе; идентифицировать угрозы информационной безопасности; проводить оценку уязвимостей информационных систем; использовать Python для сетевой безопасности; проводить этичные тесты на проникновение; устанавливать и настраивать виртуальную машину bWAPP; создавать безопасные пароли и проверять их; шифровать и расшифровывать файлы; создавать уязвимое приложение на Python; использовать различные алгоритмы хэширования паролей;

	анализировать методы защиты данных в веб-приложениях; осуществлять анализ этичности существующих веб-сайтов; умение устанавливать и настраивать операционную систему Kali Linux; создавать рабочую среду для тестирования; работать с уязвимой виртуальной машиной DVWA; формулировать рекомендации по устранению уязвимостей. 56% учебного времени Программы (84 ак.ч.) отводится на практические занятия на отработку практических навыков и умений. Программа ориентирована на развитие критического мышления, аналитических способностей и креативности учащихся: разбор реальных кейсов утечек данных; оценка рисков и уязвимостей; создание собственных инструментов для пентеста; на развитие алгоритмического мышления: проектирование решений для защиты систем; оптимизация кода для анализа данных; на развитие познавательной активности школьников: поиск и выделение необходимой информации, структурирование знаний, самостоятельное создание алгоритмов деятельности при решении проблем творческого и поискового характера; на развитие технических способностей обучающегося, логики, внимания, памяти, воображения, мотивации к дальнейшему изучению программирования. В результате обучения участники программы освоят базовые навыки разработки на языке Python, научатся использовать этот язык программирования для защиты информационных систем от кибератак, приобретут опыт использования систем ИИ для целей разработки программ на Python и этичного хакинга.
Цель программы	формирование базовых компетенций в области этичного хакинга, программирования на Python и применения искусственного интеллекта для защиты данных через практико-ориентированное обучение, развитие цифровой грамотности и осознанного подхода к кибербезопасности.
Задачи программы	*Обучающие:* ➢ ознакомление с основами кибербезопасности; с основными принципами и инструментами программирования, несложными алгоритмами, формирование первоначальных практических навыков; ➢ ознакомление с ролью ИИ в кибербезопасности; ➢ освоение элементов выбранного языка программирования и способов организации данных на соответствующем уровне сложности;

	➢ формирование навыков применения полученных знаний и умений для решения комплексных задач на соответствующем уровне сложности, использование библиотек и внешних данных; ➢ формирование навыков применения всех полученных знаний и умений для создания простых приложений в выбранной прикладной области. *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. В условиях цифровизации и роста киберугроз знание основ информационной безопасности становится критически важным навыком. Программа «Этичный хакинг: первые шаги с Python и ИИ» отвечает на ключевые вызовы цифровой эпохи, на запрос подростков, интересующихся IT, но не имеющих специализированной подготовки. Вот почему она особенно актуальна для подростков: 1. Цифровая реальность требует новых навыков: киберугрозы растут. Ежедневно происходят тысячи атак на персональные данные, соцсети и игры, которыми пользуются подростки (взлом аккаунтов, фишинг, DoS-атаки). Гаджеты — часть жизни подростков, которые активно используют смартфоны, но редко задумываются о безопасности. Программа учит защищать себя в цифровом мире. 2. Python и ИИ — ключевые технологии будущего: - Python – №1 для начинающих: Простой синтаксис позволяет быстро начать программировать, а его применение в хакинге (например, для анализа уязвимостей) делает обучение практичным. - ИИ — главный тренд: ChatGPT, нейросети для распознавания аномалий в сети — подростки видят эти технологии в жизни и хотят понимать, как они работают. Использование Python (одного из самых популярных языков) и элементов искусственного интеллекта (ИИ) делает курс современным и практико-ориентированным, соответствующим трендам в области кибербезопасности. Системы с ИИ позволяют ускорить процесс разработки программ и возможности этичного хакинга. 3. Профориентация в востребованной сфере: - нехватка специалистов в сфере IT-технологий. В мире более 3 млн незакрытых вакансий в кибербезопасности. Россия активно развивает ИТ-суверенитет, спрос на этичных хакеров будет расти. 4. Популярность хакинга в медиа. Соответствие запросам поколения Z и Alpha. Легальная альтернатива «тёмному» хакингу, так как многие подростки экспериментируют со взломом «из интереса», а данная ДОП направляет компетентность подростка в правовое русло. Отличительные особенности ДОП заключаются в том, что программа включает реальные

	кейсы: защита Wi-Fi, анализ вредоносных ссылок. Содержание курса выстроено так, что обучающийся учится работать и в офлайн (локальные сети), и в онлайне (облачные сервисы), что соответствует привычной среде подростков. Программа не просто дает актуальные навыки – она соединяет интерес подростков (гаджеты, игры, соцсети) с перспективной профессией, учит ответственности в цифровом мире и открывает путь в высокооплачиваемую IT-сферу. Это не «скучные лекции», а первый шаг в мир этичного хакинга через Python и ИИ — так, как это близко поколению Z. 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. 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 общеразвивающая 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	Начальный
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	В результате освоения программы выпускники будут знать: ➢ основы языка Python ➢ различные типы данных в Python: числа, строки, списки и словари ➢ основы создания функций в Python и передачи аргументов в них ➢ концепции обработки исключений и ее применение для предотвращения сбоев программы при возникновении ошибок ➢ основные понятия в информационной безопасности ➢ сущность этичного хакинга ➢ типы хакерских атак и методы защиты от них ➢ клиент-серверная архитектура ➢ протоколы HTTP и HTTPS ➢ основы HTML и CSS. ➢ уязвимости веб-приложений и методы их обнаружения ➢ сертификаты SSL/TLS ➢ этические принципы веб-разработки ➢ пентестинг и его цели ➢ инструменты ОС Kali Linux ➢ основы создания автоматизированных скриптов на Python с помощью ИИ Выпускники будут уметь: ➢ писать простые программы с использованием основных синтаксических конструкций языка Python ➢ создавать собственные функции, импортировать модули и использовать стандартные функции Python ➢ разрабатывать программы для решения простых задач на Python ➢ использовать условные операторы (if, elif, else) для принятия решений в программе

	➢ идентифицировать угрозы информационной безопасности, ➢ проводить оценку уязвимостей информационных систем. ➢ использовать Python для сетевой безопасности ➢ проводить этичные тесты на проникновение ➢ устанавливать и настраивать виртуальную машину bWAPP. ➢ создавать безопасные пароли и проверять их ➢ шифровать и расшифровывать файлы ➢ создавать уязвимое приложение на Python. ➢ использовать различные алгоритмы хэширования паролей. ➢ анализировать методы защиты данных в веб-приложениях ➢ осуществлять анализ этичности существующих веб-сайтов ➢ умение устанавливать и настраивать операционную систему Kali Linux ➢ создавать рабочую среду для тестирования ➢ работать с уязвимой виртуальной машиной DVWA. ➢ формулировать рекомендации по устранению уязвимостей
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. Основы Python для кибербезопасности и искусственный интеллект.	Формирование базовых знаний и практических навыков работы с языком программирования Python, необходимых для применения в области кибербезопасности.	Формирование компетенций в области программирования на Python для кибербезопасности: знания теоретических основ языка, навыки работы с различными типами данных и базовыми операциями, практические умения создания программ на Python, навыки работы с функциями и модулями языка, обработки исключений и работы с файлами, а также понимание возможностей искусственного интеллекта при разработке программ.	Создание программ для выполнения базовых математических операций, разработка простых приложений на Python для решения практических задач, работа с различными типами данных и условными операторами, написание пользовательских функций и использование модулей, выполнение операций с файлами и обработка исключений, а также задачи на применение искусственного интеллекта для генерации и анализа кода.
Модуль 2.	Формирование базовых знаний и практических навыков в области	Формирование комплексных компетенций в области	Выполнение практических заданий по анализу уязвимостей

Основы информационной безопасности с элементами ИИ и работа с компьютерными сетями	информационной безопасности и работы с компьютерными сетями, включая применение технологий искусственного интеллекта.	информационной безопасности и работы с компьютерными сетями: теоретическое понимание ключевых концепций кибербезопасности, умение выявлять и анализировать различные типы угроз и уязвимостей, практические навыки определения IP-адресов и подсетей с помощью Python, обнаружения активных портов, проведения этичного тестирования на проникновение с использованием специализированных инструментов и виртуальной машины bWAPP, применения методов защиты от хакерских атак, создания надежных паролей и шифрования данных, а также навыки использования технологий искусственного интеллекта для анализа безопасности систем и разработки программных решений.	информационных систем, исследованию методов защиты от вирусов и хакерских атак, задач на определение IP-адресов и подсетей с использованием Python, обнаружение активных портов на удаленных хостах, проведение этического тестирования на проникновение с применением инструментов и технологий искусственного интеллекта, реализация мер защиты от атак через создание надежных паролей и шифрование данных.
Модуль 3. Веб-безопасность и ИИ: обнаружение уязвимостей	Формирование знаний и практических навыков в области обеспечения безопасности веб-приложений с использованием технологий искусственного интеллекта.	Формирование компетенций в области веб-безопасности и применения технологий искусственного интеллекта: теоретическое понимание принципов работы веб-	Разработка простых веб-страниц с использованием HTML и CSS, задачи на выявление и анализ уязвимостей (SQL-инъекции, XSS, CSRF) с применением виртуальной машины bWAPP,

		приложений, клиент-серверной архитектуры, протоколов HTTP/HTTPS, основ HTML и CSS, навыки практической разработки веб-страниц, выявления и анализа уязвимостей (SQL-инъекции, XSS, CSRF) с использованием виртуальной машины bWAPP, создания уязвимых приложений на Python, применения различных методов шифрования и хэширования паролей, а также знание этических аспектов веб-безопасности.	создание уязвимых веб-приложений на Python для исследования методов атак, реализация алгоритмов хэширования паролей и шифрования данных, задачи на сравнение безопасности передачи данных через HTTP и HTTPS, а также разработка рекомендаций по обеспечению этических стандартов и защиты конфиденциальности в веб-приложениях.
Модуль 4. Практический пентестинг с Python и ИИ	Формирование практических навыков проведения тестирования на проникновение с использованием языка Python, специализированных инструментов и технологий искусственного интеллекта.	Формирование комплексных компетенций в области практического пентестинга: теоретическое понимание фаз и типов атак, навыки работы с инструментами в среде Kali Linux, умение настраивать рабочую среду на базе DVWA, автоматизировать задачи пентестинга через скриптинг на Python с использованием библиотек (Scapy, Requests), создавать комплексные решения для тестирования безопасности путем объединения различных инструментов, анализировать результаты	Выполнение практических задач по настройке рабочей среды на базе DVWA, сканированию уязвимостей с использованием инструментов Kali Linux, разработке автоматизированных скриптов на Python для тестирования на проникновение, анализу результатов и составлению отчетов с применением технологий искусственного интеллекта для оптимизации процессов сбора данных, выявления уязвимостей и формулирования рекомендаций по их

		тестирования, составлять детальные отчеты и формулировать рекомендации по устранению уязвимостей с применением технологий искусственного интеллекта для оптимизации процессов сбора данных, анализа уязвимостей и генерации отчетов.	устранению.

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	<u>Промежуточная аттестация по 1 модулю.</u> 1. Что означает алгоритм? 1. Устройство для хранения данных 2. Последовательность шагов для выполнения задачи (Правильный ответ)

	3. Способ обработки ошибок 4. Язык программирования 2. Что такое переменная? 1. Среда разработки 2. Значение, которое может изменяться в программе (Правильный ответ) 3. Комментарий в коде 4. Тип данных 3. Что такое функция? 1. Ошибка в программе 2. Набор переменных 3. Часть программы, выполняющая определенную задачу (Правильный ответ) 4. Условие выполнения цикла 4. Что такое оператор? 1. Специальный символ, указывающий на выполнение определенной операции (Правильный ответ) 2. Структура данных для хранения множества элементов 3. Логическое выражение 4. Описание типа данных 5. Что такое компиляция? 1. Процесс исполнения программы 2. Преобразование исходного кода в машинный код (Правильный ответ) 3. Сохранение программы на диске 4. Редактирование программы 6. Какая управляющая конструкция используется для выполнения определенного блока кода многократно до тех пор, пока условие истинно? 1. if-else

	2. for 3. while (Правильный ответ) 4. switch 7. Какая управляющая конструкция используется для выполнения определенного блока кода, если условие истинно, и альтернативного блока кода, если условие ложно? 1. if-else (Правильный ответ) 2. for 3. while 4. switch 8. Какая управляющая конструкция используется для перебора элементов в последовательности, такой как список или строка? 1. if-else 2. for (Правильный ответ) 3. while 4. switch 9. Необходимо создать программу, которая будет хранить уникальные элементы (например, идентификаторы пользователей). Какую структуру данных следует использовать для решения этой задачи? 1. Список (List) 2. Множество (Set) (Правильный ответ) 3. Кортеж (Tuple) 4. Словарь (Dictionary) 10. Какая структура данных используется для хранения пар ключ-значение? 1. Список (List) 2. Множество (Set) 3. Кортеж (Tuple) 4. Словарь (Dictionary) (Правильный ответ)

	11. Какая структура данных представляет собой неизменяемую последовательность элементов? 1. Список (List) 2. Множество (Set) 3. Кортеж (Tuple) (Правильный ответ) 4. Словарь (Dictionary) 12. Как объявить функцию в Python? 1. def my_function(): (Правильный ответ) 2. function my_function(): 3. define my_function(): 4. func my_function(): 13. Как передать аргументы в функцию в Python? 1. Путем указания их в определении функции в круглых скобках (Правильный ответ) 2. Путем присваивания им значений внутри функции 3. Аргументы передаются автоматически в функцию 4. Аргументы не нужны при вызове функции 14. Что такое возвращаемое значение функции? 1. Результат выполнения функции (Правильный ответ) 2. Количество аргументов функции 3. Тип данных функции 4. Имя функции 15. Как вызвать функцию в Python? 1. my_function() (Правильный ответ) 2. call my_function() 3. execute my_function()

	4. run my_function() 16. Функция для чтения всего содержимого файла в строку. Ответ: read() 17. Ключевое слово для создания анонимной функции. Ответ: lambda 18. Что выведется на экран в результате работы данной программы? a = 5 b = 7 print(a+b*a) Ответ: 40 19. С помощью какого ключевого слово можно объявить функцию в Python? Ответ: def 20. Что выведется на экран в результате работы данной программы? def add(a, b): return a + b result = add(2, 3) print(result) Ответ: 5 <u>Промежуточная аттестация по 2 модулю:</u> 1. Каковы основные аспекты информационной безопасности согласно триаде информационной безопасности? 1. Конфиденциальность, работоспособность, корректность 2. Секретность, функционирование, защита 3. <u>Конфиденциальность, целостность, доступность</u>

	4. Полезность, аутентичность, защищенность 2. Потенциальные события или действия, которые могут нанести ущерб информационной системе или данным - это… 1. Риски 2. Угрозы 3. Уязвимости 4. Опасности 3. Слабые места в системе, которые могут быть использованы злоумышленниками для нарушения безопасности - это… 1. Аутентификаторы 2. Уязвимости 3. Баги 4. Риски 4. Фишинг - это… 1. Несанкционированный доступ к аккаунтам администратора 2. Получение идентификаторов пользователей 3. Ошибки при авторизации 4. Атака, основанная на манипуляции пользователем для получения конфиденциальной информации 5. Вирусы - это… 1. Вредоносные программы, которые могут повреждать или уничтожать данные, заражать другие файлы на устройствах 2. Специальные программы, которые направлены для взлома пароля жертвы 3. ПО для кражи личных данных 4. Зловредные программы, маскирующиеся под легитимные 6. Несанкционированный доступ к компьютерным системам с целью получения конфиденциальной информации или нарушения их функциональности - это…

	1. Социальная инженерия 2. Хакерские атаки 3. Взлом персонального компьютера 4. Атака перебора пароля 7. Вы обнаружили, что в вашей локальной сети открыт порт 3389 (RDP), который доступен из внешней сети. Какие меры безопасности вы предпримете для устранения этой уязвимости? Выберите все правильные варианты. 1. Запустить файловый менеджер. 2. Удалить последние обновления операционной системы. 3. Использовать слабые пароли для входа через RDP. 4. Отключить службу удаленного рабочего стола (RDP), если она не требуется. 8. Выберите надежный способ(-ы) защиты информационных систем 1. Регулярное обновление ПО 2. Использование шифрования в данных для их передачи и хранения 3. Использование антивирусного ПО 4. Все ответы верны 9. Для каких задач можно использовать программы на языке Python? 1. Сканирование портов с помощью сокетов 2. Сканирование локальной сети 3. Сканирование локального устройства 4. Для всех перечисленных задач 10. Как называют эксперта по безопасности, который проводит тестирование на проникновение? 1. Безопасный хакер 2. Этичный хакер 3. Корректный взломщик

	4. Разработчик безопасности 11. Какой из перечисленных инструментов является одним из самых распространенных сканеров локальной сети? 1. Nikto 2. Metasploit 3. Burp Suite 4. Nmap 12. Как называется специализированная среда, которая изначально является уязвимой, для проведения тестов на проникновение? 1. Kali Linux 2. Metasploit 3. bWAPP 4. nmap 13. Какая главная причина значимости регулярного обновления ПО и операционных систем: 1. Улучшение пользовательского опыта 2. Добавление новых функций 3. Быстрота системы 4. Устранение известных уязвимостей старых версий 14. С какой целью проводится сканирование безопасности локальной сети: 1. Документирование результатов сканирования и обнаруженных уязвимостей для удобной работы с ними. 2. Разработка рекомендаций по усилению безопасности сети (закрытие портов, установку брандмауэров, обновление ПО) 3. Планирование и внедрение мер безопасности, с учетом полученных рекомендаций и настройки политик безопасности для защиты сети 4. Для всего вышеперечисленного.

15. Какие рекомендации самые эффективные для создания паролей?
    1. Добавление символов и букв разных регистров
    2. Использование длинного пароля
    3. Использование случайно сгенерированного пароля, содержащего в себе буквы, цифры и спецсимволы
    4. Использование специальных символов

16. Как называется атака, при которой злоумышленник пытается получить конфиденциальную информацию, манипулируя пользователем?
Правильный ответ: Фишинг

17. Какой инструмент используется для перехвата сетевого трафика?
Правильный ответ: Wireshark

18. Как называется процесс проверки подлинности пользователя при входе в систему?

Правильный ответ: Аутентификация

19. Какой инструмент используется для сканирования портов в сети?

Правильный ответ: Nmap

20. Как называется операционная система, специально созданная для тестирования на проникновение?
Правильный ответ: Kali Linux

Промежуточная аттестация по 3 модулю:

1. В чем основное отличие HTTP от HTTPS?
    1. Для подключения по HTTP не требуются SSL сертификаты, а для HTTPS нужен подписанный SSL сертификат

	2. HTTP использует порт 80, а HTTPS порт 433 3. HTTP использует шифрование DES, а HTTPS шифрование AES 4. Все ответы верны 2. Стандартизированный язык разметки документов для просмотра веб-страниц в браузере - это? 1. HTTP/HTTPS 2. HTML 3. XSS 4. XML 3. Часть текста/картинки, ссылающаяся на другую часть документа/другую страницу? 1. Заголовок 2. Параграф 3. Гиперссылка 4. Адрес 4. Какие элементы входят в типичную структуру HTML-страницы? 1. Тэги 2. Атрибуты 3. Заголовки 4. Все вышеперечисленное. 5. Формальный язык описания внешнего вида документа, написанного с использованием языка разметки - это? 1. CSS 2. XSS

	3. SVG 4. XML 6. Расширяемый язык разметки - это? 1. XML 2. HTML 3. Python 4. C++ 7. Уязвимость, основанная на недостатках архитектуры веб-сайта при обращении запросов к базам данных - это? 1. XSS-атаки 2. CSRF-атаки 3. SQL-инъекции 4. Brute-force атаки 8. С каким языком программирования в основном связана XSS-уязвимость? 1. SQL 2. Python 3. XML 4. Java Script 9. Атака подделки межсайтовых запросов - это? 1. XSS - межсайтовый скриптинг 2. SQL-инъекция 3. CSRF-атака 4. Brute-force

	10. Для чего используется bWAPP? 1. Демонстрация основных видов уязвимостей 2. Защита сайта от различных атак 3. Это набор инструментов специалиста по пентесту 4. Хранение информации о сайте 11. Чем отличается симметричное и асимметричное шифрование? 1. Симметричное использует один ключ для шифрования и расшифровки, а асимметричное два разных ключа 2. Различие в считывании формирующейся последовательности 3. Симметричное шифрование намного надежнее асимметричного, так как было изобретено позже 4. Симметричное использует два ключа для шифрования и расшифровки, а асимметричное три разных ключа 12. Выберите из названных алгоритмов шифрования симметричные. 1. AES 2. RSA 3. DSA 4. Elgamal 13. Выберите из названных алгоритмов шифрования асимметричные. 1. AES 2. RSA 3. DES 4. 3DES

	14. Какой процесс чаще всего применяется к паролям для их хранения? 1. Шифрование 2. Изменение 3. Хэширование 4. Удаление 15. Выберите из списка алгоритмы хэширования? 1. DES 2. AES 3. MD5 4. RSA 16. Какая организация отвечает за модернизацию языка HTML? 1. WHATWG 2. ECMA 3. Khronos 4. HTML-corp. 17. Какой номер порта по умолчанию используется протоколом HTTPS для безопасной передачи данных? Ответ: 443 18. Сколько алгоритмов хэширования перечислено в списке: MD5, SHA-256, Bcrypt, AES, RSA, DES? Правильный ответ: 3

	19. Как называется тип шифрования, при котором используется один ключ для шифрования и расшифровки данных? (Ответ напишите одним словом.) Правильный ответ: симметричное 20. Как называется процесс одностороннего шифрования? Правильный ответ: хеширование Промежуточная аттестация по 4 модулю: 1. Какие бывают типы атак при пентесте? 1. Социальная инженерия 2. Физические атаки 3. Атаки на веб-ресурсы 4. Пентест может включать в себя все вышеперечисленные атаки 2. Что такое DVWA? 1. Специальное небезопасное веб-приложение для изучения пентеста 2. Специальный набор инструментов для тестирования сайтов 3. Спроектированная система защиты веб-приложения 4. Инструмент перебора паролей. 3. Как определить этические принципы при проведении пентеста? 1. Нельзя взламывать аккаунты пользователей 2. Не проводить атаки на главные сервера сайта/организации. 3. Согласование принципов с владельцами и администраторами 4. Взламывать только друзей

	4. Какая информация требуется тестировщикам безопасности для проведения пентеста? 1. Не требуется никакой дополнительной информации 2. Требуется информация об использующейся операционной системе 3. Нужна вся информация об ОС, версиях ПО и архитектуре внутренней сети 4. Зависит от типа пентеста (black/grey/white box) 5. Какой инструмент чаще всего используется для работы с анализом трафика и перехваченными пакетами? 1. Nikto 2. Metasploit 3. Wireshark 4. Hydra 6. Как называется утилита поиска имен директорий и файлов доступного веб-сервиса? 1. Burp Suite 2. dirbuster 3. Patator 4. Nikto 7. Какая операционная система чаще всего используется тестировщиками на проникновение? 1. Ubuntu Linux 2. Kali Linux 3. Windows Server 4. MacOS 8. Какие инструменты подходят для проведения тестирования безопасности веб-сайта? 1. Burp Suite

	2. Nikto 3. sqlmap 4. Все перечисленные инструменты 9. Как называется программная библиотека для манипулирования сетевыми пакетами на языке программирования Python? 1. Scapy 2. Scrapy 3. Network 4. Packetsend 10. Какая Python библиотека используется для отправки HTTP запросов на сайты? 1. Sockets 2. Requests 3. Sites 4. Packetsend 11. Каким образом фиксируются ход и результаты проведения пентеста? 1. Эксплуатируются найденные уязвимости 2. Публикуются результаты пентеста в вышестоящие органы 3. Формируется внутренний отчет о проведенном тестировании. 4. Делаются заметки в коде 12. Каковы цели проведения пентеста? 1. Закрытие найденных уязвимостей, чтобы повысить уровень безопасности. 2. Это регулярный процесс, обусловленный требованиям законодательства для всех организаций

	3. Формирование отчетности 4. Взлом системы 13. Какой вид тестирования самый эффективный? 1. Ручное тестирование 2. Автоматизированное тестирование 3. Комбинирование ручного и автоматизированного 4. Дымное тестирование 14. Что обычно НЕ входит в отчет о проведенном пентесте? 1. Описание безопасных сервисов компании 2. Рекомендуемые способы устранения уязвимостей 3. Уровень опасности уязвимостей 4. Способ (процесс) обнаружения уязвимостей. 15. Используя инструмент ping, определите IP-адрес сервера по доменному имени localhost. Укажите IP-адрес сервера. Правильный ответ: 127.0.0.1 16. Как называется операционная система, которая чаще всего используется тестировщиками на проникновение? Напишите название этой системы. Правильный ответ: Kali Linux 17. Как называется инструмент, который чаще всего используется для анализа сетевого трафика и перехвата пакетов? Напишите название этого инструмента. Правильный ответ: Wireshark

	18. Как называется утилита, которая помогает находить скрытые директории и файлы на веб-серверах? Напишите название этой утилиты. Правильный ответ: dirbuster 19. Как называются соревнования по поиску уязвимостей и кибербезопасности? Напишите название этих соревнований (сокращение из трех букв). Правильный ответ: CTF 20. Как называется специальное небезопасное веб-приложение, которое используется для изучения пентеста? Напишите название этого приложения. Правильный ответ: DVWA
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. «Flasksiteanalyzer: инструмент анализа сайтов на flask» Задача: предоставление информации о скорости загрузки страницы, DNS параметрах,

	состоянии SSL сертификата, а также выполнить пинг для проверки доступности сайта. 2. «Детектив вирусов» Задача: Скрипт, ищущий подозрительные файлы в папке. 3. «Робот-помощник для RutTube» Задача: Бот, который ищет вредоносные ссылки в комментариях (по ключевым словам «скачать», «бесплатно»). 4. «PyLinkInspector» Задача: Инструмент для проверки безопасности внешних ссылок на веб-страницах с анализом репутации доменов через API (с использованием requests и BeautifulSoup). 5. «Анализатор cookies» Задача: Анализатор параметров безопасности cookies веб-сайтов с проверкой флагов HttpOnly/Secure (Python + Flask интерфейс). 6. «HeaderScanX» Задача: Сканер HTTP-заголовков для выявления недостатков конфигурации безопасности (Content-Security-Policy, HSTS). 7. «Безопасный чат» Задача: Мессенджер с end-to-end шифрованием для демонстрации принципов конфиденциальности (Flask-SocketIO + PyCryptoDome). 8. «Безопасность фотофайлов» Задача: Инструмент для проверки безопасности загружаемых файлов. Анализирует метаданные (EXIF в изображениях), тип файла, и использует простую эвристику (filetype, pandas) для выявления потенциально опасных файлов. 9. «Анализатор рисков» Задача: Инструмент для сканирования и анализа QR-кодов (с веб-камеры через opencv-python или загрузка из файла). Проверяет URL на безопасность (через безопасные API), декодирует информацию и предупреждает о потенциальных рисках (фишинг, вредоносные ссылки). 10. «Анализатор мэмов» Задача: Инструмент анализа популярных мемов/картинок из безопасных источников на предмет скрытого текста (стенография - LSB на примере) или потенциально вредоносных ссылок в описании с использованием PIL/OpenCV и requests/BeautifulSoup.

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: первые шаги с Python и ИИ» (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. Основы Python для кибербезопасности и искусственный интеллект.	Тема 1.1. Введение в Python: синтаксис, среды разработки	8	2	5		1	1
2.		Тема 1.2. Типы данных в Python и их применение	8	2	5		1	1
3.		Тема 1.3. Модули и функции языка Python	9	2	5	1	1	1
4.		Тема 1.4. Файлы и исключения в Python, использование ИИ при разработке программ на Python	10	2	6	1	1	1
5.		Промежуточная аттестация по 1 модулю	1				1	
6.	Модуль 2. Основы информационной безопасности	Тема 2.1. Ключевые концепции кибербезопасности	8	2	5		1	1
7.		Тема 2.2.	8	2	5		1	1

	с элементами ИИ и работа с компьютерными сетями	Угрозы безопасности и инструменты для их обнаружения						
8.		Тема 2.3. Этичный хакинг: методы тестирования с помощью ИИ	9	2	5	1	1	1
9.		Тема 2.4. Защита от атак с использованием ИИ	10	2	6	1	1	1
10.		Промежуточная аттестация по 2 модулю	1				1	
11.	Модуль 3. Веб-безопасность и ИИ: обнаружение уязвимостей	Тема 3.1. Основы веб-разработки с применением ИИ	8	2	5		1	1
12.		Тема 3.2. XSS, SQL-инъекции, и другие атаки: как ИИ помогает в защите	8	2	5		1	1
13.		Тема 3.3. Шифрование и безопасное хранение данных с применением ИИ	9	2	5	1	1	1
14.		Тема 3.4. Этические аспекты веб-безопасности с использованием ИИ	10	2	6	1	1	1
15.		Промежуточная аттестация по 3 модулю	1				1	
16.	Модуль 4. Практический пентестинг с Python и ИИ	Тема 4.1. Основы пентестинга: ручное и автоматизированное с ИИ	8	2	5		1	1
17.		Тема 4.2. Инструменты для пентеста, включая ИИ	8	2	5		1	1
18.		Тема 4.3. Автоматизация пентестинга на Python с использованием ИИ	9	2	5	1	1	1

19.		Тема 4.4. Анализ результатов и генерация отчетов с помощью 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: первые шаги с Python и ИИ» (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. Основы Python для кибербезопасности и искусственный интеллект. Описание модуля: *Модуль направлен на изучение основ языка Python, его ключевых особенностей и преимуществ. В рамках курса вы познакомитесь с выбором*	Тема 1.1. Введение в Python: синтаксис, среды разработки	Введение в язык Python: основные особенности и преимущества его использования, сферы применения. Общее представление о синтаксисе языка. Установка Python на компьютер, выбор и настройка интегрированной среды разработки, а также запуск и выполнение программ в выбранной IDE. Рассмотрение базовых синтаксических конструкций, понятия переменных и присвоения им значений. Изучение простейших типов данных - числа, строки, списки - и операций над ними: сложение, вычитание, умножение, деление, возведение в степень. Практические примеры работы с	теоретические занятия	2

и настройкой интегрированной среды разработки (IDE), установкой и запуском Python. Вы освоите базовые синтаксические конструкции, научитесь работать с разными типами данных и выполнять операции над ними, а также создавать программы на Python. Цель модуля: *Формирование базовых знаний и практических навыков работы с языком программирования Python, необходимых для применения в области кибербезопасности* Планируемые результаты: *Формирование компетенций в области программирования на Python для кибербезопасности: знания теоретических основ языка, навыки работы с различными типами данных и базовыми операциями, практические умения создания программ на Python, навыки работы с функциями и модулями языка, обработки исключений и работы с файлами, а также понимание возможностей искусственного интеллекта при разработке программ.* Типы задач/деятельности: *Создание программ для выполнения базовых математических операций,*		переменными и использованием арифметических операций.		
		Создание программ для выполнения базовых математических операций: сложение, вычитание, умножение и деление чисел.	практические занятия	5
		Разработка простой программы на языке Python, предназначенной для решения базовой задачи: вычисления среднего значения чисел	текущий контроль	1
	Тема 1.2. Типы данных в Python и их применение	Основные типы данных в Python: целые числа, числа с плавающей точкой, строки, списки и словари. Объявление и работа с этими типами в программе. Выполнение различных операций: арифметические действия и манипуляции со строками. Использование условных операторов (if, elif, else) для принятия решений в зависимости от заданных условий.	теоретические занятия	2
		Различные типы данных, выполнение операций над ними. Создание условных конструкций для принятия решений в программе. Примеры практических задач: разработка конвертера температуры и вычисление суммы чисел в списке.	практические занятия	5
		Создание программы, использующих различные типы данных и условные операторы для решения задач. Вычисление площади и периметра прямоугольника.	текущий контроль	1
	Тема 1.3. Модули и функции языка Python	Ознакомление с основами создания функций в Python и передачей аргументов в них. Изучение использования ключевого слова def для определения функции, указания её имени и списка параметров. Рассмотрение принципов передачи аргументов при вызове функций.	теоретические занятия	2
		Разработка и применение пользовательских функций в Python, подключение модулей и использование встроенных стандартных функций языка. Создание программы-генератора паролей.	практические занятия	5

разработка простых приложений на Python для решения практических задач, работа с различными типами данных и условными операторами, написание пользовательских функций и использование модулей, выполнение операций с файлами и обработка исключений, а также задачи на применение искусственного интеллекта для генерации и анализа кода.		Доработка ранее написанных программ с использованием функций и модулей.	самостоятельная работа текущий контроль	1 1
	Тема 1.4. Файлы и исключения в Python, использование ИИ при разработке программ на Python	Работа с файлами в языке Python: открытие, чтение и запись данных. Изучение основных методов работы с текстовыми файлами и операций над файловыми объектами. Введение в обработку исключений — защита программы от сбоев при возникновении ошибок и обеспечение гибкого управления исключительными ситуациями. Виды искусственного интеллекта, включая GPT-модели, способы взаимодействия с ИИ, а также практические примеры: использование искусственного интеллекта для генерации программного кода и объяснения его работы.	теоретические занятия	2
		Работа с файлами в Python: чтение данных и вывод их на экран, запись информации в файл. Применение механизма обработки исключений для предотвращения ошибок, включая деление на ноль. Освоение подходов к автоматической генерации кода с помощью ИИ и его сравнение с ручным способом написания программ.	практические занятия	6
		Разработка программ с использованием искусственного интеллекта, выполняющих обработку данных в файлах с корректной обработкой возможных исключений. Подсчёт количества строк в файле и копирование содержимого из одного файла в другой.	самостоятельная работа текущий контроль	1 1
	Промежуточная аттестация по 1 модулю	Тестирование		1
Модуль 2. Основы информационной безопасности с элементами	Тема 2.1. Ключевые концепции кибербезопасности	Введение в основные понятия информационной безопасности: конфиденциальность, целостность и доступность информации. Рассмотрение понятия угроз, их классификация и влияние на безопасность данных.	теоретические занятия	2

ИИ и работа с компьютерными сетями Описание модуля: *В рамках данного модуля происходит первоначальное ознакомление с основами информационной безопасности: изучаются ключевые понятия, сущность этичного хакинга, базовые угрозы и методы защиты информации; осваиваются навыки определения IP-адресов и подсетей с использованием Python и искусственного интеллекта; способы настройки защиты от хакерских атак, создания надежных паролей, а также шифрования файлов.* Цель модуля: *Формирование базовых знаний и практических навыков в области информационной безопасности и работы с компьютерными сетями, включая применение технологий искусственного интеллекта.* Планируемые результаты: *Формирование комплексных компетенций в области информационной безопасности и работы с компьютерными сетями: теоретическое понимание ключевых концепций кибербезопасности, умение выявлять*		Основные виды угроз — вирусы, хакерские атаки, методы социальной инженерии. Понятие уязвимостей и их роль в обеспечении информационной безопасности.		
		Ознакомление с различными угрозами информационной безопасности, такими как вирусы, хакерские атаки и фишинг. Определение возможных последствий воздействия этих угроз. Рассмотрение методов распознавания нескольких типов угроз и анализа их потенциального влияния на безопасность данных и систем.	практические занятия	5
		Проведение оценки уязвимостей в различных средах — информационных системах, компьютерах и мобильных приложениях — с точки зрения обеспечения информационной безопасности. Выявление возможных слабых мест, связанных с физической защитой, сетевыми конфигурациями, программным обеспечением, а также человеческим фактором.	текущий контроль	1
	Тема 2.2. Угрозы безопасности и инструменты для их обнаружения	Рассмотрение основных угроз безопасности в информационных системах, таких как вирусы, трояны, хакерские атаки и методы социальной инженерии. Изучение базовых способов защиты: применение надёжных паролей, шифрование данных, своевременное обновление программного обеспечения. Ознакомление с ролью брандмауэров и антивирусных программ как ключевых инструментов обеспечения информационной безопасности.	теоретические занятия	2
		Определение IP-адресов и подсетей при помощи программ на Python. Обнаружение активных портов на удалённом хосте с использованием скрипта, написанного на Python и сгенерированного с помощью искусственного интеллекта.	практические занятия	5

и анализировать различные типы угроз и уязвимостей, практические навыки определения IP-адресов и подсетей с помощью Python, обнаружения активных портов, проведения этичного тестирования на проникновение с использованием специализированных инструментов и виртуальной машины bWAPP, применения методов защиты от хакерских атак, создания надежных паролей и шифрования данных, а также навыки использования технологий искусственного интеллекта для анализа безопасности систем и разработки программных решений. <u>Типы задач/деятельности:</u> *Выполнение практических заданий по анализу уязвимостей информационных систем, исследованию методов защиты от вирусов и хакерских атак, задач на определение IP-адресов и подсетей с использованием Python, обнаружение активных портов на удаленных хостах, проведение этического тестирования на проникновение с применением инструментов и технологий искусственного интеллекта, реализация мер защиты от атак через создание надежных паролей и шифрование данных.*		Выявление открытых портов на домашнем компьютере с использованием скрипта, разработанного на языке Python.	текущий контроль	1
	<u>Тема 2.3.</u> Этичный хакинг: методы тестирования с помощью ИИ	Этичный хакинг как метод улучшения безопасности систем. Рассмотрение основных типов хакерских атак, таких как фишинг, использование вредоносных программ и перехват данных. Изучение этичных методов тестирования на проникновение, применяемых специалистами по защите информации (пентестерами) в рамках обеспечения кибербезопасности.	теоретические занятия	2
		Выполнение этических тестов на проникновение с использованием специализированных инструментов, включая средства на основе искусственного интеллекта. Установка и настройка виртуальной машины bWAPP для практического исследования уязвимостей и отработки навыков тестирования безопасности.	практические занятия	5
		Выполнение самостоятельных исследований по выявлению уязвимостей на виртуальной машине bWAPP с использованием инструментов и технологий на основе искусственного интеллекта.	самостоятельная работа текущий контроль	1 1
	<u>Тема 2.4.</u> Защита от атак с использованием ИИ	Изучение основных методов защиты от хакерских атак: применение брандмауэров и антивирусного программного обеспечения, регулярное обновление операционных систем и приложений, использование многофакторной аутентификации. Рассмотрение принципов создания безопасных паролей — включая формирование сложных, длинных комбинаций с использованием букв, цифр и специальных символов, избегание личных данных и распространённых слов. Ознакомление с ролью шифрования данных в обеспечении конфиденциальности и защите информации.	теоретические занятия	2

		Реализация мер защиты от хакерских атак, включая создание надёжных паролей и шифрование файлов. Разработка программ на языке Python с использованием ИИ для анализа паролей на устойчивость к взлому и выполнения операций шифрования данных.	практические занятия	6
		Проверка собственных паролей с использованием разработанной программы для оценки их надёжности. Выполнение тестового шифрования и расшифрования файлов на домашнем компьютере как с помощью созданной программы, так и при помощи инструментов на основе искусственного интеллекта.	самостоятельная работа текущий контроль	1 1
	Промежуточная аттестация по 2 модулю	Тестирование		1
Модуль 3. Веб-безопасность и ИИ: обнаружение уязвимостей Описание модуля: *В рамках данного модуля основное внимание уделяется безопасности веб-сервисов. Изучаются клиент-серверная архитектура, протоколы HTTP и HTTPS, их отличия, а также основы HTML для структурирования веб-контента и язык стилей CSS. Рассматриваются распространённые уязвимости веб-приложений, такие как SQL-инъекции, XSS- и CSRF-атаки, и способы защиты от них, включая использование протокола HTTPS для безопасной передачи данных.*	Тема 3.1. Основы веб-разработки с применением ИИ	Рассмотрение клиент-серверной архитектуры, основных протоколов передачи данных — HTTP и HTTPS, а также их ключевых различий. Изучение базовых понятий языка HTML для определения структуры веб-контента и каскадных таблиц стилей (CSS) для оформления и форматирования веб-страниц.	теоретические занятия	2
		Разработка простых веб-страниц и работа с HTML- и CSS-кодом: создание заголовков и параграфов, добавление изображений, стилизация текста с помощью CSS, реализация базовой навигации и форм. Настройка и запуск собственного веб-сервера на языке Python. Использование искусственного интеллекта для генерации кода и ускорения разработки.	практические занятия	5
		Создание собственной веб-страницы с применением изученных принципов HTML и CSS, а также с использованием искусственного интеллекта для ускорения разработки и оптимизации кода.	текущий контроль	1
	Тема 3.2.	Изучение распространённых уязвимостей веб-приложений, таких как SQL-инъекции, XSS- и CSRF-атаки.	теоретические занятия	2

Обучающиеся осваивают навыки разработки веб-страниц, работы с HTML и CSS, выявления и анализа уязвимостей на виртуальной машине bWAPP создания простого веб-приложения на Python, уязвимого к XSS-атаке, а также применения различных алгоритмов хэширования паролей. <u>Цель модуля:</u> *Формирование знаний и практических навыков в области обеспечения безопасности веб-приложений с использованием технологий искусственного интеллекта.* <u>Планируемые результаты:</u> *Формирование компетенций в области веб-безопасности и применения технологий искусственного интеллекта: теоретическое понимание принципов работы веб-приложений, клиент-серверной архитектуры, протоколов HTTP/HTTPS, основ HTML и CSS, навыки практической разработки веб-страниц, выявления и анализа уязвимостей (SQL-инъекции, XSS, CSRF) с использованием виртуальной машины bWAPP, создания уязвимых приложений на Python, применения различных методов шифрования и хэширования паролей, а также знание этических аспектов веб-безопасности.*	XSS, SQL-инъекции, и другие атаки: как ИИ помогает в защите	Рассмотрение причин возникновения данных уязвимостей и методов их обнаружения в тестируемых приложениях. Ознакомление с лучшими практиками, техническими средствами и методологиями, направленными на устранение или минимизацию рисков, связанных с указанными типами уязвимостей в веб-приложениях.		
		Выявление и исследование уязвимостей на виртуальной машине bWAPP, изучение методов их эксплуатации и принципов защиты от различных типов атак. Разработка собственного веб-приложения на языке Python, уязвимого к XSS-атаке, с использованием искусственного интеллекта для поддержки в написании кода.	практические занятия	5
		Проведение практического анализа безопасности публично доступных веб-приложений в Интернете для закрепления знаний по таким уязвимостям, как XSS и SQL-инъекции, с использованием искусственного интеллекта. В качестве целей рассматриваются специально подготовленные платформы для обучения: (https://xss-game.appspot.com, http://sudo.co.il/xss/, https://sql.training.hackerdom.ru/). Цель — применить полученные знания и автоматизировать исследование уязвимостей с помощью ИИ	текущий контроль	1
	<u>Тема 3.3.</u> Шифрование и безопасное хранение данных с применением ИИ	Рассматриваются принципы создания паролей с использованием симметричного и асимметричного шифрования, современные методы хеширования для их защиты, а также рекомендации по формированию надежных паролей, включая применение длинных и сложных комбинаций символов; изучаются техники безопасного хранения данных, направленные на предотвращение несанкционированного доступа и	теоретические занятия	2

Типы задач/деятельности: *Разработка простых веб-страниц с использованием HTML и CSS, задачи на выявление и анализ уязвимостей (SQL-инъекции, XSS, CSRF) с применением виртуальной машины bWAPP, создание уязвимых веб-приложений на Python для исследования методов атак, реализация алгоритмов хэширования паролей и шифрования данных, задачи на сравнение безопасности передачи данных через HTTP и HTTPS, а также разработка рекомендаций по обеспечению этических стандартов и защиты конфиденциальности в веб-приложениях*		утечек, и описываются механизмы обеспечения безопасности при передаче данных через протокол HTTPS и использование SSL/TLS-сертификатов.		
		Рассматривается применение различных алгоритмов хэширования паролей, включая пример реализации такого алгоритма в Python с помощью искусственного интеллекта, а также изучаются методы шифрования данных и приводится пример использования протокола HTTPS в Python для обеспечения безопасной передачи информации.	практические занятия	5
		Анализ способов защиты данных в веб-приложениях с использованием HTTPS и без него, а также разработка ИИ-рекомендаций для улучшения их безопасности.	самостоятельная работа текущий контроль	1 1
	Тема 3.4. Этические аспекты веб-безопасности с использованием ИИ	Этические принципы веб-разработки, включая соблюдение законодательства и этических норм, обеспечение защиты конфиденциальности данных и ответственное использование информации.	теоретические занятия	2
		Разработка стандарта для существующего веб-приложения с учетом этических аспектов и конфиденциальности данных, анализ соблюдения требований стандарта и выявление необходимых доработок для полного соответствия. Применение ИИ для проведения аудита безопасности сайта.	практические занятия	6
		Анализ веб-сайтов учебных заведений на соответствие этическим принципам и разработка рекомендаций по их улучшению с использованием ИИ.	самостоятельная работа текущий контроль	1 1
	Промежуточная аттестация по 3 модулю	Тестирование		1
Модуль 4.	Тема 4.1.	Пентестинг и его фазы. атаки на периметр, приложения, социальная инженерия, физические атаки.	теоретические занятия	2

Практический пентестинг с Python и ИИ Описание модуля: *Модуль посвящен основам пентестинга, включая изучение популярных инструментов (Nmap, Burp Suite, Hydra, Wireshark, sqlmap), скриптинга на Python, сканирования уязвимостей и эксплуатации хостов. Практические навыки включают настройку рабочей среды на базе DVWA, установку Kali Linux, разработку автоматизированных скриптов с помощью ИИ и объединение инструментов в единый рабочий процесс с использованием специализированных библиотек* Цель модуля: *Формирование практических навыков проведения тестирования на проникновение с использованием языка Python, специализированных инструментов и технологий искусственного интеллекта.* Планируемые результаты: *Формирование комплексных компетенций в области практического пентестинга: теоретическое понимание фаз и типов атак, навыки работы с инструментами в среде Kali Linux, умение настраивать рабочую*	Основы пентестинга: ручное и автоматизированное с ИИ	Подготовка рабочей среды на базе виртуальной машины DVWA, сбор данных о целевой системе и выявление уязвимостей для их последующей эксплуатации.	практические занятия	5
		Дополнительное исследование виртуальной машины DVWA, сбор данных об используемых сервисах и проведение ручного тестирования на проникновение в данной среде с применением ИИ.	текущий контроль	1
	Тема 4.2. Инструменты для пентеста, включая ИИ	Обзор популярных инструментов для тестирования на проникновение, их возможностей и применения, включая инструменты операционной системы Kali Linux: Nmap, Burp Suite, Hydra, Wireshark, dirb, sqlmap и Metasploit Framework.	теоретические занятия	2
		Работа со специализированными инструментами для тестирования на проникновение, включая установку Kali Linux на виртуальную машину и детальное изучение инструментов Nmap, Burp Suite, Hydra, Wireshark и sqlmap с их применением на уязвимой виртуальной машине DVWA, при этом ИИ используется как помощник для работы с этими инструментами.	практические занятия	5
		Поиск и эксплуатация уязвимостей на виртуальной машине DVWA с использованием ИИ для анализа и тестирования.	текущий контроль	1
	Тема 4.3. Автоматизация пентестинга на Python с использованием ИИ	Автоматизация пентестинга через скриптинг на Python, включая сканирование уязвимостей и эксплуатацию хостов, с объединением инструментов в единый скрипт с использованием библиотек, таких как Scapy для работы с сетевыми пакетами или Requests для HTTP-запросов.	теоретические занятия	2
		Разработка Python-скриптов с использованием ИИ для автоматизации тестирования на проникновение, включая сканирование и эксплуатацию уязвимых хостов, а также объединение инструментов в единый рабочий скрипт.	практические занятия	5

среду на базе DVWA, автоматизировать задачи пентестинга через скриптинг на Python с использованием библиотек (Scapy, Requests), создавать комплексные решения для тестирования безопасности путем объединения различных инструментов, анализировать результаты тестирования, составлять детальные отчеты и формулировать рекомендации по устранению уязвимостей с применением технологий искусственного интеллекта для оптимизации процессов сбора данных, анализа уязвимостей и генерации отчетов Типы задач/деятельности: *Выполнение практических задач по настройке рабочей среды на базе DVWA, сканированию уязвимостей с использованием инструментов Kali Linux, разработке автоматизированных скриптов на Python для тестирования на проникновение, анализу результатов и составлению отчетов с применением технологий искусственного интеллекта для оптимизации процессов сбора данных, выявления уязвимостей и формулирования рекомендаций по их устранению.*		Разработка собственных скриптов с использованием ИИ для автоматизации задач пентестинга, включая перебор директорий и сбор активных страниц сайта.	самостоятельная работа текущий контроль	1 1
	Тема 4.4. Анализ результатов и генерация отчетов с помощью ИИ	Составление отчетов о тестировании на проникновение, включая структуру и содержание документа, предоставленного преподавателем, а также процесс формулирования рекомендаций по устранению выявленных уязвимостей на основе результатов анализа.	теоретические занятия	2
		Создание отчета по трем выбранным уязвимостям в виртуальной машине DVWA, включая описание проведенных тестов на проникновение и формулирование рекомендаций с помощью ИИ.	практические занятия	6
		Разработка отчета с использованием ИИ о тестировании на проникновение гипотетической компании, включая анализ трех выбранных уязвимостей и предоставление рекомендаций по их устранению.	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: первые шаги с Python и ИИ»	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
24.	Модуль 1. Основы Python для кибербезопасности и искусственный интеллект.	Тема 1.1. Введение в Python: синтаксис, среды разработки	7	2 2 2 2	23.09.2025 26.09.2025 30.09.2025 03.10.2025
25.		Тема 1.2. Типы данных в Python и их применение	7	2 2 2 2	07.10.2025 10.10.2025 14.10.2025 17.10.2025
26.		Тема 1.3. Модули и функции языка Python	7	2 2 2 3	21.10.2025 24.10.2025 28.10.2025 31.10.2025
27.		Тема 1.4. Файлы и исключения в Python, использование ИИ при разработке программ на Python	8	2 2 2 2 2	07.11.2025 11.11.2025 14.11.2025 18.11.2025 21.11.2025
28.		Промежуточная аттестация по 1 модулю			25.11.2025
29.	Модуль 2. Основы информационной безопасности с элементами ИИ и работа с компьютерными сетями	Тема 2.1. Ключевые концепции кибербезопасности	7	2 2 2 2	02.12.2025 05.12.2025 09.12.2025 12.12.2025
30.		Тема 2.2. Угрозы безопасности и инструменты для их обнаружения	7	2 2 2	16.12.2025 19.12.2025 23.12.2025

				2	26.12.2025
31.		Тема 2.3. Этичный хакинг: методы тестирования с помощью ИИ	7	2 2 2 3	30.12.2025 13.01.2026 16.01.2026 20.01.2026
32.		Тема 2.4. Защита от атак с использованием ИИ	8	2 2 2 2 2	21.01.2026 23.01.2026 27.01.2026 28.01.2026 29.01.2026
33.		Промежуточная аттестация по 2 модулю			30.01.2026
34.	Модуль 3. Веб-безопасность и ИИ: обнаружение уязвимостей	Тема 3.1. Основы веб-разработки с применением ИИ	7	2 2 2 2	03.02.2026 06.02.2026 10.02.2026 13.02.2026
35.		Тема 3.2. XSS, SQL-инъекции, и другие атаки: как ИИ помогает в защите	7	2 2 2 2	17.02.2026 20.02.2026 24.02.2026 27.02.2026
36.		Тема 3.3. Шифрование и безопасное хранение данных с применением ИИ	7	2 2 2 3	03.03.2026 06.03.2026 10.03.2026 13.03.2026
37.		Тема 3.4. Этические аспекты веб-безопасности с использованием ИИ	8	2 2 2 2 2	17.03.2026 20.03.2026 24.03.2026 25.03.2026 26.03.2026
38.		Промежуточная аттестация по 3 модулю			27.03.2026
39.	Модуль 4.	Тема 4.1.	7	2	30.03.2026

	Практический пентестинг с Python и ИИ	Основы пентестинга: ручное и автоматизированное с ИИ		2 2 2	31.03.2026 03.04.2026 07.04.2026
40.		Тема 4.2. Инструменты для пентеста, включая ИИ	7	2 2 2 2	10.04.2026 14.04.2026 17.04.2026 21.04.2026
41.		Тема 4.3. Автоматизация пентестинга на Python с использованием ИИ	7	2 2 2 3	24.04.2026 28.04.2026 05.05.2026 08.05.2026
42.		Тема 4.4. Анализ результатов и генерация отчетов с помощью ИИ	8	2 2 2 2 2	15.05.2026 15.05.2026 19.05.2026 20.05.2026 21.05.2026
43.		Промежуточная аттестация по 4 модулю			22.05.2026
44.	Итоговый контроль/аттестация по ДОП			4	26.05.2026
45.	Итого по ДОП:			148	
46.	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	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	- технологий «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	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	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	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.	Black Hat Python: программирование для хакеров и пентестеров. 2-е изд. — СПб.:Питер, 2022.	Python. Разработка на основе тестирования. / пер. с англ. Логунов А. В. – М.: ДМК Пресс,	Искусство тестирования на проникновение в сеть / пер. с анг. В. С. Яценкова. – М.: ДМК

	Программируем на Python, Майкл Доусон, 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.	— 256 с.: ил. — (Серия «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»).	2018. – 622 с.: ил. 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»).	Пресс, 2021. – 310 с.: ил. 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)	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)	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)	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)
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: 05.07.2025) - 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: 05.07.2025) - 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: 05.07.2025) - 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: 05.07.2025) - 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: 05.07.2025) - Текст: электронный. Сбер — крупнейший банк в России. Сбертех, АО Официальный сайт - URL: https://sbertech.ru/ Санкт-Петербург, (дата обращения: 05.07.2025) - 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: 05.07.2025) - 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: 05.07.2025) - 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: 05.07.2025) - Текст: электронный.	кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/articles/276477/ (дата обращения: 05.07.2025) - Текст: электронный.

	05.07.2025) - Текст: электронный.	Москва. - URL: https://habr.com/ru/companies/selectel/articles/197814/ (дата обращения: 05.07.2025) - 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: 05.07.2025) - 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: 05.07.2025) - Текст:		

		электронный.		
Электронные образовательные ресурсы	Сайт pythonchik.ru — обучение основам Python - Москва. - URL: https://pythonchik.ru/osnovy/ (дата обращения: 05.07.2025) - Текст: электронный. Простым языком об HTTP. Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/post/215117/(дата обращения: 05.07.2025) - 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: 05.07.2025) - Текст: электронный. Практическое задание в Cisco Packet Tracer. http://ncti.ru/files/studentu/Olimpiada/zadanie_II_.pdf (дата обращения: 05.07.2025) - Текст: электронный. Easy-Network - обучающий курс по сетевым технологиям. Лабораторные работы по Cisco CCNA. URL: https://easy-network.ru/zadaniya.html (дата обращения: 05.07.2025) - Текст: электронный. Форум информационной	PortSwigger: официальный сайт. - URL: https://portswigger.net/web-security (дата обращения: 05.07.2025) - Текст: электронный. TryHackMe - тренинг по кибербезопасности: официальный сайт. - Лондон. - URL: https://tryhackme.com/(дата обращения: 05.07.2025) - Текст: электронный. HACKTHEBOX URL: https://www.hackthebox.com/ (дата обращения: 05.07.2025) - Текст: электронный.	TryHackMe - тренинг по кибербезопасности: официальный сайт. - Лондон. - URL: https://tryhackme.com/(дата обращения: 05.07.2025) - Текст: электронный. Блог “NetSkills” URL: http://blog.netskills.ru/ (дата обращения: 05.07.2025) - Текст: электронный.

		безопасности - CODEBY.NET._URL: https://codeby.net/threads/cisco-ccna-1-2019-zadanija-v-cisco-packet-tracer.69507/ (дата обращения: 05.07.2025) - Текст: электронный.		