РУКОН ЦЕЛЬ
МНОГОПРОФИЛЬНЫЙ ЦЕНТР КВАЛИФИКАЦИЙ

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«МНОГОПРОФИЛЬНЫЙ ЦЕНТР КВАЛИФИКАЦИЙ «ЦЕЛЬ»
(АНО ДПО «МЦК «Цель»)

Санкт-Петербург

ПРИКАЗ

7 июля 2025 года № 18 п/2025-ОП

Об утверждении Комплекта дополнительных общеобразовательных общеразвивающих программ «Этичный хакинг на Python с ИИ»

На основании Федерального закона от 29 декабря 2012 года №273-ФЗ «Об образовании в Российской Федерации», Приказа Министерства просвещения Российской Федерации от 27 июля 2022 года №629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам», Протокола заседания педагогического совета от 4 июля 2025 г. № 1,

ПРИКАЗЫВАЮ:

1. Утвердить Комплект дополнительных общеобразовательных общеразвивающих программ «Этичный хакинг на Python с ИИ», включающий:

1.1. Дополнительную общеобразовательную общеразвивающую программу «Этичный хакинг: первые шаги с Python и ИИ» (начальный уровень);

1.2. Дополнительную общеобразовательную общеразвивающую программу «Этичный хакинг: инструменты защиты на Python и ИИ» (базовый уровень);

1.3. Дополнительную общеобразовательную общеразвивающую программу «Этичный хакинг: миг уникальности» (продвинутый уровень).

2. Контроль исполнения настоящего приказа оставляю за собой.

Директор О.В. Самоварова

Общие данные о Комплекте ДОП
Этичный хакинг на Python с ИИ

1. Сведения об организации

№ п/п	Наименование поля	Значение поля
1.1	**Наименование образовательной организации**	РУКОН Цель
1.2	**Логотип образовательной организации**	РУКОН ЦЕЛЬ МНОГОПРОФИЛЬНЫЙ ЦЕНТР КВАЛИФИКАЦИЙ
1.3	**ИНН**	7728470220
1.4	**Ответственный за реализацию Комплекта ДОП, ФИО**	Рыбалёва Ирина Александровна
1.5	**Ответственный за реализацию Комплекта ДОП, должность**	Руководитель образовательного процесса
1.6	**Ответственный за реализацию Комплекта ДОП, телефон**	+79623450600
1.7	**Ответственный за реализацию Комплекта ДОП, электронная почта**	centre@mckcel.ru

2. Комплекс основных характеристик Комплекта ДОП

Основные данные

№ п/п	Наименование поля	Значение поля
1.	**Направление**	Современные языки программирования
2.	**Название Комплекта ДОП**	Этичный хакинг на Python с ИИ
3.	**Название каждой ДОП Комплекта ДОП**	Этичный хакинг: первые шаги с Python и ИИ Этичный хакинг: инструменты защиты на Python и ИИ Этичный хакинг: миг уникальности
4.	**Вид входящих в Комплект ДОП программ дополнительного образования детей и взрослых**	Дополнительная общеобразовательная программа
5.	**Ссылка на страницу обучения на Курсе**	https://www.odin.study/ru/Division/Info/1313
6.	**Форма обучения**	Очная форма обучения
7.	**Формат обучения по ДОП Комплекта ДОП**	Онлайн

8.	**Целевая аудитория/ категория обучающихся (для которого будет актуальным обучение по ДОП данного Комплекта ДОП)**	Школьники 8 - 11 классов Обучающиеся по программам среднего профессионального образования по профессиям и (или) специальностям, включенным в Перечень профессий и специальностей среднего профессионального образования в области информационных технологий, предусмотренный приложением к Концепции
9.	**Язык программирования**	Python
10.	**Формируемые базовые навыки в области информационных технологий и искусственного интеллекта**	
11.	**Направление робототехники**	

Аннотация

№ п/п	Наименование поля	Значение поля
1.	Аннотация Комплекта ДОП	Комплект ДОП «Этичный хакинг на Python с ИИ» включает в себя три дополнительные общеобразовательные общеразвивающие программы разного уровня сложности (начальный, базовый и продвинутый уровни) (далее – Программы): «Этичный хакинг: первые шаги с Python и ИИ» (начальный уровень); «Этичный хакинг: инструменты защиты на Python и ИИ» (базовый уровень) и «Этичный хакинг: миг уникальности» (продвинутый уровень). Все Программы Комплекта относятся к технической направленности. Формат обучения по Программам Комплекта ДОП: онлайн с применением дистанционных образовательных технологий и электронного обучения на образовательной платформе «Odin». Категория обучающихся по Программам Комплекта 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. Трудоемкость каждой Программы Комплекта ДОП: 148 ак.ч. Структура Комплекта ДОП. Каждая Программа состоит из 4 модулей, каждый модуль (по 36 ак.ч.) включает в себя 4 темы с различными типами занятий (теоретическое занятие (лекция), практическое занятие и самостоятельная работа). По каждой теме имеются задания (тестовая форма) для текущего контроля и самоконтроля. По итогам прохождения каждого модуля проводится промежуточная аттестация (тестовая форма контроля). Итоговый контроль по Программе: представление проекта. 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. Новизна Комплекта 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. Интеграционные возможности Комплекта ДОП и актуальность его содержания Все программы Комплекта не только развивают IT-навыки, но и укрепляют междисциплинарные связи, помогая учащимся применять знания из других предметов на практике. Педагоги-наставники по всем Программам Комплекта дают не только базовые знания, но и готовят учащихся

к участию в престижных IT-соревнованиях и олимпиадах:
Всероссийская олимпиада школьников (ВсОШ) по информатике;
Олимпиада «Кибербезопасность» от НТИ (Национальной технологической инициативы);
CTF-соревнования;
Хакатоны и проектные конкурсы: WorldSkills Russia (компетенция «Кибербезопасность»); Конкурс «Большие вызовы» (Сириус) и др.
Все программы Комплекта разработаны с учетом актуальных запросов IT-индустрии и направлены на формирование навыков, востребованных в профессиональной сфере. Содержание курса ориентировано на раннюю профориентацию учащихся 8-11 классов для ключевых IT-ролей: Junior Security Analyst; пентестер (Ethical Hacker); специалист по SOC (Security Operations Center), а также разработчик скриптов автоматизации безопасности. Наши выпускники смогут самостоятельно писать Python-скрипты, проводить аудит безопасности веб-приложений, работать с инструментами Kali Linux (Metasploit, Burp Suite), понимать принципы работы ИИ в кибербезопасности и др.
Для усиления связи с рынком труда программа предусматривает: приглашение экспертов из IT-компаний на мастер-классы, реальные кейсы от партнеров (например, анализ уязвимостей тестового сайта) и т.д.
Комплект ДОП предлагает различные образовательные мероприятия, обеспечивающие возможность индивидуализации обучения и развития. Все форматы являются гибкими и адаптируются под интересы и уровень учащихся: уровни Программ по сложности содержания обучения, так и возможности выбора задания в рамках одной Программы (практические занятия и самостоятельная работа), также для любознательных на занятиях предполагаются персонализированные задания со звездочкой; индивидуальные и групповые проекты; менторская поддержка каждого участника Программы в чатах мессенджеров и в чате Образовательной платформы «Odin»; участие по желанию учащихся в соревновательных форматах (внутренние CTF-турниры (например, «Защити сервер школы»); Хакатоны с партнерами (разработка прототипов защитных систем). Также предусмотрены в рамках реализации каждой Программы Комплекта индивидуальные консультации (разбор сложных тем 1-on-1 с преподавателем). На образовательной платформе также предусмотрен электронный журнал с отслеживанием прогресса каждого учащегося в выбранных активностях. Все мероприятия добровольные и не перегружают основной курс по Программам Комплекта.
Для обеспечения преемственности и взаимодействия между участниками Программ Комплекта реализованы следующие форматы взаимодействия. 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 QA-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. Предусмотрена система мотивации наставничества и взаимодействия: бейджи за менторство («Золотой наставник»), баллы, которые каждый учащийся может обменять в Магазине знаний провайдера на гаджеты и пр.
Содержание Комплекта ДОП «Этичный хакинг на Python с ИИ» предполагает системную интеграцию с технологиями искусственного интеллекта во всех уровнях Программ, так как реализует сквозное внедрение основ искусственного интеллекта как в теоретических, так и в практических занятиях.
В Комплект ДОП включены элементы робототехники, обеспечивающие изучение кибербезопасности IoT/роботизированных систем, разработку защитных механизмов для физических устройств, применение Python для программирования роботов. Комбинация робототехники и этичного хакинга делает уникальным данный Комплекс ДОП.
Все три уровня Программ Комплекта ДОП предполагают сквозное изучение кибербезопасности. В сравнении с традиционными Программами наш Комплект содержит до 95% тем по кибербезопасности (от основ до проф. инструментов (Wireshark, Burp Suite), где 56% отведено формированию и совершенствованию компетенций по кибербезопасности, причем со связью с ИИ (AI-анализ угроз на Python), с актуальным разбором свежих утечек данных (2022-2024).

На продвинутом уровне учащиеся исследуют реальный кейс утечки данных через SQL-инъекцию (с разрешения владельца тестового сайта). Кибербезопасность в Комплекте ДОП связана с ИИ; робототехникой: защита IoT-устройств от взлома и Python: автоматизация пентест-инструментов.
Безусловной задачей Комплекта «Этичный хакинг на Python с ИИ» является освоение типовых библиотек и фреймворков, что закреплено в учебных планах Программ всех уровней, конкретные библиотеки и фреймворки прописаны в методических материалах Программ, в конспектах практических занятий, а также в конспектах самостоятельных работ в качестве самоконтроля и контроля за полученными знаниями и сформированными умениями. Более 80% учебного времени отведено работе с реальными инструментами; все выпускные проекты требуют применения указанных технологий: начальный уровень: requests, socket (базовые сетевые инструменты); базовый: Scapy, BeautifulSoup (анализ трафика/данных); продвинутый: SQLAlchemy, Django (ИИ и веб-безопасность).
В Комплекте ДОП частично используется VR/AR технологии через оборудование и ПО: VR-гарнитуры (Oculus/Meta Quest), AR-приложения (Unity+Vuforia) и собственные VR-тренажеры для кибербезопасности для имитации хакерских атак в виртуальных сетях, 3D-визуализация работы нейросетей и в качестве AR-подсказки при решении CTF-задач.
На начальном уровне осваиваются ознакомительные VR-туры по сетевой инфраструктуре; на базовом: AR-тренажеры для работы с терминалом, а на продвинутом - VR-симуляторы SOC-центра.
Безусловно, через содержание Программ в Комплекте ДОП раскрыты различные перспективные технологические направления:
квантовые вычисления и криптография: изучение основ квантовой криптографии; практикумы на симуляторах и разбор уязвимостей современных шифров к квантовым атакам;
блокчейн и смарт-контракты: анализ безопасности блокчейн-сетей;
биотехнологии и кибербезопасность: защита биометрических данных;
гибридный интеллект: симбиоз ИИ и человеческого мышления и когнитивная безопасность (защита от манипуляций).
Содержание Программ Комплекта ДОП, работа с педагогами – наставниками, наставничество /менторство внутри групп учащихся из разного уровня Программ в рамках Комплекта ДОП, 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.
Таким образом, все Программы Комплекта ДОП не просто учат Python и хакингу с ИИ, а воспитывают специалистов будущего — гибких, коммуникабельных и этичных.
Комплект ДОП «Этичный хакинг на Python с ИИ» системно формирует ответственное отношение к инновациям через практико-ориентированные кейсы (легальный пентест, анализ цифровых следов), интеграцию этических принципов в технические задания (чек-листы, ethical coding), взаимодействие с юристами и HR для отработки реальных сценариев. С целью ответственного отношения к инновациям в программе будут реализованы такие образовательные мероприятия, как кейс-стади с разбором реальных инцидентов (утечки данных, DDoS-атаки), дебаты: «Можно ли взломать систему, чтобы доказать её уязвимость?», ролевые игры: «Суд над хакером» с участием юристов и др.
Программы Комплекта ДОП целенаправленно развивают навыки, необходимые для активного участия в профессиональных IT-сообществах. Так, техническая экспертиза - углубленное изучение Python и инструментов кибербезопасности позволяет учащимся вносить содержательный вклад в open-source проекты и профессиональные дискуссии. Практика коллаборации – работа в командах над проектами, участие в хакатонах и CTF-соревнованиях формирует навыки Git-взаимодействия и распределенной разработки. Культура ответственного раскрытия – обучение этичным принципам работы с уязвимостями готовит к участию в bug bounty программах и сотрудничеству с CERT-сообществами. Публичная активность - защита проектов, ведение технических блогов и выступления на конференциях развивают навыки презентации идей. Сетевые компетенции - использование профессиональных платформ (GitHub, HackTheBox, CTFtime) с первых занятий интегрирует учащихся в мировое IT-сообщество.
Особенности Программ

		каждого уровня Программа ««Этичный хакинг: первые шаги с Python и ИИ» (начальный уровень) 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. Программа ««Этичный хакинг: первые шаги с Python и ИИ» (начальный уровень) формирует базовые компетенции 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. Программа «Этичный хакинг: инструменты защиты на Python и ИИ» (базовый уровень) Входные требования к Получателям поддержки: начальный уровень владения одним из современных языков программирования и знание основ ООП; Получатель поддержки должен уметь использовать стандартные структуры данных и библиотеки, иметь начальные представление об объектно-ориентированном подходе, иметь опыт решения прикладных задач. Программа «Этичный хакинг: инструменты защиты на Python и ИИ» (базовый уровень) ориентирована на специализированное изучение выбранного языка программирования, освоение типовых библиотек и фреймворков, решение классических задач по программированию и использования профессиональных инструментов. Программа «Этичный хакинг: миг уникальности» (продвинутый уровень) Входные требования к Получателям поддержки: знания в области программирования и математики; уверенное владение базовыми навыками в технологиях искусственного интеллекта, знание основных методов машинного обучения и нейронных сетей, умение применять их для решения типовых задач, иметь опыт работы с данными и использования библиотек искусственного интеллекта. Программа «Этичный хакинг: миг уникальности» (продвинутый уровень) ориентирована на углубленное изучение продвинутых методов и моделей искусственного интеллекта, освоение специализированных областей (например, компьютерное зрение, обработка естественного языка), формирование навыков решения комплексных задач с использованием актуальных инструментов и фреймворков.

Основные данные ДОП: УРОВЕНЬ НАЧАЛЬНЫЙ

№ п/п	Наименование поля	Значение поля
1.	Название ДОП	Этичный хакинг: первые шаги с Python и ИИ
2.	Уровень сложности ДОП	НАЧАЛЬНЫЙ
3.	Объем/общая трудоемкость ДОП (общий объем освоения ДОП в академических часах)	148.00
4.	Объем каждого модуля в ак.ч.	Модуль1 - 36 Модуль2 - 36 Модуль3 - 36 Модуль4 - 36
5.	Общее количество образовательных мероприятий	16
6.	Объем недельной нагрузки обучающегося	4.00
7.	Дата начала и дата окончания обучения по ДОП (срок освоения ДОП)	С 2025-09-22 по 2026-05-29
9.	Выдаваемый по окончании обучения документ	Сертификат

Описание ДОП

№ п/п	Наименование поля	Значение поля

1.	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 оффлайне (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.

2.	Цель и задачи ДОП	Цель ДОП: формирование у Получателей поддержки 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 ДОП: 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.

3.	Планируемые результаты	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
4.	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.

5.	Дополнительно (в соответствующих отдельных графах) может быть дана следующая информация по ДОП:	
5.1.	Стоимость обучения по ДОП	37304.00

5.2.	Рекомендации по обучению на ДОП	РЕКОМЕНДАЦИИ ДЛЯ УЧАЩИХСЯ 1. Требования к техническому оснащению: • Компьютер или ноутбук с доступом в Интернет • Установленные программы: o Python o IDE: PyCharm или Visual Studio Code • Виртуальные машины (Kali Linux, bWAPP, DVWA) • Браузер • Средства связи (MAX, Telegram и/или электронная почта) 2. Навыки, необходимые для успешного обучения: • Уверенное владение базовыми компьютерными навыками • Умение работать с браузером и файлами • Навыки самостоятельного поиска и анализа информации • Готовность к самоподготовке и командной работе • Способность презентовать собственные решения 3. Поведенческие рекомендации: • Занимайтесь регулярно: не менее 2–3 раз в неделю • Ведите дневник проекта (изученное, успехи, трудности) • Не стесняйтесь обращаться к преподавателю за разъяснениями • Ищите аналогии — это поможет лучше понять материал • Работайте в профессиональной среде разработки, используйте официальную документацию • Помните: ошибки — не провал, а путь к обучению 4. Правила: • Не пропускайте занятия: темы логически связаны • Не копируйте чужой код — важно понимание • Соблюдайте этику — курс обучает защите, а не атаке • Работайте с виртуальными машинами только в учебной среде РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ 1. Использование учебно-методического комплекса (УМК): Для реализации программы необходимо использовать утверждённый УМК, включающий: • Рабочую программу и календарно-тематическое планирование • Презентации, практические задания, тесты и кейсы по модулям • Задания для самостоятельной работы и проектов • Документационные шаблоны: чек-листы, формы отчётов, критерии оценки Преподаватель обязан строго соблюдать структуру курса и утверждённые контрольные точки. 2. Этическое сопровождение обучения: Преподавателю необходимо: • Формировать у обучающихся понимание границ этичного хакинга • Акцентировать внимание на правовой ответственности в цифровой среде • Развивать навыки цифровой гигиены и киберэтики: o Защита персональных данных o Уважительное взаимодействие в сети • Контролировать соблюдение этики в онлайн и офлайн-коммуникации 3. Требования к техническому оснащению: Для проведения занятий в очной форме с применением дистанционных образовательных технологий, в том числе с применением средств электронного обучения требуется: • Компьютер с предустановленным необходимым ПО • Стабильный доступ к ВКС • Рабочие аккаунты в LMS, мессенджерах, электронной почте • Высокоскоростной Интернет, обеспечивающий: o Загрузку

		и работу с виртуальными машинами o Проведение видеозанятий без потерь связи o Доступ к облачным сервисам и библиотекам ИИ

3. Комплекс организационно-педагогических условий реализации ДОП:
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	Введение в Python: синтаксис, среды разработки	8	2	5	0	1	0
2.		Типы данных в Python и их применение	8	2	5	0	1	0
3.		Модули и функции языка Python	9	2	5	1	1	0
4.		Файлы и исключения в Python, использование ИИ при разработке программ на Python	10	2	6	1	1	0
5.		Промежуточная аттестация	1	0	0	0	1	0
6.	Модуль 2 Основы информационной безопасности с элементами ИИ и работа с компьютерными сетями	Ключевые концепции кибербезопасности	8	2	5	0	1	0
7.		Угрозы безопасности и инструменты для их обнаружения	8	2	5	0	1	0
8.		Этичный хакинг: методы тестирования с помощью ИИ	9	2	5	1	1	0
9.		Защита от атак с использованием ИИ	10	2	6	1	1	0
10.		Промежуточная аттестация	1	0	0	0	1	0
11.	Модуль 3 Веб-безопасность и ИИ: обнаружение уязвимостей	Основы веб-разработки с применением ИИ	8	2	5	0	1	0
12.		XSS, SQL-инъекции, и другие атаки: как ИИ помогает в защите	8	2	5	0	1	0
13.		Шифрование и безопасное хранение данных с применением ИИ	9	2	5	1	1	0

14.		Этические аспекты веб-безопасности с использованием ИИ	10	2	6	1	1	0
15.		Промежуточная аттестация	1	0	0	0	1	0
16.	Модуль 4 Практический пентестинг с Python и ИИ	Основы пентестинга: ручное и автоматизированное тестирование с ИИ	8	2	5	0	1	0
17.		Инструменты для пентеста, включая ИИ	8	2	5	0	1	0
18.		Автоматизация пентестинга на Python с использованием ИИ	9	2	5	1	1	0
19.		Анализ результатов и генерация отчетов с помощью ИИ	10	2	6	1	1	0
20.		Промежуточная аттестация	1	0	0	0	1	0
Итоговый контроль/аттестация по ДОП			4.00	0	0	0	4.00	0
Итого по ДОП:			148	32	84	8	24	0
ИТиСИ			Часы ИТиСИ не входят в общую трудоемкость ДОП, но участие в ИТиСИ обязательно для всех успешно прошедших итоговый контроль/аттестацию по ДОП					

Рабочая программа с описанием каждого модуля ДОП

Элементы ДОП (модули и итоговый контроль/аттестация по 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 Модуль направлен на изучение основ языка Python, его ключевых особенностей и преимуществ. В рамках курса вы познакомитесь с выбором 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	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 переменными и использованием арифметических операций.	Теоретическая подготовка	2
		Создание программ для выполнения базовых математических операций: сложение, вычитание, умножение и деление чисел.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Введение в Python: синтаксис, среды разработки"	Текущий контроль	1

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, 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.	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.	Теоретическая подготовка	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
			Самостоятельная работа	0
		Текущий контроль по теме "Типы данных в Python и их применение"	Текущий контроль	1
	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	Теоретическая подготовка	2
		Разработка и применение пользовательских функций в Python, подключение модулей и использование встроенных стандартных функций языка. Создание программы-генератора паролей.	Практические занятия	5
		Доработка ранее написанных программ с использованием функций и модулей.	Самостоятельная работа	1
		Текущий контроль по теме "Модули и функции языка Python"	Текущий контроль	1
	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.	Теоретическая подготовка	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	1
		Текущий контроль по теме "Файлы и исключения в Python, использование ИИ при разработке программ на Python"	Текущий контроль	1

	Промежуточная аттестация	Тестирование 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.	Промежуточная аттестация	1
Модуль 2 Основы информационной безопасности с элементами ИИ и работа с компьютерными сетями 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 и	Ключевые концепции кибербезопасности	Введение в основные понятия информационной безопасности: конфиденциальность, целостность и доступность информации. Рассмотрение понятия угроз, их классификация и влияние на безопасность данных. Основные виды угроз — вирусы, хакерские атаки, методы социальной инженерии. Понятие уязвимостей и их роль в обеспечении информационной безопасности.	Теоретическая подготовка	2
		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
			Самостоятельная работа	0
		Текущий контроль по теме "Ключевые концепции кибербезопасности"	Текущий контроль	1
	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.	Теоретическая подготовка	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
			Самостоятельная работа	0
		Текущий контроль по теме "Угрозы безопасности и инструменты для их обнаружения"	Текущий контроль	1
	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.	Теоретическая подготовка	2

анализировать различные типы угроз и уязвимостей, практические навыки определения IP-адресов и подсетей с помощью Python, обнаружения активных портов, проведения этичного те-стирования 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. Типы задач/деятельности: 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.		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	1
		Текущий контроль по теме "Этичный хакинг: методы тестирования с помощью ИИ"	Текущий контроль	1
	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.	Теоретическая подготовка	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	1
		Текущий контроль по теме "Защита от атак с использованием ИИ"	Текущий контроль	1
	Промежуточная аттестация	Тестирование 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.	Промежуточная аттестация	1
Модуль 3 Веб-безопасность и ИИ: обнаружение уязвимостей В рамках данного модуля основное внимание уделяется	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.	Теоретическая подготовка	2

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. 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. Цель модуля: Формирование знаний и практических навыков в области обеспечения безопасности веб-приложений с использованием технологий искусственного интеллекта. Планируемые результаты: 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		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
			Самостоятельная работа	0
		Текущий контроль по теме "Основы веб-разработки с применением ИИ"	Текущий контроль	1
	XSS, SQL-инъекции, и другие атаки: как ИИ помогает в защите	Изучение распространённых уязвимостей веб-приложений, таких как SQL-инъекции, XSS- и CSRF-атаки. 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.	Теоретическая подготовка	2
		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
			Самостоятельная работа	0
		Текущий контроль по теме "XSS, SQL-инъекции, и другие атаки: как ИИ помогает в защите"	Текущий контроль	1
	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 утечек, и описываются механизмы обеспечения безопасности при передаче данных через протокол HTTPS и использование SSL/TLS-сертификатов.	Теоретическая подготовка	2
		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	1

уязвимых приложений на Python, применения различных методов шифрования и хэширования паролей, а также знание этических аспектов веб-безопасности. 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.		Текущий контроль по теме "Шифрование и безопасное хранение данных с применением ИИ"	Текущий контроль	1
	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.	Теоретическая подготовка	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	1
		Текущий контроль по теме "Этические аспекты веб-безопасности с использованием ИИ"	Текущий контроль	1
	Промежуточная аттестация	Тестирование 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.	Промежуточная аттестация	1
Модуль 4 Практический пентестинг с Python и ИИ 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	Основы пентестинга: ручное и автоматизированное тестирование с ИИ	Пентестинг и его фазы. атаки на периметр, приложения, социальная инженерия, физические атаки.	Теоретическая подготовка	2
		Подготовка рабочей среды на базе виртуальной машины DVWA, сбор данных о целевой системе и выявление уязвимостей для их последующей эксплуатации.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Основы пентестинга: ручное и автоматизированное тестирование с ИИ"	Текущий контроль	1
	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.	Теоретическая подготовка	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

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 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.		Поиск и эксплуатация уязвимостей на виртуальной машине DVWA с использованием ИИ для анализа и тестирования.	Самостоятельная работа	0
		Текущий контроль по теме "Инструменты для пентеста, включая ИИ"	Текущий контроль	1
	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.	Теоретическая подготовка	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
		Разработка собственных скриптов с использованием ИИ для автоматизации задач пентестинга, включая перебор директорий и сбор активных страниц сайта.	Самостоятельная работа	1
		Текущий контроль по теме "Автоматизация пентестинга на Python с использованием ИИ"	Текущий контроль	1
	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.	Теоретическая подготовка	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	1
		Текущий контроль по теме "Анализ результатов и генерация отчетов с помощью ИИ"	Текущий контроль	1
	Промежуточная аттестация	Тестирование 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.	Промежуточная аттестация	1

Итоговый контроль/аттестация	Итоговый контроль/аттестация по ДОП	Представление итогового проекта 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).	Итоговый контроль/аттестация	4.00

		Объем в ак.ч.	**Объем в %**
ИТОГО ПО ПРОГРАММЕ:	Теоретическая подготовка	32,00	21,62
	Практическая работа	84,00	56,76
	Самостоятельная работа	8,00	5,41
	Текущий контроль	16,00	10,81
	Промежуточная аттестация	4,00	2,70
	Итоговый контроль/аттестация	4.00	2,70
	Всего:	**148**	

ИТиСИ	Часы ИТиСИ не входят в общую трудоемкость ДОП, но участие в ИТиСИ обязательно для всех успешно прошедших итоговый контроль/аттестацию по ДОП

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	2025-09-22	1	2025-09-22	69	2026-05-29
				2	2025-12-01	64	
				3	2026-02-03	56	
				4	2026-03-30	61	

Сведения об условиях реализации ДОП (в том числе материально-техническое, информационное, кадровое обеспечение)

Материально-технические и информационные условия реализации ДОП

Наименование поля	Значение полей	Значение полей	Значение полей	Значение полей
Порядковый номер модуля	1	2	3	4
Перечень требований к оснащению площадки (для офлайн-формата)	«Не заполняется»	«Не заполняется»	«Не заполняется»	«Не заполняется»

Наименование требуемого оборудования (для онлайн-формата)	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 (для онлайн-формата)	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).

Информационные условия реализации ДОП (заполняется по каждому модулю):

Наименование поля	Значение полей	Значение полей	Значение полей	Значение полей
Порядковый номер модуля	1	2	3	4

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 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: 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. 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. - 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.	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 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.	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 кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/articles/276477/ (дата обращения: 05.07.2025) - Текст: электронный.

Наименование поля	Значение полей	Значение полей	Значение полей	Значение полей
Порядковый номер модуля	1	2	3	4

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 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.	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.

Кадровое обеспечение

Сведения о работниках, привлекаемых к реализации и разработке ДОП

ФИО	Роль	Наименование основного места работы	Должность	Ученая степень	Ученое звание	Ссылка на веб-страницы с портфолио	Образование. Наименование учебного заведения	Образование. Год окончания учебного заведения	Образование. Полученная специальность	Стаж работы в данной (аналогичной) должности	Основание для привлечения к реализации ДОП (трудовой договор, договор ГПХ, иное)	Информация о курсах повышения квалификации по профилю преподаваемой дисциплины (за последние 3 года)	Опыт работы в сфере ИТ (в области программирования, робототехники, искусственного интеллекта)	Отметка о полученном согласии на обработку персональных данных
строка	строка	строка	строка	строка	строка	каждая ссылка с новой строки	строка	числовое значение	строка	числовое значение	строка	строка	строка	строка
Сойманова Светлана Викторовна	Разработчик	РУКОН Цель	Методист			https://цель-обучение.рф/experts/soymanova	Пермский государственный университет	2002	Географ. Преподаватель. по специальности "География"	10	Трудовой договор	Вопросы применения средств криптографической защиты информации (СКЗИ), 72 час., Автономная некоммерческая организация дополнительного профессионального образования «Центр профессионального развития ПРОФИ», 2024 г.		Да

Зигуля Андрей Сергеевич	Разработчик	ООО «Дилибриум»	Генеральный директор ООО «Дилибриум»			https://цель-обучение.рф/experts/zigulya	Сумской техникум пищевой промышленности	2002	Специальность "Обслуживание компьютерных и интеллектуальных систем и сетей"	10	Договор ГПХ	Проектно-образовательный интенсив «Архипелаг 2024»	Опыт работы: 21 год. Работа в составе экспертной группы проекта «Масштабирование на региональном уровне модели кадрового обеспечения внедрения передовых производственных технологий» Агентство по развитию человеческого капитала в Северо-Западном федеральном округе и Фонда инфраструктурных и образовательных программ (группа РОСНАНО), сотрудничество в области инновационного развития с ОАО «РЖД», направленного на внедрение высокотехнологичных инновационных решений предусматривающих использование технологий, процессов или продуктов, ранее не применявшихся ОАО «РЖД», Aquamatica – роботизированные аквафермы (действующий резидент Сколково), участие в круглых столах Государственной Думы РФ посвященных информационной безопасности. Выступление в Государственной Думе РФ с докладом «Манипуляция общественным сознанием посредством интернет технологий». Финалист конкурса Архипелаг 20.35. Автор учебных курсов «Цифровая трансформация бизнеса» совместно с Санкт-Петербургским Государственным Университетом,	Да

													образовательная платформа Coursera, «Цифровая трансформация в государственном управлении» совместно с Российской Академией Народного Хозяйства и Государственной Службы при Президенте РФ.	
Почаевец Андрей Андреевич	Преподаватель	РУКОН Цель	Программный директор АНО ДПО МЦК "Цель", преподаватель линейки программ 1С. Эксперт в области программирования в 1С и управления командой разработчиков.			https://цель-обучение.рф/experts/pochaevets	Государственное образовательное учреждение высшего профессионального образования "Архангельский государственный технический университет"	2007	Инженер по специальности "Информационные системы и технологии"	4	Трудовой договор		Опыт работы в сфере IT более 15 лет. Участие в проектах цифровизации бизнес-процессов и внедрения ERP-решений в компаниях различных отраслей. Опыт автоматизации от продаж и маркетинга до комплексных систем управления предприятиями. Основное направление деятельности – внедрение и адаптация 1С для решения задач управленческого учета, бюджетирования и контроля проектов. Опыт внедрения таких решений как 1С:ERP, 1С:Комплексная автоматизация, 1С:CRM и настройка их интеграцию с другими бизнес-системами. Успешная практика реализации проектов в строительной сфере, тяжелом машиностроении, производстве, энергетике и гостиничном бизнесе. Участие в разработке и проведении обучающих программ по работе с 1С. Подготовка более 2000 аналитиков и программистов. А также опыт работы в международных проектах и работе с крупными промышленными предприятиями, где требуется комплексный подход к цифровой трансформации.	Да

Волков Александр Георгиевич	Преподаватель, Разработчик	Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»	Директор Института развития квалификаций	Кандидат технических наук	Доцент	https://цель-обучение.рф/experts/volkov	Мордовский ордена Дружбы народов госуниверситет им. Н.П. Огарева	1983	Промышленная электроника	21	Трудовой договор			Да
Рыбалёва Ирина Александровна	Разработчик	РУКОН Цель	Руководитель образовательного процесса	Кандидат педагогических наук		https://цель-обучение.рф/experts/rybaleva	Комсомольский-на-Амуре государственный педагогический институт (учитель русского языка и литературы	1994	Учитель русского языка и литературы	15	Договор об оказании услуг с индивидуальным предпринимателем	Развитие инфраструктуры авиационных систем на современном этапе, 72 час., АНО ДПО "МЦК "Цель", 2024 г.		Да
Пантелеев Сергей Владимирович	Преподаватель, Разработчик	Филиал НИТУ МИСиС г. Выкса	Доцент кафедры БД	Кандидат технических наук	Доцент	https://цель-обучение.рф/futurecode/panteleev	Владимирский государственный университет	1999	Инженер по специальности "Проектирование и технология радиоэлектронных средств"	26	Договор об оказании услуг с самозанятым лицом	Интенсив от университета Зерокодинга: AI-ассистент, интегрированный в Telegram, 2025 г.	Преподавание IT-дисциплин (Муромский институт ВлГУ, Выксунский металлургический техникум, Выксунский филиал НИТУ МИСиС) Программирование, системное администрирование с 2012 года (АО "Выксаэнерго", Нижновэнерго). Разработка сайтов с 2005 года (ООО "Виртуальная Выкса", самозанятость) к.т.н по искусственному интеллекту, специальность 05.13.01 "Системный анализ, управление и обработка информации", тема диссертации "Разработка, исследование и применение нейросетевых алгоритмов идентификации и управления динамическими системами". Преподаватель курсов «Технология программирования» (на Python), «Вычислительные машины, системы и сети», «Протоколы сетей», «Интернет-технологии» (HTML, CSS, PHP, Python, JavaScript, Jquery, MySQL, CMS).	Да

Кротов Александр Викторович	Разработчик	Код Грин Инжиниринг	Генеральный директор			https://цель-обучение.рф/experts/krotov	ФГБОУ ВПО "Санкт-Петербургский государственный электротехнический университет"ЛЭТИ" им. В.И. Ульянова (Ленина), 2012	2012	Инженер по специальности "Электронные приборы и устройства"	9	Договор ГПХ		Опыт работы в сфере IT - 8 лет. Компании: ЦНИИ РТК, ООО "НИЦ Радиотехники", Код Грин Инжиниринг.	Да

Формы аттестации и оценочные материалы (комплект контрольно-измерительных материалов, позволяющих определить достижение Получателями поддержки планируемых результатов)

Наименование поля	Значение полей
Текущий контроль	
Модуль 1, Основы Python для кибербезопасности и искусственный интеллект, Введение в Python: синтаксис, среды разработки	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что означает аббревиатура IDE в контексте разработки программного обеспечения? 2. Какой из перечисленных типов данных используется для хранения целых чисел в Python? 3. При установке Python на компьютер рекомендуется отметить опцию "Add python.exe to 4. Какая функция используется для получения данных от пользователя в Python? 5. Какое расширение имеет файл с исходным кодом Python? 6. Что будет результатом выполнения выражения `5 / 2` в Python? 7. Какой символ используется для создания однострочного комментария в Python? 8. Какая из перечисленных IDE является официальной средой разработки для Python? 9. Какая функция используется для преобразования строки в вещественное число? 10. Что будет результатом выполнения `print("Hello" * 3)`? 11. Какая функция используется для округления числа до двух знаков после запятой? 12. Какой оператор используется для возведения числа в степень? 13. Что делает функция len() применительно к списку? 14. Какой тип данных будет у переменной после выполнения x = 5 + 3.0? 15. Что произойдет, если не соблюдать отступы в Python?
Модуль 1, Основы Python для кибербезопасности и искусственный интеллект, Типы данных в Python и их применение	
Количество академических часов	1
Формы контроля	Тестовая форма контроля
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.

Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что из перечисленного является целочисленным типом данных в Python? 2. Какой тип данных используется для хранения текстовой информации? 3. Какой оператор используется для проверки равенства значений в условных выражениях? 4. Какая структура данных является изменяемой? 5. Что будет результатом выполнения кода: print(type(3.14))? 6. Какая функция используется для преобразования строки в целое число? 7. Какой метод используется для добавления элемента в конец списка? 8. Что будет результатом выполнения кода: "Python" + " is awesome"? 9. Какой оператор используется для проверки неравенства? 10. Какая из следующих структур данных является упорядоченной и может содержать дубликаты? 11. Что будет результатом выполнения кода: len("hello")? 13. Какой тип данных получится при делении двух целых чисел? 14. Что будет результатом выполнения кода: 5 // 2? 15. Что будет результатом выполнения кода: "hello"[1]?
Модуль 1, Основы Python для кибербезопасности и искусственный интеллект, Модули и функции языка Python	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что такое функция в Python? 2. Какое ключевое слово используется для создания функции в Python? 3. Что возвращает функция в Python, если явно не указано возвращаемое значение? 4. Как правильно импортировать модуль math? 5. Для чего используется модуль random? 6. Какой метод используется для выбора случайного элемента из списка? 7. Что будет результатом выполнения: math.sqrt(16)? 8. Какой символ используется для начала тела функции? 9. Можно ли использовать одну функцию внутри другой? 10. Что такое параметры функции? 11. Какая функция используется для округления числа? 12. Как проверить длину строки s? 13. Что будет результатом: 'abc' in 'abcdef'? 14. Что делает функция re.findall()? 15. Какой модуль нужен для работы с регулярными выражениями?
Модуль 1, Основы Python для кибербезопасности и искусственный интеллект, Файлы и исключения в Python, использование ИИ при разработке программ на Python	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.

Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какой режим открытия файла в Python используется для чтения? 2. Что произойдет, если открыть файл в режиме 'w', а файл с таким именем уже 3. Какой метод используется для записи строки в файл? 4. Что делает конструкция with ... as при работе с файлами? 5. Какая ошибка возникает при попытке деления на ноль? 6. Какой блок используется для выполнения кода независимо от того, возникло исключение или нет? 7. Какой метод возвращает текущую позицию указателя в файле? 8. Какая ошибка возникает при попытке открыть несуществующий файл для чтения? 9. Какой формат файла удобен для обмена данными между программами благодаря структуре "ключ-значение"? 10. Что делает метод readlines()? 11. Какой метод устанавливает позицию указателя в файле? 12. Какой вид ИИ специализируется на одной или нескольких задачах? 13. Какая команда преобразует строку в число с плавающей точкой? 14. Что происходит с файлом, если он не был явно закрыт после работы? 15. Какой метод используется для чтения всего содержимого файла?
Модуль 2, Основы информационной безопасности с элементами ИИ и работа с компьютерными сетями, Ключевые концепции кибербезопасности	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что из перечисленного является основной целью этичного хакера? 2. Какой из перечисленных портов обычно используется для HTTP-трафика? 3. Что из перечисленного НЕ является частью триады информационной безопасности? 4. Какая служба обычно работает на порту 445 TCP в Windows? 5. Какой из следующих методов НЕ является эффективным способом защиты информации? 6. Какое действие следует предпринять при обнаружении подозрительного открытого порта? 7. Какой порт используется для HTTPS? 8. Что из перечисленного является примером социальной инженерии? 9. Какой инструмент используется для сканирования открытых портов? 10. Какой порт обычно используется для DNS? 11. Какой стандарт регламентирует управление информационной безопасностью? 12. Что из перечисленного является примером уязвимости? 13. Какой из перечисленных портов используется для SSH? 14. Что из перечисленного является важным элементом защиты от вирусов? 15. Какой из перечисленных методов является эффективным способом защиты от фишинга?
Модуль 2, Основы информационной безопасности с элементами ИИ и работа с компьютерными сетями, Угрозы безопасности и инструменты для их обнаружения	
Количество академических часов	1

Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что из перечисленного НЕ является угрозой информационной безопасности? 2. Какое основное правило информационной безопасности? 3. Какой метод НЕ относится к методам обеспечения безопасности? 4. Что из перечисленного НЕ является инструментом обеспечения безопасности? 5. Какая библиотека Python используется для работы с сетевыми пакетами? 6. Какой протокол является основным для передачи данных в сетях? 7. Какая функция модуля socket используется для получения IP-адреса по имени хоста? 8. Какой порт по умолчанию используется для HTTP? 9. Какой метод Python используется для проверки открытых портов? 10. Какой адрес является широковещательным MAC-адресом? 11. Какой тип сканирования используется для определения активных хостов в сети? 12. Какой модуль Python используется для работы с IP-адресами и сетями? 13. Какой метод используется для отправки пакетов в Scapy? 14. Какое значение возвращает метод connect_ex при успешном соединении? 15. Какой протокол используется для получения MAC-адреса по IP?
Модуль 2, Основы информационной безопасности с элементами ИИ и работа с компьютерными сетями, Этичный хакинг: методы тестирования с помощью ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что такое этичный хакинг? 2. Какой инструмент используется для сканирования сети и обнаружения уязвимостей? 3. Какой режим работы сетевого адаптера в VirtualBox необходим для доступа к bWAPP с основной ОС? 4. Какое веб-приложение используется для тренировки навыков поиска уязвимостей? 5. Что такое пентестинг? 6. Какой командой можно узнать IP-адрес в Linux? 7. Для чего используется VirtualBox в обучении этичному хакингу? 8. Какой тип системы нужно выбрать при создании bWAPP в VirtualBox? 9. Что является основной целью этичного хакинга? 10. Какой инструмент используется для анализа трафика? 11. Что необходимо заключить перед проведением этичного хакинга? 12. Что делать, если скачанный файл bWAPP помечается как зловредный? 13. Какой принцип важен при проведении этичного хакинга? 14. Какой этап является первым при подготовке тестовой среды? 15. Где можно легально скачать образ bWAPP?
Модуль 2, Основы информационной безопасности с элементами ИИ и работа с компьютерными сетями, Защита от атак с использованием ИИ	

Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что является одной из основных мер безопасности для защиты информации? 2. Какой пакет Python используется для шифрования данных? 3. Какой метод шифрования использует один и тот же ключ для шифрования и расшифровки данных? 4. Какой модуль из пакета cryptography предоставляет простой способ шифрования файлов? 5. Какой модуль Python используется для генерации случайных паролей? 6. Какой алгоритм шифрования используется в модуле Fernet? 7. Что обязательно должно содержаться в надежном пароле? 8. Какая функция используется для генерации ключа в модуле Fernet? 9. Какой метод защиты данных обеспечивает конфиденциальность даже при хранении и передаче по незащищенным каналам связи? 10. Что такое RockYou? 11. Какой тип шифрования использует пару ключей - открытый и закрытый? 12. Какой символ используется для обозначения байтовой строки в Python? 13. Что НЕ рекомендуется делать при создании надежного пароля? 14. Какой метод используется для расшифровки данных в модуле Fernet? 15. Какой метод защиты от хакерских атак требует подтверждения через несколько различных способов аутентификации?
Модуль 3, Веб-безопасность и ИИ: обнаружение уязвимостей, Основы веб-разработки с применением ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.

	1. Что означает аббревиатура HTTP? 2. Какой протокол обеспечивает безопасную передачу данных? 3. Какой тег используется для создания заголовка первого уровня в HTML? 4. Где должен располагаться CSS файл styles.css по стандарту Flask? 5. Какой метод маршрутизации используется во Flask для обработки главной страницы? 6. Какой модуль необходимо импортировать для работы с Flask? 7. Какой тег используется для подключения CSS файла в HTML документ? 8. Какой атрибут используется для указания ссылки на изображение в HTML? 9. Какой командой запускается Flask приложение? 10. Как называется папка, где хранятся HTML шаблоны во Flask? 11. Какой тег используется для создания гиперссылки в HTML? 12. Каким образом можно задать цвет текста в CSS? 13. Какой порт по умолчанию использует Flask при запуске? 14. Какой язык используется для стилизации HTML документов? 15. Какой метод используется для отображения шаблонов во Flask?
Модуль 3, Веб-безопасность и ИИ: обнаружение уязвимостей, XSS, SQL-инъекции, и другие атаки: как ИИ помогает в защите	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что такое XSS-атака? 2. Какой метод защиты наиболее эффективен против SQL-инъекций? 3. Что такое CSRF-атака? 4. Какая из перечисленных уязвимостей относится к HTML-инъекциям? 5. Введите XSS-инъекцию, которая вызовет alert с текстом "12345". 6. Что является основным механизмом защиты от большинства веб-уязвимостей? 7. Какой тип XSS-атаки хранит вредоносный код на сервере? 8. Что делает следующий SQL-запрос: SELECT * FROM users WHERE id=1 OR 1=1? 9. Какой символ часто используется для комментирования части SQL-запроса? 10. Какой HTTP-метод чаще всего используется для отправки данных формы? 11. Какой метод защиты рекомендуется использовать против CSRF-атак? 12. Какой результат даст следующий JavaScript код: document.getElementById('test')? 13. Какой тип XSS-атаки отражает вредоносный код обратно пользователю? 14. Как называется процесс проверки подлинности пользователя? 15. Какой метод защиты рекомендуется использовать для предотвращения XSS-атак?
Модуль 3, Веб-безопасность и ИИ: обнаружение уязвимостей, Шифрование и безопасное хранение данных с применением ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.

Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что такое XSS-атака? 2. Какой метод помогает ИИ обнаруживать SQL-инъекции? 3. Какая из следующих мер наиболее эффективна против XSS-атак? 4. Что такое SQL-инъекция? 5. Какую роль играет искусственный интеллект в защите от XSS? 6. Какой из нижеперечисленных методов НЕ помогает защититься от SQL-инъекций? 7. Каков код ответа при успешном обращении на сайт? 8. Какой из следующих типов XSS является наиболее опасным? 9. Какой из следующих методов является частью стратегии защиты от XSS? 10. Как называется тип XSS-атаки, при котором вредоносный код сохраняется на сервере? 11. Какую роль играет механизм SameSite в cookie для защиты от CSRF? 12. Какую задачу решает механизм Escaping в контексте защиты от XSS? 13. Какой из следующих методов помогает защититься от CSRF-атак? 14.Какая библиотека Python используется для отправки запросов на сайт? 15. Какой из следующих методов является наиболее эффективной защитой от всех типов.
Модуль 3, Веб-безопасность и ИИ: обнаружение уязвимостей, Этические аспекты веб-безопасности с использованием ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что такое XSS-атака в контексте веб-безопасности? 2. Какая функция Python используется для экранирования специальных символов HTML для защиты от XSS-атак? 3. Какой механизм защиты рекомендуется использовать для предотвращения CSRF-атак? 4. Что является основной целью внедрения HTTPS в веб-приложениях? 5. Какое ограничение рекомендуется устанавливать для комментариев пользователей с точки зрения безопасности? 6. Какой язык программирования в основном используется для внедрения XSS-инъекций? 7. Какой метод защиты данных рекомендуется использовать при хранении паролей пользователей? 8. Какой стандарт безопасности необходимо соблюдать при разработке этичного веб-приложения? 9. Что рекомендуется делать с неиспользуемыми портами на сервере? 10. Как часто рекомендуется обновлять зависимости веб-приложения? 11. Что такое Content Security Policy (CSP)? 12. Какой метод проверки входных данных наиболее эффективен для предотвращения SQL-инъекций? 13. Что необходимо делать с журналами безопасности сервера? 14. Какой метод аутентификации считается наиболее безопасным? 15. Какой метод защиты рекомендуется использовать против brute-force атак?
Модуль 4, Практический пентестинг с Python и ИИ, Основы пентестинга: ручное и автоматизированное тестирование с ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.

Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что означает термин "пентестинг"? 2. Какая из перечисленных областей НЕ относится к основным направлениям пентестинга? 3. Какой первый этап в процессе проведения пентестинга? 4. Какое правило является главным при проведении пентестинга? 5. Какой протокол передачи данных обеспечивает безопасное соединение? 6. Какую команду можно использовать для определения IP-адреса в Linux? 7. Какой из перечисленных сервисов является системой управления базами данных? 8. Как называется тип атаки, при которой злоумышленник может объединить результаты 9. Какой уровень безопасности нужно выбрать в DVWA для выполнения базовой SQL-инъекции? 10. Какой из перечисленных портов обычно используется для HTTP-сервисов? 11. Какой инструмент можно использовать для сканирования открытых портов? 12. Какой метод защиты от XSS реализован в DVWA на уровне Medium? 13. Какой из перечисленных элементов обязательно должен быть включен в отчет о пентесте? 14. Какой протокол используется для безопасного удаленного подключения к серверу? 15. Какой из перечисленных вариантов является примером SQL-инъекции?
Модуль 4, Практический пентестинг с Python и ИИ, Инструменты для пентеста, включая ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какая операционная система предоставляет предустановленный набор инструментов для пентестинга? 2. Какой инструмент используется для перехвата сетевого трафика и анализа пакетов? 3. С помощью какого инструмента можно проводить автоматизированный перебор паролей? 4. Какое приложение помогает находить уязвимости SQL-инъекций? 5. Для чего используется инструмент Dirbuster? 6. Какой тип сетевого адаптера нужно выбрать в VirtualBox для связи Kali Linux с DVWA? 7. Какой из инструментов НЕ входит в состав Kali Linux? 8. Какую команду можно использовать для проверки связи между виртуальными машинами? 9. Как называется инструмент для анализа безопасности веб-приложений, который позволяет просматривать HTTP-трафик? 10. Какой инструмент предназначен для сканирования уязвимостей веб-серверов? 11. В какой категории приложений Kali Linux находится Wireshark? 12. Что означает аббревиатура DVWA? 13. Какой компонент Burp Suite отвечает за перехват HTTP-трафика? 14. Какой метод защиты может помешать успешному перехвату трафика в реальных условиях? 15. Какой процесс автоматизирует sqlmap?
Модуль 4, Практический пентестинг с Python и ИИ, Автоматизация пентестинга на Python с использованием ИИ	
Количество академических часов	1

Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что такое автоматизированное тестирование безопасности? 2. Какая библиотека Python используется для работы с SSH? 3. Какой HTTP-статус код обычно указывает на успешный запрос? 4. Что такое Scapy? 5. Какой модуль Python часто используется для отправки HTTP-запросов? 6. Какой порт обычно используется для SSH-подключения? 7. Какой метод HTTP чаще всего используется для отправки данных формы? 8. Какая команда используется для сканирования открытых портов? 9. Какой метод рекомендуется использовать при разработке скриптов для пентестинга? 10. Какой тип уязвимости может позволить удаленно выполнять команды на сервере? 11. Какой из следующих элементов НЕ является частью HTTP-запроса? 12. Что такое payload в контексте пентестинга? 13. Какой из следующих элементов важен при тестировании на проникновение? 14. Что делает функция requests.get()? 15. Какой из следующих элементов является важным при написании скриптов для пентестинга?
Модуль 4, Практический пентестинг с Python и ИИ, Анализ результатов и генерация отчетов с помощью ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какой инструмент рекомендуется использовать для сканирования открытых портов в процессе тестирования на проникновение? 2. Какая уязвимость характеризуется возможностью внедрения и выполнения вредоносного JavaScript кода? 3. Что является основной рекомендацией по устранению уязвимости SQL-инъекции? 4. Какой методологией рекомендуется руководствоваться при проведении тестирования на проникновение? 5. Что рекомендуется использовать для защиты от атак подбора пароля SSH? 6. Какой элемент должен быть обязательно включен в заключительную часть отчета о тестировании на проникновение? 7. Какой инструмент рекомендуется использовать для обнаружения известных уязвимостей на веб-сервере? 8. Какое действие рекомендуется предпринять при обнаружении уязвимости XSS? 9. Какой тип тестирования проводился для веб-приложений DVWA и bWAPP? 10. Какой инструмент рекомендуется использовать для перебора директорий и файлов на веб-сервере? 11. Какие меры безопасности рекомендуется внедрить для защиты от атак подбора пароля? 12. Какую информацию необходимо указать в разделе "Объект тестирования" отчета? 13. Какой элемент НЕ является обязательным при составлении отчета о тестировании на проникновение? 14. Какой порт обычно используется для SSH-соединений? 15. Какой уровень критичности имеет уязвимость SQL-инъекции?

Промежуточная аттестация (по модулям)	
Основы Python для кибербезопасности и искусственный интеллект, Модуль 1	
Количество академических часов	1
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.
Варианты заданий (представлены в качестве приложения к ДОП)	1. Что означает алгоритм? 2. Что такое переменная? 3. Что такое функция? 4. Что такое оператор? 5. Что такое компиляция? 6. Какая управляющая конструкция используется для выполнения определенного блока кода многократно до тех пор, пока условие истинно? 7. Какая управляющая конструкция используется для выполнения определенного блока кода, если условие истинно, и альтернативного блока кода, если условие ложно? 8. Какая управляющая конструкция используется для перебора элементов в последовательности, такой как список или строка? 9. Необходимо создать программу, которая будет хранить уникальные элементы (например, идентификаторы пользователей). Какую структуру данных следует использовать для решения этой задачи? 10. Какая структура данных используется для хранения пар ключ-значение? 11. Какая структура данных представляет собой неизменяемую последовательность элементов? 12. Как объявить функцию в Python? 13. Как передать аргументы в функцию в Python? 14. Что такое возвращаемое значение функции? 15. Как вызвать функцию в Python? 16. Функция для чтения всего содержимого файла в строку. 17. Ключевое слово для создания анонимной функции. 18. Что выведется на экран в результате работы данной программы? a = 5 b = 7 print(a+b*a) 19. С помощью какого ключевого слово можно объявить функцию в Python? 20. Что выведется на экран в результате работы данной программы? def add(a, b): return a + b result = add(2, 3) print(result)
Шкала оценивания, нижнее значение	0
Шкала оценивания, верхнее значение	20
Шкала оценивания, минимальный проходной балл	10
Основы информационной безопасности с элементами ИИ и работа с компьютерными сетями, Модуль 2	
Количество академических часов	1
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.
Варианты заданий (представлены в качестве приложения к ДОП)	1. Каковы основные аспекты информационной безопасности согласно триаде информационной безопасности? 2. Потенциальные события или действия, которые могут нанести ущерб информационной системе или данным - это… 3. Слабые места в системе, которые могут быть использованы злоумышленниками для нарушения безопасности - это… 4. Фишинг - это… 5. Вирусы - это… 6. Несанкционированный доступ к компьютерным системам с целью получения конфиденциальной информации или нарушения их функциональности - это… 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. 8. Выберите надежный способ(-ы) защиты информационных систем. 9. Для каких задач можно использовать программы на языке Python? 10. Как называют эксперта по безопасности, который проводит тестирование на проникновение? 11. Какой из перечисленных инструментов является одним из самых распространенных сканеров локальной сети? 12. Как называется специализированная среда, которая изначально является уязвимой, для проведения тестов на проникновение? 13. Какая главная причина значимости регулярного обновления ПО и операционных систем: 14. С какой целью проводится сканирование безопасности локальной сети: 15. Какие рекомендации самые эффективные для создания паролей? 16. Как называется атака, при которой злоумышленник пытается получить конфиденциальную информацию, манипулируя пользователем? 17. Какой инструмент используется для перехвата сетевого трафика? 18. Как называется процесс проверки подлинности пользователя при входе в систему? 19. Какой инструмент используется для сканирования портов в сети? 20. Как называется операционная система, специально созданная для тестирования на проникновение?
Шкала оценивания, нижнее значение	0
Шкала оценивания, верхнее значение	20
Шкала оценивания, минимальный проходной балл	10
Веб-безопасность и ИИ: обнаружение уязвимостей, Модуль 3	
Количество академических часов	1
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.

Варианты заданий (представлены в качестве приложения к ДОП)	1. В чем основное отличие HTTP от HTTPS? 2. Стандартизированный язык разметки документов для просмотра веб-страниц в браузере- это? 3. Часть текста/картинки, ссылающаяся на другую часть документа/другую страницу? 4. Какие элементы входят в типичную структуру HTML-страницы? 5. Формальный язык описания внешнего вида документа, написанного с использованием языка разметки - это? 6. Расширяемый язык разметки - это? 7. Уязвимость, основанная на недостатках архитектуры веб-сайта при обращении запросов к базам данных - это? 8. С каким языком программирования в основном связана XSS-уязвимость? 9. Атака подделки межсайтовых запросов - это? 10. Для чего используется bWAPP? 11. Чем отличается симметричное и асимметричное шифрование? 12. Выберите из названных алгоритмов шифрования симметричные. 13. Выберите из названных алгоритмов шифрования асимметричные. 14. Какой процесс чаще всего применяется к паролям для их хранения? 15. Выберите из списка алгоритмы хэширования? 16. Какая организация отвечает за модернизацию языка HTML? 17. Какой номер порта по умолчанию используется протоколом HTTPS для безопасной передачи данных? 18. Сколько алгоритмов хэширования перечислено в списке: MD5, SHA-256, Bcrypt, AES, RSA, DES? 19. Как называется тип шифрования, при котором используется один ключ для шифрования и расшифровки данных? (Ответ напишите одним словом.) 20. Как называется процесс одностороннего шифрования?
Шкала оценивания, нижнее значение	0
Шкала оценивания, верхнее значение	20
Шкала оценивания, минимальный проходной балл	10
Практический пентестинг с Python и ИИ, Модуль 4	
Количество академических часов	1
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.

Варианты заданий (представлены в качестве приложения к ДОП)	1. Какие бывают типы атак при пентесте? 2. Что такое DVWA? 3. Как определить этические принципы при проведении пентеста? 4. Какая информация требуется тестировщикам безопасности для проведения пентеста? 5. Какой инструмент чаще всего используется для работы с анализом трафика и перехваченными пакетами? 6. Как называется утилита поиска имен директорий и файлов доступного веб-сервиса? 7. Какая операционная система чаще всего используется тестировщиками на проникновение? 8. Какие инструменты подходят для проведения тестирования безопасности веб-сайта? 9. Как называется программная библиотека для манипулирования сетевыми пакетами на языке программирования Python? 10. Какая Python библиотека используется для отправки HTTP запросов на сайты? 11. Каким образом фиксируются ход и результаты проведения пентеста? 12. Каковы цели проведения пентеста? 13. Какой вид тестирования самый эффективный? 14. Что обычно НЕ входит в отчет о проведенном пентесте? 15. Используя инструмент ping, определите IP-адрес сервера по доменному имени localhost. Укажите IP-адрес сервера. 16. Как называется операционная система, которая чаще всего используется тестировщиками на проникновение? Напишите название этой системы. 17. Как называется инструмент, который чаще всего используется для анализа сетевого трафика и перехвата пакетов? Напишите название этого инструмента. 18. Как называется утилита, которая помогает находить скрытые директории и файлы на веб-серверах? Напишите название этой утилиты. 19. Как называются соревнования по поиску уязвимостей и кибербезопасности? Напишите название этих соревнований (сокращение из трех букв). 20. Как называется специальное небезопасное веб-приложение, которое используется для изучения пентеста? Напишите название этого приложения.
Шкала оценивания, нижнее значение	0
Шкала оценивания, верхнее значение	20
Шкала оценивания, минимальный проходной балл	10

Итоговый контроль / аттестация	
Количество академических часов	4.00
Формы контроля	Представление итогового проекта
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).
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.

Варианты заданий (представлены в качестве приложения к ДОП)	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 (стеногрaфия - LSB на примере) или потенциально вредоносных ссылок в описании с использованием PIL/OpenCV и requests/BeautifulSoup.
Шкала оценивания, нижнее значение	0.00
Шкала оценивания, верхнее значение	30.00
Шкала оценивания, минимальный проходной балл	16.00
Дополнительные сведения (предложения по ЕВИ и ИТиСИ)	

Вопросы для ЕВИ	1. Что такое алгоритм? - Устройство для хранения данных - Последовательность шагов для выполнения задачи - Способ обработки ошибок - Язык программирования 2. Какая управляющая конструкция используется для выполнения определенного блока кода многократно до тех пор, пока условие истинно? - if-else - for - while - switch 3. Что делает оператор "not"? - Инвертирует логическое значение - Проверяет равенство - Делает цикл - Вызывает функцию 4. Что такое переменная? - Устройство для хранения данных - Изменяемое значение в программе - Комментарий - Оператор 5. Какой тип данных представляет собой целое число? - float - str - int - bool 6. Какой оператор используется для проверки равенства? - = - == - != - <= 7. Какой результат будет у выражения: 3 * 2 + 1? - 7 - 9 - 8 - 6 8. Что выведет код: print(2**3)? 9. Какой оператор используется для присваивания?

	- = - == - := - === 10. Что возвращает функция type()? - Тип объекта - Значение переменной - Имя переменной - Размер объекта 11. Что делает функция print() в Python? - Принимает ввод - Сохраняет данные - Выводит информацию на экран - Очищает экран 12. Какой результат у выражения 9 // 2? - 4 - 4.5 - 5 - Ошибка 13. Что вернет выражение len("12345")? - 4 - 5 - 3 - Ошибка 14. Что означает выражение a += 2? - Умножение - Деление - Увеличение на 2 -Ошибка 15. Какой тип данных возвращает выражение 5 > 3? - str - int - bool - float

Вопросы для ИТиСИ	1. Укажите, какой результат будет выведен на экран после выполнения кода a = 12 b = 13 c = 2 a, b = b, a print(a - b + c) 2. Укажите, какой результат будет выведен на экран после выполнения кода. x = 5 y = 7 c = x x = y y = c print(x) 3. С помощью какого ключевого слово можно объявить функцию в Python? 4 . Какой тип данных создается конструкцией {}? - Список - Множество - Словарь - Кортеж 5. Что делает функция enumerate()? - Возвращает пары индекс-значение - Сортирует элементы - Удаляет элементы - Преобразует строку 6. Какая функция возвращает минимальное значение? 7. Какой метод преобразует список в строку? - join() - split() - convert() - map() 8. Что делает pass? 9. Укажите, какой результат будет выведен на экран после выполнения кода. try: a = 7 / 0 print(a) except: print(10)

	10. Что делает функция round()? - Преобразует строку в число - Возвращает целое число - Округляет число - Делит число 11. Что вернет выражение bool(0)? - True - 0 - False - None 12. Укажите, какой результат будет выведен на экран после выполнения кода a = 10 b = 15 c = a f, c = b + a , a print(f + c) 13. Что вернёт: print("Python"[0])? 14. Что делает функция int("5")? - Преобразует строку в число (Правильный ответ) - Удаляет пробелы - Создает список - Проверяет тип 15. Укажите, какой результат будет выведен на экран после выполнения кода. a = 10 b = 3 a = a - a % 3 a, b = b, a print(b ** a)

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», геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного 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, - технологий «перевернутого класса», геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного 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, - технологий «перевернутого класса», геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного 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, - технологий «перевернутого класса», геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного обучения.

Методические разработки (представлены в качестве приложения к ДОП)	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 (представлены в качестве приложения к ДОП)	Материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, 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.	Материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, 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.	Материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, 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.	Материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, 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, 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.	Black Hat Python: программирование для хакеров и пентестеров. 2-е изд. — СПб.:Питер, 2022. — 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»).	Python. Разработка на основе тестирования. / пер. с англ. Логунов А. В. – М.: ДМК Пресс, 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»).	Искусство тестирования на проникновение в сеть / пер. с анг. В. С. Яценкова. – М.: ДМК 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»).

Основные данные ДОП: УРОВЕНЬ БАЗОВЫЙ

№ п/п	Наименование поля	Значение поля
1.	Название ДОП	Этичный хакинг: инструменты защиты на Python и ИИ
2.	Уровень сложности ДОП	БАЗОВЫЙ
3.	Объем/общая трудоемкость ДОП (общий объем освоения ДОП в академических часах)	148.00
4.	Объем каждого модуля в ак.ч.	Модуль1 - 36 Модуль2 - 36 Модуль3 - 36 Модуль4 - 36
5.	Общее количество образовательных мероприятий	116
6.	Объем недельной нагрузки обучающегося	4.00

7.	Дата начала и дата окончания обучения по ДОП (срок освоения ДОП)	С 2025-09-22 по 2026-05-29
9.	Выдаваемый по окончании обучения документ	Сертификат

Описание ДОП

№ п/п	Наименование поля	Значение поля
1.	Актуальность ДОП	Программа «Этичный хакинг: инструменты защиты на Python и ИИ» (базовый уровень) разработана в ответ на стремительное развитие цифровых технологий и растущие угрозы в сфере кибербезопасности. В условиях глобальной цифровизации, когда кибератаки становятся всё более сложными и масштабными, подготовка специалистов, способных противостоять этим вызовам, является критически важной., т.к.: во-первых, Программа соответствует современным вызовам и запросам рынка: рост киберугроз. По данным международных исследований, количество кибератак увеличивается ежегодно на 20–30%, а ущерб от них исчисляется триллионами рублей. Это требует подготовки специалистов, способных выявлять и устранять уязвимости на ранних этапах. дефицит кадров в сфере кибербезопасности. В России и мире наблюдается острый недостаток квалифицированных специалистов по информационной безопасности. Программа помогает сформировать у школьников интерес к этой профессии и даёт им конкурентное преимущество при дальнейшем обучении. использование искусственного интеллекта в защите данных. Современные системы безопасности всё чаще полагаются на AI для анализа угроз и автоматизации защиты. Программа учит применять ИИ для оптимизации кода, анализа уязвимостей и создания защитных решений, что соответствует мировым трендам; во-вторых, востребованность навыков в образовательной и профессиональной среде: подготовка к будущим профессиям. Программа развивает ключевые компетенции, необходимые для таких профессий, как этичный хакер, специалист по кибербезопасности, аналитик данных, разработчик защищённых систем. интеграция в школьное и дополнительное образование. Курс сочетает теорию и практику, что соответствует требованиям ФГОС и концепции развития цифровых навыков у учащихся. поддержка олимпиадного и проектного движения. Полученные знания помогут школьникам участвовать в конкурсах и хакатонах по информационной безопасности (например, CTF-соревнованиях), что повышает их мотивацию и шансы на поступление в ведущие IT-вузы; в-третьих, содержание Программы соответствует государственным приоритетам. Программа отвечает ключевым направлениям, заявленным в «Стратегии развития информационного общества в РФ», Национальной программе «Цифровая экономика» и инициативах по развитию IT-образования в школах. Она способствует: повышению цифровой грамотности молодёжи; подготовке кадров для технологического суверенитета страны; развитию отечественных решений в сфере кибербезопасности. Программа «Этичный

		хакинг: инструменты защиты на Python и ИИ» не только соответствует актуальным запросам времени, но и опережает стандартные школьные курсы, предлагая учащимся востребованные навыки будущего. Её реализация поможет сформировать новое поколение IT-специалистов, способных обеспечивать безопасность цифрового пространства России. Отличительные особенности ДОП заключаются в том, что Программа не только развивает IT-навыки, но и укрепляет междисциплинарные связи, помогая учащимся применять знания из других предметов на практике. Содержание Программы предполагает интеграцию с дисциплинами школьного цикла: информатика, математика, физика, обществознание и право, этика, английский язык. Педагоги-наставники в рамках образовательного процесса дают не только базовые знания, но и готовят учащихся к участию в престижных IT-соревнованиях и олимпиадах. Программа включает реальные кейсы: защита Wi-Fi, анализ вредоносных ссылок. Инновационность и практическая значимость программы заключаются в использовании Python и ИИ: Python — один из самых популярных языков в сфере безопасности и анализа данных. Обучение его применению в сочетании с искусственным интеллектом делает программу уникальной. Практико-ориентированный подход: учащиеся не только изучают теорию, но и разрабатывают реальные скрипты для сканирования сетей, тестирования веб-приложений и защиты от атак, что формирует прикладные навыки и формирует ответственное цифровое поведение. Программа учит этичным принципам работы с уязвимостями, что особенно важно в эпоху цифровой трансформации. 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 практический 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.

2.	Цель и задачи ДОП	Цель ДОП: Специализированное изучение выбранного языка программирования, освоение типовых библиотек и фреймворков, решение классических задач по программированию и использования профессиональных инструментов. Задачи ДОП: Обучающие: формирование базовых концепции и прикладных аспектов программирования на Python и применение ИИ; знакомство с различиями этичного хакинга и нелегальных действий, понимание ключевых принципов и кодекса этичного хакера, с классификациями атак и разрешенных действий; знакомство с основами сетевой безопасности, включая протоколы IP, TCP, UDP, HTTP, HTTPS, принципы анализа трафика, методы защиты сети, системы IDS/IPS, противодействие DDoS и угрозам Wi-Fi; знакомство с основными компонентами и уязвимостями веб-приложений, включая протоколы HTTP/HTTPS, архитектуры клиент-сервер, типов атак (XSS, SQL-инъекции и другие), методов защиты (валидация ввода, подготовленные запросы, фильтрация данных). Развивающие: развитие навыков автоматизации рутинных задач с помощью ИИ, анализа данных и создания отчётов об угрозах; 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.

3.	Планируемые результаты	В результате освоения программы выпускники будут знать: базовые концепции и прикладные аспекты программирования на Python; основы этичного хакинга, включая его отличия от нелегальных действий, методы сбора информации, принципы атак и защиты; основы сетевой безопасности, включая протоколы IP, TCP, UDP, HTTP, HTTPS, принципы анализа трафика, методы защиты сети, системы IDS/IPS, противодействие DDoS и угрозам Wi-Fi; основные компонентов и уязвимостей веб-приложений, включая протоколы HTTP/HTTPS, архитектуры клиент-сервер, типов атак (XSS, SQL-инъекции и другие), методов защиты (вали-дация ввода, подготовленные запросы, фильтрация данных). Выпускники будут уметь: применять базовые концепции программирования на Python, включая работу с переменными, типами данных, операторами, условиями, циклами, функциями, модулями и структурами данных, для написания простых программ и скриптов; эффективно обрабатывать ошибки с помощью механизмов исключений, работать с файловой системой, создавать собственные модули и использовать возможности искусственного интеллекта для генерации и оптимизации кода, что позволит им заложить прочную основу для дальнейшего изучения более сложных аспектов программирования и этичного хакинга; писать практические программы с использованием возможностей искусственного интеллекта в программировании; различать этичный хакинг от нелегальных действий, понимать ключевые принципы и кодекс этичного хакера, классифицировать атаки и разрешенные действия, использовать Python-скрипты для проверки безопасности сети, анализа доменов, проведения запросов и разработки программ для эксплуатации и защиты; применять методы сбора информации, анализировать уязвимости с помощью инструментов и сканеров, разрабатывать защитные меры против распространенных уязвимостей (буферное переполнение, инъекции кода, DoS); создавать детальные отчеты об уязвимостях и рекомендациях по защите с использованием возможностей искусственного интеллекта для автоматизации рутинных задач; анализировать сетевой трафик с помощью инструментов типа Wireshark и библиотеки pcapy, разрабатывать клиент-серверные приложения на Python, создавать программы для сканирования сети и анализа активных устройств, симулировать работу фаервола с правилами фильтрации трафика, применять методы защиты от DDoS-атак, проводить аудит безопасности Wi-Fi сетей, выявлять уязвимости в беспроводных соединениях и предлагать меры по их устранению; использовать возможности искусственного интеллекта для анализа сетевой безопасности, автоматизации процессов мониторинга и усиления защитных механиз-мов; понимать архитектуру веб-приложений, протоколы HTTP/HTTPS, основные уязвимости (XSS, SQL-инъекции и другие), методы их эксплуатации и защиты, разрабатывать безопасные веб-приложения на Flask, создавать демонстрационные страницы для исследования атак, анализировать уязвимости баз данных, применять методы валидации ввода, подготовленных запросов и фильтрации данных, проводить аудит
		безопасности веб-приложений, использовать искусственный интеллект для анализа кода, выявления угроз и усиления защитных механизмов; разрабатывать рекомендации по защите от кибератак и внедрению современных методов аутентификации и авторизации.
4.	Дополнительная информация о ДОП	Перечень обязательных для выполнения каждым Получателем поддержки ра-бот/контрольных точек по каждому модулю Программы и по Программе в целом: в рамках текущего контроля обязательные к выполнению задания самостоятельной ра-боты (4 по каждому модулю), т.е. 16 контрольных точек являются обязательными активностя-ми; 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.
5.	Дополнительно (в соответствующих отдельных графах) может быть дана следующая информация по ДОП:	
5.1.	Стоимость обучения по ДОП	37304.00

5.2.	Рекомендации по обучению на ДОП	РЕКОМЕНДАЦИИ ДЛЯ УЧАЩИХСЯ 1. Требования к техническому оснащению: • Компьютер или ноутбук с доступом в Интернет • Установленные программы: o Python o IDE: PyCharm или Visual Studio Code • Виртуальные машины (Kali Linux, bWAPP, DVWA) • Браузер • Средства связи (MAX, Telegram и/или электронная почта) 2. Навыки, необходимые для успешного обучения: • Уверенное владение базовыми компьютерными навыками • Умение работать с браузером и файлами • Навыки самостоятельного поиска и анализа информации • Готовность к самоподготовке и командной работе • Способность презентовать собственные решения 3. Поведенческие рекомендации: • Занимайтесь регулярно: не менее 2–3 раз в неделю • Ведите дневник проекта (изученное, успехи, трудности) • Не стесняйтесь обращаться к преподавателю за разъяснениями • Ищите аналогии — это поможет лучше понять материал • Работайте в профессиональной среде разработки, используйте официальную документацию • Помните: ошибки — не провал, а путь к обучению 4. Правила: • Не пропускайте занятия: темы логически связаны • Не копируйте чужой код — важно понимание • Соблюдайте этику — курс обучает защите, а не атаке • Работайте с виртуальными машинами только в учебной среде РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ 1. Использование учебно-методического комплекса (УМК): Для реализации программы необходимо использовать утверждённый УМК, включающий: • Рабочую программу и календарно-тематическое планирование • Презентации, практические задания, тесты и кейсы по модулям • Задания для самостоятельной работы и проектов • Документационные шаблоны: чек-листы, формы отчётов, критерии оценки Преподаватель обязан строго соблюдать структуру курса и утверждённые контрольные точки. 2. Этическое сопровождение обучения: Преподавателю необходимо: • Формировать у обучающихся понимание границ этичного хакинга • Акцентировать внимание на правовой ответственности в цифровой среде • Развивать навыки цифровой гигиены и киберэтики: o Защита персональных данных o Уважительное взаимодействие в сети • Контролировать соблюдение этики в онлайн и офлайн-коммуникации 3. Требования к техническому оснащению: Для проведения занятий в очной форме с применением дистанционных образовательных технологий, в том числе с применением средств электронного обучения требуется: • Компьютер с предустановленным необходимым ПО • Стабильный доступ к ВКС • Рабочие аккаунты в LMS, мессенджерах, электронной почте • Высокоскоростной Интернет, обеспечивающий: o Загрузку

		и работу с виртуальными машинами o Проведение видеозанятий без потерь связи o Доступ к облачным сервисам и библиотекам ИИ

3. Комплекс организационно-педагогических условий реализации ДОП:
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 языка Python с применением ИИ	Основы Python	8	2	5	0	1	0
2.		Основные программные конструкции Python	8	2	5	0	1	0
3.		Модули и функции в Python	9	2	5	1	1	0
4.		Обработка исключений и работа с файлами в Python, использование ИИ в программировании	10	2	6	1	1	0
5.		Промежуточная аттестация	1	0	0	0	1	0
6.	Модуль 2 Базовые основы этичного хакинга и возможности ИИ для рутинных задач	Этичный хакинг с помощью ИИ	8	2	5	0	1	0
7.		Разведка и сбор информации с помощью ИИ	8	2	5	0	1	0
8.		Уязвимости и их анализ с применением ИИ	9	2	5	1	1	0
9.		Защита от атак и эксплуатация уязвимостей с применением ИИ	10	2	6	1	1	0
10.		Промежуточная аттестация	1	0	0	0	1	0
11.	Модуль 3 Компьютерные сети и их безопасность с использованием ИИ	Сетевые протоколы и применение ИИ для работы с ними	8	2	5	0	1	0
12.		Инструменты анализа сетевого трафика, в том числе с ИИ	8	2	5	0	1	0
13.		Обнаружение сетевых атак и защита сети с помощью ИИ	9	2	5	1	1	0
14.		Wi-Fi сети и их безопасность с использованием ИИ	10	2	6	1	1	0

15.		Промежуточная аттестация	1	0	0	0	1	0
16.	Модуль 4 Безопасность Веб-приложений с применением ИИ	Разработка веб-приложений с использованием ИИ	8	2	5	0	1	0
17.		Основы кросс-сайтового скриптинга (XSS) с применением ИИ	8	2	5	0	1	0
18.		Базы данных и их уязвимости, защита от инъекций с помощью ИИ	9	2	5	1	1	0
19.		Веб-приложения и их защита с помощью ИИ	10	2	6	1	1	0
20.		Промежуточная аттестация	1	0	0	0	1	0
Итоговый контроль/аттестация по ДОП			4.00	0	0	0	4.00	0
Итого по ДОП:			148	32	84	8	24	0
ИТиСИ			Часы ИТиСИ не входят в общую трудоемкость ДОП, но участие в ИТиСИ обязательно для всех успешно прошедших итоговый контроль/аттестацию по ДОП					

Рабочая программа с описанием каждого модуля ДОП

Элементы ДОП (модули и итоговый контроль/аттестация по 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 языка Python с применением ИИ Модуль посвящен изучению основ Python, включая синтаксис, операторы, выражения, циклы, структуры данных, функции и рекурсию, с практическим применением этих знаний для написания простых программ, работы со списками, модулями (например, math_operations.py, string_operations.py), обработки исключений, работы с файлами	Основы Python	Введение в Python: история, особенности и применение языка, установка окружения, основы синтаксиса (переменные, типы данных, операторы, условия, циклы), работа с консолью и файлами, создание функций и использование модулей, а также обработка исключений для управления ошибками.	Теоретическая подготовка	2
		Написание программы, которая запрашивает имя пользователя и приветствует его, затем предлагает ввести два числа и выводит результаты их сложения, вычитания, умножения и деления.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Основы Python".	Текущий контроль	1

и создания программ для чтения/записи данных с использованием ИИ. Цель модуля: Изучение базовых концепций и прикладных аспектов программирования на Python, включая основы синтаксиса, операторы, структуры данных, функции и модули, обработку исключений и работу с файлами, с последующим применением этих знаний для написания практических про-грамм и использования возможностей искусственного интеллекта в программировании. Планируемые результаты: Применять базовые концепции программирования на Python, включая работу с переменными, типами данных, операторами, условиями, циклами, функциями, модулями и структурами данных, для написания простых программ и скриптов; эффективно обрабатывать ошибки с помощью механизмов исключений, работать с файловой системой, создавать собственные модули и использовать возможности искусственного интеллекта для генерации и оптимизации кода, что позволит им заложить прочную основу для дальнейшего изучения более сложных аспектов программирования и этичного хакинга. Типы задач/деятельности: Программы для выполнения базовых операций (арифметических вычислений, обработки строк, работы с файлами), создание функций и модулей для решения практических задач, реализация алгоритмов с использованием условий,	Основные программные конструкции Python	Рассматриваются операторы и выражения в Python (арифметические, сравнения, логические), условные конструкции (if-else, elif, вложенные условия), циклы (while, for, break, continue), структуры данных (списки, кортежи, словари, множества) и работа с индексацией и срезами для доступа к элементам.	Теоретическая подготовка	2
		Написание программ, которые включают проверку числа на четность/нечетность, вывод чисел от 1 до 10 с пропуском числа 3 и фильтрацию слов, начинающихся на букву "а", из списка, введенного пользователем.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Основные программные конструкции Python".	Текущий контроль	1
	Модули и функции в Python	Рассматриваются определение функций в Python (синтаксис, аргументы, возвращаемые значения), локальные и глобальные переменные, работа с модулями (импорт, использование, создание собственных), рекурсия (определение и примеры) и применение встроенных функций.	Теоретическая подготовка	2
		Создание модуля math_operations.py с функциями для сложения, вычитания, умножения и деления, и использование его в программе для выполнения арифметических операций над числами, введенными пользователем.	Практические занятия	5
		Создание модуля string_operations.py с функциями для работы со строками (подсчет символов, поиск подстроки, замена) и программы, использующую этот модуль для выполнения операций над строками, введенными пользователем.	Самостоятельная работа	1
		Текущий контроль по теме "Модули и функции в Python".	Текущий контроль	1
	Обработка исключений и работа с файлами в Python, использование ИИ в программировании	Рассматриваются основы работы с файлами в Python (функция open(), режимы, методы чтения и записи), обработка исключений (try-except, finally), управление ресурсами через with, работа с путями (os.path), а также виды ИИ, GPT-модели, способы взаимодействия с ИИ и примеры его применения для генерации и объяснения кода.	Теоретическая подготовка	2
		Написание программы чтения файла data.txt и вывода его содержимого, записи пользовательской строки в файл output.txt, фильтрации строк из data.txt по ключевому слову, а также генерация кода вручную и с помощью ИИ с последующим сравнительным анализом	Практические занятия	6
		Создание программы с помощью ИИ, которая копирует содержимое одного текстового файла в другой, используя имена файлов, заданные пользователем.	Самостоятельная работа	1
		Текущий контроль по теме "Обработка исключений и работа с файлами в Python, использование ИИ в программировании".	Текущий контроль	1

циклов и структур данных (списков, словарей, множеств), разработка скриптов для обработки исключений и управления ошибками, а также выполнение задач по анализу и оптимизации кода с применением возможностей искусственного интеллекта.	Промежуточная аттестация	Тестирование 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.	Промежуточная аттестация	1
Модуль 2 Базовые основы этичного хакинга и возможности ИИ для рутинных задач Модуль знакомит с основами этичного хакинга, включая отличия от нелегальных действий, методы сбора информации, принципы атак и защиты, а также обнаружение угроз, и развивает навыки написания Python-скриптов для проверки безопасности сети, анализа доменов, проведения запросов и разработки программ для эксплуатации и защиты, в том числе с применением ИИ. Цель модуля: Знакомство с основами этичного хакинга, включая его отличия от нелегальных действий, методы сбора информации, принципы атак и защиты, а также развитие навыков написания Python-скриптов для проверки безопасности сети, анализа доменов, проведения запросов и разработки программ для эксплуатации и защиты, с применением возможностей искусственного интеллекта для автоматизации рутинных задач. Планируемые результаты: Знать различия этичного хакинга и нелегальных действий, понимать ключевые принципы и кодекс этичного хакера, классифицировать атаки и разрешенные действия, использовать Python-скрипты	Этичный хакинг с помощью ИИ	Понятие этичного хакинга, его отличие от нелегальных действий, ключевые принципы и кодекс хакера, классификация атак, разрешенные действия, а также сертификация и лицензии в данной области.	Теоретическая подготовка	2
		Разработка с помощью ИИ Python-скрипта для проверки безопасности сети, который сканирует указанный IP-адрес или диапазон, выявляет открытые порты и предоставляет рекомендации по устранению уязвимостей.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Этичный хакинг с помощью ИИ".	Текущий контроль	1
	Разведка и сбор информации с помощью ИИ	Рассматриваются методы и инструменты сбора информации (поиск в открытых источниках, специализированные программы), основы сетевого сканирования и анализа уязвимостей, а также правовые и этические аспекты разведки.	Теоретическая подготовка	2
		Создание с помощью ИИ Python-программы, которая извлекает информацию о домене (IP-адрес, WHOIS-данные, DNS-записи) с использованием библиотек socket, python-whois и dnspython для взаимодействия с сервисами.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Разведка и сбор информации с помощью ИИ".	Текущий контроль	1
	Уязвимости и их анализ с применением ИИ	Рассматриваются принципы и методы анализа уязвимостей, инструменты для их обнаружения (сканеры, анализаторы кода), оценка и классификация, а также отчетность и документирование выявленных проблем.	Теоретическая подготовка	2

использовать Python-скрипты для проверки безопасности сети, анализа доменов, проведения запросов и разработки программ для эксплуатации и защиты, а также смогут применять мето-ды сбора информации, анализировать уязвимости с помощью инструментов и сканеров, разрабатывать защитные меры против распространенных уязвимостей (буферное переполнение, инъекции кода, DoS) и создавать детальные отчеты об уязвимо-стях и рекомендациях по защите с использованием возможностей искусственного интеллекта для автоматизации рутинных задач. Типы задач/деятельности: Задачи по анализу сетевой без-опасности, включая сканирование IP-адресов и портов, выявление уязвимостей с использованием Python-скриптов и инструментов, сбор информации о доменах и DNS-записях, проведение исследований известных уязвимостей (буферное переполнение, SQL-инъекции, DoS), разработка про-грамм для эксплуатации слабых паролей, создание отчетов об угрозах и рекомендациях по за-щите, а также применение искусственного интеллекта для автоматизации анализа данных и генерации кода.		Создание с помощью ИИ Python-программы для сканирования уязвимостей сети, используя библиотеку scapy для отправки, получения и анализа сетевых пакетов с целью выявления уязвимых устройств или служб.	Практические занятия	5
		Исследование известных уязвимостей или угроз (например, Spectre, WannaCry), подготовка с помо-щью ИИ сообщения о принципе их работы, послед-ствиях и рекомендациях по защите.	Самостоятельная работа	1
		Текущий контроль по теме "Уязвимости и их анализ с применением ИИ".	Текущий контроль	1
	Защита от атак и эксплуатация уязвимостей с применением ИИ	Рассматриваются основы эксплуатации уязвимостей, инструменты и методы атак, защитные меры, техники обнаружения атак, а также разработка и внедрение политик безопасности.	Теоретическая подготовка	2
		Создание с помощью ИИ Python-скрипта для взлома слабых паролей, используя словарь для попыток авторизации в учетных записях с ненадежными паролями.	Практические занятия	6
		Исследование и анализ известных уязвимостей (буферное переполнение, инъекции кода, DoS и др.), создание с помощью ИИ детального отчета с описанием каждой уязвимости, её влияния на систему и способов защиты.	Самостоятельная работа	1
		Текущий контроль по теме "Защита от атак и эксплуатация уязвимостей с применением ИИ".	Текущий контроль	1
	Промежуточная аттестация	Тестирование 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.	Промежуточная аттестация	1
Модуль 3 Компьютерные сети и их безопасность с использованием ИИ Модуль посвящен сетевой безопасности: изучению протоколов (IP, TCP, UDP, HTTP, HTTPS), анализа трафика, методов защиты сети, систем IDS/IPS	Сетевые протоколы и применение ИИ для работы с ними	Рассматриваются основные протоколы сетевого взаимодействия (IP, TCP, UDP, HTTP, HTTPS), их функции и особенности, а также принципы маршрутизации и пересылки пакетов в сети.	Теоретическая подготовка	2
		Разработка с помощью ИИ клиент-серверного приложения на Python, реализующего обмен данными через TCP протокол.	Практические занятия	5

систем IDS/IPS, противодействия DDoS и угроз Wi-Fi. Осваиваются навыки разработки клиент-серверных приложений, сканирования сети, анализа трафика с помощью Wireshark и библиотеки pcapy, симуляции фаервола, а также программ для аудита Wi-Fi сетей на Python, использование ИИ для анализа и усиления сетевой безопасности. Цель модуля: Изучение основ сетевой безопасности, включая протоколы IP, TCP, UDP, HTTP, HTTPS, принципы анализа трафика, методы защиты сети, системы IDS/IPS, противодействие DDoS и угро-зам Wi-Fi, а также развитие навыков разработки клиентсерверных приложений, сканирования сети, анализа трафика с помощью Wireshark и библиотеки pcapy, симуляции фаервола и про-грамм для аудита Wi-Fi сетей на Python с применением ИИ для анализа и усиления сетевой безопасности. Планируемые результаты: Понимать принципы работы основных сетевых протоколов (IP, TCP, UDP, HTTP, HTTPS), анализировать сетевой трафик с помощью инструментов типа Wireshark и библиотеки pcapy, разрабатывать клиент-серверные приложения на Python, создавать программы для сканирования сети и анализа активных устройств, симулировать работу фаервола с правилами фильтрации трафика, применять методы защиты от DDoS-атак, проводить аудит безопасности Wi-Fi сетей, выявлять уязвимости в беспроводных соединениях и предлагать меры			Самостоятельная работа	0
		Текущий контроль по теме "Сетевые протоколы и применение ИИ для работы с ними".	Текущий контроль	1
	Инструменты анализа сетевого трафика, в том числе с ИИ	Рассматриваются основы анализа сетевого трафика для обеспечения безопасности, программа Wireshark, анализ протоколов на уровнях модели OSI, а также методы идентификации сетевых атак, таких как DoS и переполнение буфера.	Теоретическая подготовка	2
		Изучение инструмента Wireshark: установка, захват и анализ сетевого трафика, исследование содержимого пакетов на разных уровнях модели OSI, вклю-чая протоколы, адреса, порты и другие параметры.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Инструменты анализа сетевого трафика, в том числе с ИИ".	Текущий контроль	1
	Обнаружение сетевых атак и защита сети с помощью ИИ	Рассматриваются методы защиты сети, включая фаерволы, антивирусы, IDS и IPS, техники обнаружения атак (сигнатурный анализ, аномалии, статистика), принципы работы IDS/IPS, использование сетевых масок для фильтрации трафика и методы противодействия DDoS-атакам.	Теоретическая подготовка	2
		Создание с помощью ИИ программы на Python симуляции фаервола, которая обрабатывает сетевой трафик и применяет правила фильтрации для разрешения или блокировки пакетов.	Практические занятия	5
		Рассмотрение методов защиты от DDoS-атак и разработка с помощью ИИ плана для вымышленной компании, включающий использование специализированных устройств и программного обеспечения.	Самостоятельная работа	1
		Текущий контроль по теме "Обнаружение сетевых атак и защита сети с помощью ИИ".	Текущий контроль	1

соединениях и предлагать меры по их устранению, а также использовать возможности искусственного интеллекта для анализа сетевой безопасности, автоматизации процессов мониторинга и усиления защитных механизмов. Типы задач/деятельности: Задачи по анализу сетевого трафика с использованием инструментов типа Wireshark и библиотеки pcapy, разработка клиент-серверных приложений на Python для обмена данными через TCP/UDP протоколы, создание программ для сканирования сети и выявления активных устройств, симуляция работы фаервола с правилами фильтрации трафика, исследование методов защиты от DDoS-атак, проведение аудита безопасности Wi-Fi сетей, анализ уязвимостей в беспроводных соединениях и разработка рекомендаций по их устранению с применением искусственного интеллекта для автоматизации анализа и усиления сетевой безопасности.	Wi-Fi сети и их безопасность с использованием ИИ	Рассматриваются угрозы безопасности Wi-Fi (перехват трафика, подмена точек доступа, атаки на протоколы), методы защиты (безопасные протоколы, настройка устройств, VPN), виды шифрования (WEP, WPA, WPA2, WPA3) и проведение аудита для выявления уязвимостей.	Теоретическая подготовка	2
		Создание с помощью ИИ программы на Python, которая сканирует Wi-Fi сети, выводит данные об уровне сигнала, типе шифрования и защите, а также реализация скрипта для аудита безопасности, проверяющего шифрование, выявляющего уязвимости и дающего рекомендации по их устранению.	Практические занятия	6
		Проведение исследования безопасности домашней Wi-Fi сети, выявление уязвимостей и предложение мер для их устранения, а затем составление с помощью ИИ отчета, детально описывающего найденные проблемы и рекомендации по улучшению защиты.	Самостоятельная работа	1
		Текущий контроль по теме "Wi-Fi сети и их безопасность с использованием ИИ".	Текущий контроль	1
	Промежуточная аттестация	Тестирование 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.	Промежуточная аттестация	1
Модуль 4 Безопасность Веб-приложений с применением ИИ Модуль посвящен изучению компонентов веб-приложений, протоколов HTTP/HTTPS, уязвимостей (XSS, инъекции баз данных) и методов защиты, а также освоению практических навыков: разработки веб-приложений на Flask, создания страниц с уязвимостями для исследования атак и проведения аудита безопасности с применением ИИ. Цель модуля: Изучение основных компонентов и уязвимостей веб-приложений, включая протоколы HTTP/HTTPS, архитектуры	Разработка веб-приложений с использованием ИИ	Рассматриваются основные компоненты веб-приложений (HTML, CSS, JavaScript) для клиента и для сервера, протоколы HTTP/HTTPS, архитектура клиент-сервер, а также ключевые уязвимости, такие как недостаточная валидация ввода, обработка ошибок и уязвимости баз данных.	Теоретическая подготовка	2
		Разработка простого веб-приложения на фреймворке Flask с формой для ввода данных пользователем и выводом этих данных на странице.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Разработка веб-приложений с использованием ИИ".	Текущий контроль	1

клиент-сервер, типов атак (XSS, SQL-инъекции и другие), методов защиты (валидация ввода, подготовленные запросы, фильтрация данных), а также развитие навыков разработки безопасных веб-приложений на Flask, создания демонстрационных страниц для исследования атак и проведения аудита безопасности с использованием возможностей искусственного интеллекта для анализа и усиления защиты веб-систем. Планируемые результаты: Понимать архитектуру веб-приложений, протоколы HTTP/HTTPS, основные уязвимости (XSS, SQL-инъекции и другие), методы их эксплуатации и защиты, разрабатывать безопасные веб-приложения на Flask, создавать демонстрационные страницы для исследования атак, анализировать уязвимости баз данных, применять методы валидации ввода, подготовленных запросов и фильтрации данных, проводить аудит безопасности веб-приложений, использовать искусственный интеллект для анализа кода, выявления угроз и усиления защитных механизмов, а также разрабатывать рекомендации по защите от кибератак и внедрению современных методов аутентификации и авторизации. Типы задач/деятельности: Разработка веб-приложений на Flask с реализацией форм для ввода данных и вывода результатов, создание страниц с уязвимостями (XSS, SQL-инъекции) для	Основы кросс-сайтового скриптинга (XSS) с применением ИИ	Рассматриваются основы кросс-сайтового скриптинга (XSS), включая его принципы работы, типы атак (stored, reflected, DOM-based), уязвимые места веб-приложений, возможные последствия и методы защиты от XSS.	Теоретическая подготовка	2
		Разработка веб-страницы с уязвимостью к XSS-атакам на Flask, демонстрация внедрения вредоносного скрипта через форму ввода данных и выбор методов защиты от таких атак.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Основы кросс-сайтового скриптинга (XSS) с применением ИИ".	Текущий контроль	1
	Базы данных и их уязвимости, защита от инъекций с помощью ИИ	Изучение инъекций и уязвимостей баз данных, включая SQL, командные и NoSQL-инъекции, их последствия, а также методы защиты с использованием подготовленных запросов, фильтрации ввода и ограничения привилегий.	Теоретическая подготовка	2
		Разработка веб-страницы с формой для ввода данных, которые используются для выполнения SQL-запросов к базе данных, с применением Python и ИИ для обработки данных и получения результатов.	Практические занятия	5
		Исследование типов инъекций (SQL, командные, NoSQL) и разработка с помощью ИИ демонстрационных приложений для их иллюстрации, анализа способов эксплуатации уязвимостей и методов их предотвращения.	Самостоятельная работа	1
		Текущий контроль по теме "Базы данных и их уязвимости, защита от инъекций с помощью ИИ".	Текущий контроль	1
	Веб-приложения и их защита с помощью ИИ	Основы защиты веб-приложений, включая анализ угроз (XSS, инъекции, перехват данных и др.) и методы защиты: валидация ввода, безопасные архитектурные подходы, контроль доступа, шифрование, управление сеансами и мониторинг событий.	Теоретическая подготовка	2
		Разработка веб-приложения на Flask, проведение аудита безопасности с помощью ИИ для выявления уязвимостей и реализации мер защиты, включая валидацию ввода и контроль доступа.	Практические занятия	6

исследования атак и методов защиты, анализ типов XSS-атак (stored, reflected, DOM-based) и разработка демонстрационных примеров для их иллюстрации, исследование различных видов инъекций (SQL, командные, NoSQL) с созданием программ для их выявления и предотвращения, проведение аудита безопасности веб-приложений с использованием ИИ для анализа угроз и внедрения защитных мер, таких как валидация ввода, подготовленные запросы и многофакторная аутентификация.		Исследование методов аутентификации и авторизации веб-приложений, включая многофакторную аутентификацию, токены доступа и JWT, с использованием ИИ для анализа их особенностей.	Самостоятельная работа	1
		Текущий контроль по теме "Веб-приложения и их защита с помощью ИИ".	Текущий контроль	1
	Промежуточная аттестация	Тестирование 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.	Промежуточная аттестация	1
Итоговый контроль/аттестация	Итоговый контроль/аттестация по ДОП	Представление итогового проекта 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)	Итоговый контроль/аттестация	4.00

		Объем в ак.ч.	**Объем в %**
ИТОГО ПО ПРОГРАММЕ:	Теоретическая подготовка	32,00	21,62
	Практическая работа	84,00	56,76
	Самостоятельная работа	8,00	5,41
	Текущий контроль	16,00	10,81
	Промежуточная аттестация	4,00	2,70
	Итоговый контроль/аттестация	4.00	2,70
	Всего:	**148**	

ИТиСИ	Часы ИТиСИ не входят в общую трудоемкость ДОП, но участие в ИТиСИ обязательно для всех успешно прошедших итоговый контроль/аттестацию по ДОП

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: инструменты защиты на Python и ИИ	1	2025-09-22	1	2025-09-22	69	2026-05-29
				2	2025-12-01	64	
				3	2026-02-03	56	
				4	2026-03-30	61	

Сведения об условиях реализации ДОП (в том числе материально-техническое, информационное, кадровое обеспечение)

Материально-технические и информационные условия реализации ДОП

Наименование поля	Значение полей	Значение полей	Значение полей	Значение полей
Порядковый номер модуля	1	2	3	4
Перечень требований к оснащению площадки (для офлайн-формата)	«Не заполняется»	«Не заполняется»	«Не заполняется»	«Не заполняется»
Наименование требуемого оборудования (для онлайн-формата)	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 (для онлайн-формата)	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).

Информационные условия реализации ДОП (заполняется по каждому модулю):

Наименование поля	Значение полей	Значение полей	Значение полей	Значение полей
Порядковый номер модуля	1	2	3	4

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 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: 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. 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. - 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.	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 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.	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 кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/articles/276477/ (дата обращения: 05.07.2025) - Текст: электронный.

Наименование поля	Значение полей	Значение полей	Значение полей	Значение полей
Порядковый номер модуля	1	2	3	4

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 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.	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.

Кадровое обеспечение

Сведения о работниках, привлекаемых к реализации и разработке ДОП

ФИО	Роль	Наименование основного места работы	Должность	Ученая степень	Ученое звание	Ссылка на веб-страницы с портфолио	Образование. Наименование учебного заведения	Образование. Год окончания учебного заведения	Образование. Полученная специальность	Стаж работы в данной (аналогичной) должности	Основание для привлечения к реализации ДОП (трудовой договор, договор ГПХ, иное)	Информация о курсах повышения квалификации по профилю преподаваемой дисциплины (за последние 3 года)	Опыт работы в сфере ИТ (в области программирования, робототехники, искусственного интеллекта)	Отметка о полученном согласии на обработку персональных данных
строка	строка	строка	строка	строка	строка	каждая ссылка с новой строки	строка	числовое значение	строка	числовое значение	строка	строка	строка	строка
Сойманова Светлана Викторовна	Разработчик	РУКОН Цель	Методист			https://цель-обучение.рф/experts/soymanova	Пермский государственный университет	2002	Географ. Преподаватель. по специальности "География"	10	Трудовой договор	Вопросы применения средств криптографической защиты информации (СКЗИ), 72 час., Автономная некоммерческая организация дополнительного профессионального образования «Центр профессионального развития ПРОФИ», 2024 г.		Да

Зигуля Андрей Сергеевич	Разработчик	ООО «Дилибриум»	Генеральный директор ООО «Дилибриум»			https://цель-обучение.рф/experts/zigulya	Сумской техникум пищевой промышленности	2002	Специальность "Обслуживание компьютерных и интеллектуальных систем и сетей"	10	Договор ГПХ	Проектно-образовательный интенсив «Архипелаг 2024»	Опыт работы: 21 год. Работа в составе экспертной группы проекта «Масштабирование на региональном уровне модели кадрового обеспечения внедрения передовых производственных технологий» Агентство по развитию человеческого капитала в Северо-Западном федеральном округе и Фонда инфраструктурных и образовательных программ (группа РОСНАНО), сотрудничество в области инновационного развития с ОАО «РЖД», направленного на внедрение высокотехнологичных инновационных решений предусматривающих использование технологий, процессов или продуктов, ранее не применявшихся ОАО «РЖД», Aquamatica – роботизированные аквафермы (действующий резидент Сколково), участие в круглых столах Государственной Думы РФ посвященных информационной безопасности. Выступление в Государственной Думе РФ с докладом «Манипуляция общественным сознанием посредством интернет технологий». Финалист конкурса Архипелаг 20.35. Автор учебных курсов «Цифровая трансформация бизнеса» совместно с Санкт-Петербургским Государственным Университетом,	Да

													образовательная платформа Coursera, «Цифровая трансформация в государственном управлении» совместно с Российской Академией Народного Хозяйства и Государственной Службы при Президенте РФ.	
Почаевец Андрей Андреевич	Преподаватель	РУКОН Цель	Программный директор АНО ДПО МЦК "Цель", преподаватель линейки программ 1С. Эксперт в области программирования в 1С и управления командой разработчиков.			https://цель-обучение.рф/experts/pochaevets	Государственное образовательное учреждение высшего профессионального образования "Архангельский государственный технический университет"	2007	Инженер по специальности "Информационные системы и технологии"	4	Трудовой договор		Опыт работы в сфере IT более 15 лет. Участие в проектах цифровизации бизнес-процессов и внедрения ERP-решений в компаниях различных отраслей. Опыт автоматизации от продаж и маркетинга до комплексных систем управления предприятиями. Основное направление деятельности – внедрение и адаптация 1С для решения задач управленческого учета, бюджетирования и контроля проектов. Опыт внедрения таких решений как 1С:ERP, 1С:Комплексная автоматизация, 1С:CRM и настройка их интеграцию с другими бизнес-системами. Успешная практика реализации проектов в строительной сфере, тяжелом машиностроении, производстве, энергетике и гостиничном бизнесе. Участие в разработке и проведении обучающих программ по работе с 1С. Подготовка более 2000 аналитиков и программистов. А также опыт работы в международных проектах и работе с крупными промышленными предприятиями, где требуется комплексный подход к цифровой трансформации.	Да

Волков Александр Георгиевич	Преподаватель, Разработчик	Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»	Директор Института развития квалификаций	Кандидат технических наук	Доцент	https://цель-обучение.рф/experts/volkov	Мордовский ордена Дружбы народов госуниверситет им. Н.П. Огарева	1983	Промышленная электроника	21	Трудовой договор			Да
Рыбалёва Ирина Александровна	Разработчик	РУКОН Цель	Руководитель образовательного процесса	Кандидат педагогических наук		https://цель-обучение.рф/experts/rybaleva	Комсомольский-на-Амуре государственный педагогический институт (учитель русского языка и литературы	1994	Учитель русского языка и литературы	15	Договор об оказании услуг с индивидуальным предпринимателем	Развитие инфраструктуры авиационных систем на современном этапе, 72 час., АНО ДПО "МЦК "Цель", 2024 г.		Да
Пантелеев Сергей Владимирович	Преподаватель, Разработчик	Филиал НИТУ МИСиС г. Выкса	Доцент кафедры БД	Кандидат технических наук	Доцент	https://цель-обучение.рф/futurecode/panteleev	Владимирский государственный университет	1999	Инженер по специальности "Проектирование и технология радиоэлектронных средств"	26	Договор об оказании услуг с самозанятым лицом	Интенсив от университета Зерокодинга: AI-ассистент, интегрированный в Telegram, 2025 г.	Преподавание IT-дисциплин (Муромский институт ВлГУ, Выксунский металлургический техникум, Выксунский филиал НИТУ МИСиС) Программирование, системное администрирование с 2012 года (АО "Выксаэнерго", Нижновэнерго). Разработка сайтов с 2005 года (ООО "Виртуальная Выкса", самозанятость) к.т.н по искусственному интеллекту, специальность 05.13.01 "Системный анализ, управление и обработка информации", тема диссертации "Разработка, исследование и применение нейросетевых алгоритмов идентификации и управления динамическими системами". Преподаватель курсов «Технология программирования» (на Python), «Вычислительные машины, системы и сети», «Протоколы сетей», «Интернет-технологии» (HTML, CSS, PHP, Python, JavaScript, Jquery, MySQL, CMS).	Да

Кротов Александр Викторович	Разработчик	Код Грин Инжиниринг	Генеральный директор			https://цель-обучение.рф/experts/krotov	ФГБОУ ВПО "Санкт-Петербургский государственный электротехнический университет"ЛЭТИ" им. В.И. Ульянова (Ленина), 2012	2012	Инженер по специальности "Электронные приборы и устройства"	9	Договор ГПХ		Опыт работы в сфере IT - 8 лет. Компании: ЦНИИ РТК, ООО "НИЦ Радиотехники", Код Грин Инжиниринг.	Да

Формы аттестации и оценочные материалы (комплект контрольно-измерительных материалов, позволяющих определить достижение Получателями поддержки планируемых результатов)

Наименование поля	Значение полей
Текущий контроль	
Модуль 1, Основы языка Python с применением ИИ, Основы Python	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какие преимущества не относятся к языку программирования Python по сравнению с другими? 2. Кто создал язык программирования Python? 3. В каком году был создан язык программирования Python? 4. В честь чего был назван язык программирования Python? 5. Какие из этих операторов Python НЕ относятся к математическим? 6. С помощью какой функции осуществляется ввод данных в Python? 7. Что не включает в себя синтаксис языка программирования Python? 8. Что нельзя отнести к синтаксическим конструкциям языка программирования Python? 9. Что нельзя отнести к типам данных языка программирования Python? 10. Как называются числа с плавающей точкой языка программирования Python? 11. Как обозначается тип данных для хранения упорядоченной коллекции элементов? 12. Как называются специальные символы или ключевые слова, которые выполняют различные действия над данными и значениями? 13. Как называется совокупность правил, определяющих структуру кода на языке программирования Python и его внешний вид? 14. Что появится на экране в результате выполнения данного кода? 15. Какой оператор Python обозначает «остаток от деления»?
Модуль 1, Основы языка Python с применением ИИ, Основные программные конструкции Python	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.

Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какой оператор используется для возведения числа в степень в Python? 2. Что будет результатом выражения «5 == 5 and 3 > 2»? 3. Какой из следующих операторов проверяет, что два значения не равны? 4. Какой из вариантов правильно проверяет, является ли число x четным? 5. Что делает оператор elif в условной конструкции? 6. Какой из следующих фрагментов кода выведет числа от 1 до 10 с пропуском числа 3? 7. Что делает оператор break в цикле? 8. Какой из следующих фрагментов кода подсчитывает сумму элементов списка numbers? 9. Как получить доступ к третьему элементу списка `my_list`? 10. Что будет результатом выполнения my_list[1:3], если my_list = [10, 20, 30, 40]? 11. Какой из следующих типов данных является изменяемым? 12. Как создать пустой словарь в Python? 13. Как добавить элемент в конец списка my_list? 14. Как удалить элемент из множества my_set? 15. Какой из следующих фрагментов кода выводит слова, начинающиеся на букву "o", из списка words?
Модуль 1, Основы языка Python с применением ИИ, Модули и функции в Python	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какой синтаксис используется для определения функции в Python? 2. Что такое параметры функции в Python? 3. Какой оператор используется для возврата значения из функции? 4. Что произойдет, если функция не содержит оператора return? 5. Какие переменные называются локальными? 6. Каким ключевым словом можно изменить глобальную переменную внутри функции? 7. Как импортировать модуль math_operations.py в программу? 8. Как вызвать функцию add из модуля math_operations? 9. Что делает следующий код: «import string_operations as so»? 10. Что такое рекурсия в Python? 11. Какой из следующих примеров является рекурсивной функцией? 12. Какая встроенная функция используется для получения длины строки или списка? 13. Какая встроенная функция используется для преобразования строки в целое число? 14. Как создать пользовательский модуль в Python? 15. Как организовать программу, которая использует модуль math_operations для сложения двух чисел?
Модуль 1, Основы языка Python с применением ИИ, Обработка исключений и работа с файлами в Python, использование ИИ в программировании	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.

Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какой режим открытия файла в Python позволяет только читать данные, но не изменять их? 2. Что произойдет, если попытаться открыть несуществующий файл в режиме 'r'? 3. Какой блок используется для перехвата исключений в Python? 4. Какой метод используется для закрытия файла после работы с ним? 5. Какую конструкцию лучше использовать для автоматического управления ресурсами файла? 6. Какая библиотека в Python помогает работать с путями к файлам? 7. Что делает следующий код: «with open('file.txt', 'r') as file: print(file.read())»? 8. Какой режим открытия файла позволяет дописывать данные в конец файла? 9. Какой тип ИИ чаще всего используется для генерации кода? 10. Что такое GPT? 11. Какая функция поможет проверить существование файла? 12. Что делает следующий код: «open('output.txt', 'w').write('Hello')»? 13. Как правильно обработать несколько типов исключений? 14. Какой метод считывает одну строку из файла? 15. Какой параметр функции open() устанавливает кодировку?
Модуль 2, Базовые основы этичного хакинга и возможности ИИ для рутинных задач, Этичный хакинг с помощью ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какая из сертификаций этичного хакинга самая сложная для управления безопасностью? 2. Что такое этичный хакинг? 3. Какой принцип является ключевым в этичном хакинге? 4. Какая из перечисленных сертификаций фокусируется на практическом тестировании проникновения? 5. Какой тип атаки направлен на человека? 6. Какой порт обычно используется для HTTP-трафика? 7. Какие действия считаются разрешенными в рамках этичного хакинга? 8. Какой сертификат требует сдачи сложного экзамена с практической частью, имитирующей реальные условия? 9. Какой метод используется для выявления открытых портов в сети? 10. Какой стандарт шифрования используется для защиты HTTPS-соединений? 11. Какой сертификат подходит для специалистов, занимающихся управлением информационной безопасностью? 12. Какой принцип ИИ может быть использован для анализа сетевого трафика? 13. Какой сертификат требует как минимум 5 лет опыта работы в области информационной безопасности? 14. Какой сертификат требует сдачи экзамена, включающего защиту лабораторной сети в реальном времени? 15. Какую шляпу носит этичный хакер?
Модуль 2, Базовые основы этичного хакинга и возможности ИИ для рутинных задач, Разведка и сбор информации с помощью ИИ	
Количество академических часов	1

Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Как называется запрос в Google Dorks для определения типа файла? 2. Какой метод используется для получения IP-адреса домена в Python с использованием библиотеки socket? 3. Что из перечисленного НЕ является этическим аспектом при проведении разведки? 4. Какая библиотека Python используется для получения WHOIS-информации? 5. При использовании расширенных операторов Google, что означает оператор site:? 6. Какой метод помогает оценить релевантность найденной информации? 7. Какая команда используется для базового сетевого сканирования в Nmap? 8. Какой элемент обычно включается в WHOIS-данные? 9. Какая библиотека Python используется для работы с DNS-записями? 10. Что является важным аспектом при составлении отчета о собранной информации? 11. Как называется процесс систематического исследования сети на предмет уязвимостей? 12. Какой метод помогает проверить достоверность WHOIS-информации? 13. Что из перечисленного является типом DNS-записи? 14. Какой принцип является основополагающим при проведении легальной разведки? 15. Что является важным при анализе результатов разведки?
Модуль 2, Базовые основы этичного хакинга и возможности ИИ для рутинных задач, Уязвимости и их анализ с применением ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какой метод анализа уязвимостей предполагает изучение исходного кода программы без её запуска? 2. Какая библиотека в Python часто используется для работы с сетевыми пакетами при анализе уязвимостей? 3. Что такое CVE в контексте анализа уязвимостей? 4. Какой компонент системы целесообразно проверять с помощью динамического анализа? 5. Какие данные наиболее важны при составлении отчета об уязвимости? 6. Какой протокол можно анализировать с помощью scapy для выявления уязвимых служб? 7. Что является основной целью сканирования сети на уязвимости? 8. Какую задачу решает анализ сетевых пакетов с помощью scapy? 9. Какой формат часто используется для автоматизированного описания уязвимостей? 10. Какое действие следует выполнить после обнаружения критической уязвимости? 11. Какой элемент анализа уязвимостей можно автоматизировать с помощью ИИ? 12. Какой инструмент используется для динамического анализа приложений? 13. Какой метод анализа уязвимостей предполагает имитацию атак для оценки устойчивости системы? 14. Какой параметр функции sniff в Scapy указывает на сетевой интерфейс, который нужно анализировать? 15. Какая команда используется для просмотра списка доступных сетевых интерфейсов в Unix-системах?
Модуль 2, Базовые основы этичного хакинга и возможности ИИ для рутинных задач, Защита от атак и эксплуатация уязвимостей с применением ИИ	

Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что такое эксплуатация уязвимостей? 2. Какой инструмент используется для сканирования сетей и выявления уязвимых хостов и служб? 3. Что такое буферное переполнение? 4. Что такое SQL-инъекция? 5. Какой тип уязвимости позволяет злоумышленнику внедрять вредоносные скрипты на веб-странице? 6. Какой инструмент специализируется на обнаружении и эксплуатации уязвимостей, связанных с SQL-инъекциями? 7. Что является важным аспектом при использовании инструментов для тестирования на проникновение? 8. Какая система не только обнаруживает атаки, но и принимает меры по их блокировке? 9. Какой метод реагирования на подозрительную активность предполагает немедленное прекращение атак? 10. Какое ключевое слово используется в Python для работы с сокетами? 11. Какой метод защиты предполагает изучение обычных шаблонов поведения систем и пользователей? 12. Какой тип уязвимости связан с перегрузкой ресурсов системы или сети? 13. Какой из перечисленных принципов относится к этапу после успешной атаки? 14. Какой инструмент используется для автоматизированного тестирования на проникновение с использованием множества модулей? 15. Как называется основная общедоступная база данных известных уязвимостей?
Модуль 3, Компьютерные сети и их безопасность с использованием ИИ, Сетевые протоколы и применение ИИ для работы с ними	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.

	1. Что означает аббревиатура TCP? 2. Какой протокол является менее надежным, но более быстрым по сравнению с TCP? 3. Какой порт обычно использует HTTPS протокол? 4. Что такое IP-адрес? 5. Какой метод используется для проверки занятости порта в Python? 6. Что происходит при переполнении буфера в сетевом соединении? 7. Какой метод в Python socket используется для прослушивания входящих соединений? 8. Что из следующего является функцией DNS? 9. Какой метод используется для отправки данных через сокет в Python? 10. Что такое ICMP? 11. Как называется компактная нотация записи IP-адресов? 12. Какой метод в Python socket используется для принятия входящего соединения? 13. Что такое маршрутизация в сетях? 14. Какой порт обычно использует HTTP протокол? 15. Что такое таблицы маршрутизации?
Модуль 3, Компьютерные сети и их безопасность с использованием ИИ, Инструменты анализа сетевого трафика, в том числе с ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Как называется инструмент для анализа сетевого трафика с графическим интерфейсом? 2. Какая библиотека в Python используется для захвата сетевого трафика? 3. Какой уровень модели OSI отвечает за MAC-адреса? 4. Какой протокол используется для получения IP-адреса по MAC-адресу? 5. Какой фильтр в Wireshark показывает только HTTP-трафик? 6. Какой командой в Linux устанавливается Wireshark? 7. Какой метод в scapy используется для захвата пакетов? 8. Что показывает команда "Follow TCP Stream" в Wireshark? 9. Какой протокол обеспечивает надежную передачу данных? 10. В каком формате сохраняются файлы захвата в Wireshark? 11. Какой флаг TCP указывает на начало соединения? 12. Какой уровень модели OSI отвечает за маршрутизацию? 13. Какой параметр IP-пакета указывает на время жизни пакета? 14. Какой протокол используется для разрешения доменных имен? 15. Какой командой в scapy отправляется пакет?
Модуль 3, Компьютерные сети и их безопасность с использованием ИИ, Обнаружение сетевых атак и защита сети с помощью ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.

Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что такое фаервол в контексте сетевой безопасности? 2. Какой метод обнаружения атак анализирует отклонения от нормального сетевого поведения? 3. Какую функцию выполняют сетевые маски в правилах фильтрации? 4. Что такое DDoS-атака? 5. Что делает метод add_allowed_port в классе Firewall? 6. Какая система может не только обнаруживать, но и активно предотвращать атаки? 7. Какой метод защиты от DDoS-атак помогает распределить нагрузку между серверами? 8. Что такое сигнатурный анализ? 9. Что делает метод block_ip в классе Firewall? 10. Какой метод используется для временного хранения ресурсов и снижения нагрузки на серверы? 11. Что такое генерация сетевого трафика в симуляции фаервола? 12. Какой порт обычно используется для SSH-подключений? 13. Какой метод обнаружения атак использует статистические модели? 14. Для чего используется метод print_rules в классе Firewall? 15. Какой диапазон портов обычно используется для пользовательских приложений?
Модуль 3, Компьютерные сети и их безопасность с использованием ИИ, Wi-Fi сети и их безопасность с использованием ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какой протокол обеспечивает самый высокий уровень безопасности Wi-Fi сети? 2. Какой метод защиты рекомендуется использовать для предотвращения несанкционированного доступа к Wi-Fi сети? 3. Что рекомендуется делать при подключении к общественной Wi-Fi сети? 4. Какая угроза возникает при использовании устаревшего протокола WEP? 5. Какой аббревиатурой называют «имя сети»? 6. Какой командой можно получить имя текущей Wi-Fi сети в Windows? 7. Что рекомендуется делать с паролями Wi-Fi сети? 8. Какой метод защиты Wi-Fi сети считается наиболее надежным? 9. Какой метод рекомендуется использовать для проверки безопасности домашней Wi-Fi сети? 10. Какое действие помогает защитить данные при использовании общественного Wi-Fi? 11. Какой метод защиты помогает изолировать гостей от основной сети? 12. Какой метод защиты рекомендуется использовать для предотвращения перехвата трафика? 13. Какой командой можно выключить Wi-Fi адаптер в Linux? 14. Какой метод защиты помогает предотвратить несанкционированный доступ к административному интерфейсу роутера? 15. Какой метод рекомендуется использовать для мониторинга подключенных устройств?
Модуль 4, Безопасность Веб-приложений с применением ИИ, Разработка веб-приложений с использованием ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.

Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что такое Flask в контексте разработки веб-приложений? 2. Какой метод HTTP-запроса используется для отправки данных на сервер? 3. Какой протокол обеспечивает безопасную передачу данных между клиентом и сервером? 4. Что такое SQL-инъекция? 5. Какая уязвимость позволяет атакующему внедрять вредоносные скрипты на веб-страницы? 6. Что такое санитизация данных? 7. Как называется архитектура, при которой клиент и сервер выполняют разные роли? 8. Какая функция Flask используется для рендеринга HTML-шаблонов? 9. Где хранятся HTML-шаблоны в типичном Flask-приложении? 10. Какой метод используется для обработки ошибок в веб-приложениях? 11. Какой язык используется для стилизации HTML-элементов? 12. Что такое маршрутизация в Flask? 13. Какой метод HTTP используется для получения данных с сервера? 14. Какой метод используется для перенаправления пользователя на другую страницу в Flask? 15. Какой компонент веб-приложения отвечает за структуру страницы?
Модуль 4, Безопасность Веб-приложений с применением ИИ, Основы кросс-сайтового скриптинга (XSS) с применением ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что означает аббревиатура XSS? 2. Какой тип XSS-атаки сохраняет вредоносный код на сервере? 3. Какой метод защиты помогает предотвратить выполнение вредоносного кода? 4. Какой HTTP заголовок помогает защититься от XSS-атак? 5. Где может быть внедрен вредоносный код при DOM-based XSS? 6. Какая функция Python помогает защититься от XSS? 7. Что является основной целью XSS-атаки? 8. Какой элемент чаще всего используется для внедрения XSS? 9. Как называется процесс удаления потенциально опасных символов из пользовательского ввода? 10. Какой инструмент можно использовать для тестирования на XSS-уязвимости? 11. Какой тип XSS-атаки передается через URL-параметры? 12. Какой метод защиты рекомендуется применять к пользовательскому вводу? 13. Как часто рекомендуется проводить проверку безопасности веб-приложений? 14. Что может быть последствием успешной XSS-атаки? 15. Что такое Content Security Policy (CSP)?
Модуль 4, Безопасность Веб-приложений с применением ИИ, Базы данных и их уязвимости, защита от инъекций с помощью ИИ	
Количество академических часов	1

Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что такое SQL-инъекция? 2. Какой метод является наиболее эффективным для предотвращения SQL-инъекций? 3. Что такое NoSQL-инъекция? 4. Что такое командная инъекция? 5. Какой из следующих методов НЕ используется для предотвращения инъекций? 6. Что такое слепая SQL-инъекция? 7. Какой инструмент рекомендуется использовать для работы с базами данных в Python? 8. Какой метод используется для создания таблицы в SQLAlchemy? 9. Что такое подготовленные выражения (prepared statements)? 10. Какой метод используется для добавления нового пользователя в базу данных в SQLAlchemy? 11. Какой метод используется для фильтрации входных данных в Flask? 12. Что такое ORM? 13. Какой метод используется для сохранения изменений в базе данных в SQLAlchemy? 14. Какой метод используется для получения всех пользователей из базы данных в SQLAlchemy? 15. Что такое параметризованные запросы?
Модуль 4, Безопасность Веб-приложений с применением ИИ, Веб-приложения и их защита с помощью ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что является одной из самых ценных целей для киберпреступников в контексте веб-приложений? 2. Какая уязвимость позволяет злоумышленникам внедрять и выполнять вредоносный код на стороне клиента? 3. Что является основным методом защиты от SQL-инъекций? 4. Какой архитектурный шаблон рекомендуется использовать для безопасной разработки веб-приложений? 5. Какой протокол обеспечивает защиту данных при передаче между клиентом и сервером? 6. Как называется процесс проверки входных данных на соответствие определенным форматам? 7. Какой принцип контроля доступа предполагает предоставление минимально необходимых прав? 8. Какой метод аутентификации считается наиболее безопасным? 9. Как часто рекомендуется проводить обновление компонентов веб-приложения? 10. Какой инструмент используется для создания форм в Flask? 11. Какой тип атаки позволяет выполнить действия от имени аутентифицированного пользователя? 12. Что является важным аспектом управления сессиями? 13. Какой метод помогает предотвратить XSS-атаки? 14. Какие данные рекомендуется хранить в зашифрованном виде? 15. Что является важным аспектом тестирования безопасности веб-приложений?
Промежуточная аттестация (по модулям)	

Основы языка Python с применением ИИ, Модуль 1	
Количество академических часов	1
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.
Варианты заданий (представлены в качестве приложения к ДОП)	1. Что означает алгоритм? 2. Что такое переменная? 3. Что такое функция? 4. Что такое оператор? 5. Что такое компиляция? 6. Какая управляющая конструкция используется для выполнения определенного блока кода многократно до тех пор, пока условие истинно? 7. Какая управляющая конструкция используется для выполнения определенного блока кода, если условие истинно, и альтернативного блока кода, если условие ложно? 8. Какая управляющая конструкция используется для перебора элементов в последовательности, такой как список или строка? 9. Необходимо создать программу, которая будет хранить уникальные элементы (например, идентификаторы пользователей). Какую структуру данных следует использовать для решения этой задачи? 10. Какая структура данных используется для хранения пар ключ-значение? 11. Какая структура данных представляет собой неизменяемую последовательность элементов? 12. Как объявить функцию в Python? 13. Как передать аргументы в функцию в Python? 14. Что такое возвращаемое значение функции? 15. Как вызвать функцию в Python? 16. Функция для чтения всего содержимого файла в строку. 17. Ключевое слово для создания анонимной функции. 18. Что выведется на экран в результате работы данной программы? a = 5 b = 7 print(a+b*a) 19. С помощью какого ключевого слово можно объявить функцию в Python? 20. Что выведется на экран в результате работы данной программы? def add(a, b): return a + b result = add(2, 3) print(result)
Шкала оценивания, нижнее значение	0
Шкала оценивания, верхнее значение	20
Шкала оценивания, минимальный проходной балл	10
Базовые основы этичного хакинга и возможности ИИ для рутинных задач, Модуль 2	
Количество академических часов	1
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.
Варианты заданий (представлены в качестве приложения к ДОП)	1. Что отличает этичного хакера от злоумышленника? 2. Какой документ регламентирует легальность действий этичного хакера? 3. Какой принцип НЕ входит в кодекс хакера? 4. Какая сертификация НЕ относится к этичному хакингу? 5. Какая библиотека Python используется для сетевого сканирования? 6. Какой метод помогает выявлять открытые порты? 7. Как называется сетевой протокол прикладного уровня, который позволяет получить регистрационные данные о владельцах доменных имён? 8. Какой оператор Google помогает искать данные только на определённом сайте? 9. Какой инструмент НЕ используется для анализа уязвимостей? 10. Назовите ключевые принципы этичного хакинга. 11. Составьте поисковый запрос в Google для нахождения PDF-отчётов об уязвимости Spectre 12. Какой закон РФ регулирует вопросы кибербезопасности? 13. Какая атака использует подделку DNS-записей? 14. Какой тип атаки НЕ относится к web-уязвимостям? 15. Какой инструмент используется для анализа сетевого трафика? 16. Какой метод НЕ является защитой от DDoS-атак? 17. Какой тип шифрования используется в HTTPS? 18. Самый мошный хакерский инструмент для поиска и эксплуатации язвимостей? 19. Каков будет результат работы этого скрипта на Python? import requests url = "https://example.com" response = requests.get(url) print(f"Status code: {response.status_code}") 20. Чем известен вирус WannaCry?
Шкала оценивания, нижнее значение	0
Шкала оценивания, верхнее значение	20
Шкала оценивания, минимальный проходной балл	10
Компьютерные сети и их безопасность с использованием ИИ, Модуль 3	
Количество академических часов	1
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.

Варианты заданий (представлены в качестве приложения к ДОП)	1. Какой метод используется для отправки данных через сокет? 2. Какой протокол используется по умолчанию в сокетах? 3. Какой инструмент используется для захвата сетевого трафика? 4. Какой протокол используется для разрешения IP-адресов в MAC-адреса? 5. Какой протокол обеспечивает надежную передачу данных? 6. Какой уровень модели OSI отвечает за маршрутизацию пакетов? 7. Какой метод используется для закрытия сокета? 8. Что такое «бэклог» в методе listen()? 9. Какая библиотека Python используется для работы с сокетами? 10. Какой протокол используется для отправки ICMP-запросов (ping)? 11. Какой тип атаки может быть реализован через переполнение буфера? 12. Какой тип данных обычно используется для передачи данных через сокет? 13. Какой фильтр используется в Wireshark для отображения только HTTP-трафика? 14. Что такое "адресное семейство" в сокетах? 15. Что выполняет IDS-система? 16. Какой уровень модели OSI отвечает за маршрутизацию? 17. Какой порт обычно используется для тестирования клиент-серверных приложений? 18. Для чего используют сетевые маски? 19. Какой метод класса socket используется для прослушивания входящих подключений? 20. Что такое Метод трансляции IP-адресов?
Шкала оценивания, нижнее значение	0
Шкала оценивания, верхнее значение	20
Шкала оценивания, минимальный проходной балл	10
Безопасность Веб-приложений с применением ИИ, Модуль 4	
Количество академических часов	1
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.

Варианты заданий (представлены в качестве приложения к ДОП)	1. Какой протокол обеспечивает шифрование данных между клиентом и сервером в веб? 2. Какая уязвимость возникает, если веб-приложение не проверяет ввод пользователя перед вставкой в HTML? 3. Какой HTTP-заголовок помогает предотвратить XSS-атаки? 4. Какой тип XSS возникает, когда вредоносный скрипт сохраняется в базе данных? 5. Какой метод защиты от XSS предполагает экранирование спецсимволов (`<`, `>`, `&`)? 6. Какой из этих тегов HTML наиболее опасен с точки зрения XSS? 7. Что произойдет, если злоумышленник введет `&apos; OR &apos;1&apos;=&apos;1` в поле логина без защиты от SQL-инъекций? 8. Какой метод предотвращает SQL-инъекции в Python? 9. Какой тип инъекции возможен в NoSQL-базах? 10. С помощью какой функции во Flask экранировать пользовательский ввод для защиты от XSS? (напишите только название функции) 11. Какой метод НЕ является безопасным для хранения паролей? 12. Какой HTTP-код возвращается при успешной аутентификации? 13. Как ИИ может помочь в предотвращении SQL-инъекций? 14. Какой HTTP-метод следует использовать для передачи конфиденциальных данных? 15. Какой тип XSS эксплуатируется через изменение DOM без перезагрузки страницы? 16. Какая уязвимость возможна, если приложение выполняет команды ОС через пользовательский ввод? 17. Какой код состояния HTTP указывает на отсутствие доступа? 18. Как ИИ помогает обнаруживать аномалии в HTTP-запросах? 19. Как защититься от CSRF-атак в Flask приложении? 20. Что проверяет DAST-сканер?
Шкала оценивания, нижнее значение	0
Шкала оценивания, верхнее значение	20
Шкала оценивания, минимальный проходной балл	10

Итоговый контроль / аттестация	
Количество академических часов	4.00
Формы контроля	Представление итогового проекта
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)
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

Варианты заданий (представлены в качестве приложения к ДОП)	Темы для итогового проекта (по выбору учащегося): 1. «Система управления паролями» Задача: создать систему управления паролями, которая поможет пользователям генерировать, хранить и обновлять надежные пароли. 2. «Умный антивирус». Задача: разработать Python-скрипт, анализирующий файлы на наличие вредоносного кода с помощью библиотеки pyclamd. 3. «Бот-разведчик уязвимостей». Задача: Создать Telegram-бота на python-telegram-bot, который проверяет сайты на уязвимости (SQL-инъекции, XSS). 4. «Робот-пентестер Wi-Fi». Задача: Автоматизировать поиск слабых точек в домашних сетях с помощью scapy и airodump-ng. 5. «Шифрователь файлов» Задача: Инструмент для шифрования/дешифрования файлов с графическим интерфейсом (Tkinter) или веб-интерфейсом (Flask). Поддерживает симметричное шифрование (AES) и опционально асимметричное (RSA для ключей). 6. «Секретный редактор» Задача: Шифрующий текстовый редактор (Tkinter) для безопасного ведения записей. Автоматически шифрует/дешифрует содержимое при сохранении/открытии файла с использованием пароля пользователя (AES). 7. «Мастер ключей» Задача: Система управления цифровыми ключами (API-ключами, токенами). Хранит чувствительные строки в зашифрованном виде (SQLite + AES), предоставляет безопасный интерфейс для копирования (без отображения в открытом виде). 8. «Монитор сети» Задача: Простейший монитор сетевой активности (на основе socket и scapy в режиме без привилегий). Визуализирует (графики/таблицы в Tkinter или Flask) входящие/исходящие соединения на локальной машине. 9. «Чистильщик ссылок» Задача: Инструмент для "очистки" и проверки URL. Удаляет трекеры (utm-параметры), предупреждает о подозрительных доменах. Может интегрироваться как веб-сервис (Flask) или десктоп-приложение. 10. «Мониторинг входа» Задача: Система мониторинга попыток входа для учебного веб-приложения (Flask). Логирует IP, время, успешность попыток входа. Визуализирует данные и реализует простую защиту от брутфорса.
Шкала оценивания, нижнее значение	0.00
Шкала оценивания, верхнее значение	30.00
Шкала оценивания, минимальный проходной балл	16.00
Дополнительные сведения (предложения по ЕВИ и ИТиСИ)	

Вопросы для ЕВИ	1. Укажите, какой результат будет выведен на экран после выполнения кода a = 10 b = 11 c = 12 a, b = b, a print(a - b * c) 2. Укажите, какой результат будет выведен на экран после выполнения кода. x = 5 y = 7 c = x x = y y = c print(x) 3. С помощью какого ключевого слово можно объявить функцию в Python? 4. Какой тип данных создается конструкцией {}? - Список - Множество - Словарь - Кортеж 5. Что делает функция enumerate()? - Возвращает пары индекс-значение - Сортирует элементы - Удаляет элементы - Преобразует строку 6. Какая функция возвращает минимальное значение? 7. Какой метод преобразует список в строку? - join() - split() - convert() - map() 8. Что делает pass? 9. Укажите, какой результат будет выведен на экран после выполнения кода. try: a = 7 / 0 print(a) except: print(10)

	10. Что делает функция round()? - Преобразует строку в число - Возвращает целое число - Округляет число - Делит число 11. Что вернет выражение bool(0)? - True - 0 - False - None 12. Укажите, какой результат будет выведен на экран после выполнения кода a = 10 b = 15 c = a f, c = b + a , a print(f + c) 13. Что вернёт: print("Python"[0])? 14. Что делает функция int("5")? - Преобразует строку в число - Удаляет пробелы - Создает список - Проверяет тип 15. Укажите, какой результат будет выведен на экран после выполнения кода. a = 10 b = 3 a = a - a % 3 a, b = b, a print(b ** a)

Вопросы для ИТиСИ	1. Как вызвать собственную функцию с именем greet? - call greet - greet() (Правильный ответ) - func greet - start greet 2. Сколько раз выполнится цикл: k = 1 while k < 10: k += 2 3. Что вернёт range(1, 5)? - [1, 2, 3, 4] - [1, 2, 3, 4, 5] - [0, 1, 2, 3, 4] - [1, 5] 4. Укажите, какой результат будет выведен на экран после выполнения кода a = 'Привет' b = 'мир' str = f"Привет {b}" print(len(str)) 5. Что произойдёт, если открыть несуществующий файл с режимом 'r'? - Создастся новый файл - Ничего - Произойдёт ошибка - Откроется пустой файл 6. Каков результат данной операции: len({"a": 1, "b": 2})? - 1 - 2 - 0 - Ошибка 7. Какой из этих методов строк удаляет пробелы в начале строки? - strip() - trim() - lstrip() - startstrip() 8. Напишите число, которое мы увидим на экране после выполнения программы. lst = [1, 2, 3, 4, 5] value = 0

	i = 0
	j = len(lst)
	for r in range(i, j):
	  value = value + lst[r]
	print(value)
	9. Что делает функция round(4.567, 2)?
	- Округляет до целого
	- Округляет до 3 знаков
	- Округляет до двух знаков после запятой
	- Удаляет дробную часть
	10. Как называется исключение, возникающее при попытке деления на ноль?
	11. Что произойдет, если попытаться открыть несуществующий файл без обработки ошибок?
	- Файл создастся
	- Файл проигнорируется
	- Выдаст исключение
	- Возвратится пустая строка
	12. Какой результат у выражения "a" * 3?
	- aaa
	- 3a
	- Error
	- a3
	13. Укажите, сколько раз будет выведена на экран буква «A» после выполнения кода.
	a = -1
	while a < 10:
	  a += 1
	  if a >= 7:
	  continue
	  print("A")
	14. Какое ключевое слово используется для передачи управления исключению?
	15. Какое ключевое слово используется для объявления цикла, в котором условие проверяется после выполнения тела?
	- do...while
	- while
	- for
	- Нет такого ключевого слова

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», геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного 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, - технологий «перевернутого класса», геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного 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, - технологий «перевернутого класса», геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного 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, - технологий «перевернутого класса», геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного обучения.
Методические разработки (представлены в качестве приложения к ДОП)	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 (представлены в качестве приложения к ДОП)	Материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, 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.	Материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, 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.	Материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, 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.	Материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, 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, 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.	Black Hat Python: программирование для хакеров и пентестеров. 2-е изд. — СПб.:Питер, 2022. — 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»).	Python. Разработка на основе тестирования. / пер. с англ. Логунов А. В. – М.: ДМК Пресс, 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»).	Искусство тестирования на проникновение в сеть / пер. с анг. В. С. Яценкова. – М.: ДМК 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»).

Основные данные ДОП: УРОВЕНЬ ПРОДВИНУТЫЙ

№ п/п	Наименование поля	Значение поля
1.	Название ДОП	Этичный хакинг: миг уникальности
2.	Уровень сложности ДОП	ПРОДВИНУТЫЙ
3.	Объем/общая трудоемкость ДОП (общий объем освоения ДОП в академических часах)	148.00
4.	Объем каждого модуля в ак.ч.	Модуль1 - 36 Модуль2 - 36 Модуль3 - 36 Модуль4 - 36
5.	Общее количество образовательных мероприятий	16
6.	Объем недельной нагрузки обучающегося	4.00
7.	Дата начала и дата окончания обучения по ДОП (срок освоения ДОП)	С 2025-09-22 по 2026-05-29
9.	Выдаваемый по окончании обучения документ	Сертификат

Описание ДОП

№ п/п	Наименование поля	Значение поля
1.	Актуальность ДОП	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-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.

2.	Цель и задачи ДОП	Цель ДОП: 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 ДОП: 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.

3.	Планируемые результаты	В результате освоения программы выпускники будут знать: 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; Выпускники будут уметь: 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.
4.	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.
5.	Дополнительно (в соответствующих отдельных графах) может быть дана следующая информация по ДОП:	
5.1.	Стоимость обучения по ДОП	37304.00

5.2.	Рекомендации по обучению на ДОП	РЕКОМЕНДАЦИИ ДЛЯ УЧАЩИХСЯ 1. Требования к техническому оснащению: • Компьютер или ноутбук с доступом в Интернет • Установленные программы: o Python o IDE: PyCharm или Visual Studio Code • Виртуальные машины (Kali Linux, bWAPP, DVWA) • Браузер • Средства связи (MAX, Telegram и/или электронная почта) 2. Навыки, необходимые для успешного обучения: • Уверенное владение базовыми компьютерными навыками • Умение работать с браузером и файлами • Навыки самостоятельного поиска и анализа информации • Готовность к самоподготовке и командной работе • Способность презентовать собственные решения 3. Поведенческие рекомендации: • Занимайтесь регулярно: не менее 2–3 раз в неделю • Ведите дневник проекта (изученное, успехи, трудности) • Не стесняйтесь обращаться к преподавателю за разъяснениями • Ищите аналогии — это поможет лучше понять материал • Работайте в профессиональной среде разработки, используйте официальную документацию • Помните: ошибки — не провал, а путь к обучению 4. Правила: • Не пропускайте занятия: темы логически связаны • Не копируйте чужой код — важно понимание • Соблюдайте этику — курс обучает защите, а не атаке • Работайте с виртуальными машинами только в учебной среде РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ 1. Использование учебно-методического комплекса (УМК): Для реализации программы необходимо использовать утверждённый УМК, включающий: • Рабочую программу и календарно-тематическое планирование • Презентации, практические задания, тесты и кейсы по модулям • Задания для самостоятельной работы и проектов • Документационные шаблоны: чек-листы, формы отчётов, критерии оценки Преподаватель обязан строго соблюдать структуру курса и утверждённые контрольные точки. 2. Этическое сопровождение обучения: Преподавателю необходимо: • Формировать у обучающихся понимание границ этичного хакинга • Акцентировать внимание на правовой ответственности в цифровой среде • Развивать навыки цифровой гигиены и киберэтики: o Защита персональных данных o Уважительное взаимодействие в сети • Контролировать соблюдение этики в онлайн и офлайн-коммуникации 3. Требования к техническому оснащению: Для проведения занятий в очной форме с применением дистанционных образовательных технологий, в том числе с применением средств электронного обучения требуется: • Компьютер с предустановленным необходимым ПО • Стабильный доступ к ВКС • Рабочие аккаунты в LMS, мессенджерах, электронной почте • Высокоскоростной Интернет, обеспечивающий: o Загрузку

		и работу с виртуальными машинами o Проведение видеозанятий без потерь связи o Доступ к облачным сервисам и библиотекам ИИ

3. Комплекс организационно-педагогических условий реализации ДОП:
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	Инструменты Python для решения сложных задач	8	2	5	0	1	0
2.		Базы данных и обработка файлов на Python	8	2	5	0	1	0
3.		Основы параллельных вычислений и многопоточного программирования	9	2	5	1	1	0
4.		Создание графических интерфейсов на Python и применению ИИ для разработки программ	10	2	6	1	1	0
5.		Промежуточная аттестация	1	0	0	0	1	0
6.	Модуль 2 Защита от сетевых атак с применением ИИ	Уязвимости сетевых протоколов и их анализ с помощью ИИ	8	2	5	0	1	0
7.		Анализ и перехват трафика с применением ИИ	8	2	5	0	1	0
8.		ARP-атаки и сниффинг	9	2	5	1	1	0
9.		Защита сетевых ресурсов с применением ИИ	10	2	6	1	1	0
10.		Промежуточная аттестация	1	0	0	0	1	0
11.	Модуль 3 Безопасность веб-приложений с применением ИИ	Эксплуатация уязвимостей веб-приложений с помощью ИИ	8	2	5	0	1	0
12.		Защита баз данных с применением ИИ	8	2	5	0	1	0

13.		Аутентификация и атаки на сессии с применением ИИ	9	2	5	1	1	0
14.		Защита и противодействие атакам на веб-приложения с помощью ИИ	10	2	6	1	1	0
15.		Промежуточная аттестация	1	0	0	0	1	0
16.	Модуль 4 Комплексная безопасность информационных систем с применением ИИ	Цифровая экспертиза с применением ИИ	8	2	5	0	1	0
17.		Манипулятивные атаки с применением ИИ	8	2	5	0	1	0
18.		Обход системы защиты и противодействие этому с помощью ИИ	9	2	5	1	1	0
19.		Безопасные системы с применением ИИ	10	2	6	1	1	0
20.		Промежуточная аттестация	1	0	0	0	1	0
Итоговый контроль/аттестация по ДОП			4.00	0	0	0	4.00	0
Итого по ДОП:			148	32	84	8	24	0
ИТиСИ			Часы ИТиСИ не входят в общую трудоемкость ДОП, но участие в ИТиСИ обязательно для всех успешно прошедших итоговый контроль/аттестацию по ДОП					

Рабочая программа с описанием каждого модуля ДОП

Элементы ДОП (модули и итоговый контроль/аттестация по 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 с потоками, параллельные	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.	Теоретическая подготовка	2
		Реализация декоратора timer для измерения времени выполнения функции и создание генератора, выводящего последовательность чисел Фибоначчи до заданного предела.	Практические занятия	5
			Самостоятельная работа	0

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. Типы задач/деятельности: Программные решения с использованием продвинутых возможностей Python, включая создание декораторов и генераторов для оптимизации работы функций, реализацию паттернов проектирования		Текущий контроль по теме "Инструменты Python для решения сложных задач".	Текущий контроль	1
	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).	Теоретическая подготовка	2
		Создание и работа с файлом (запись и чтение данных) и базой данных SQLite (создание таблицы users, добавление записей).	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Базы данных и обработка файлов на Python".	Текущий контроль	1
	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 процесса-ми, обмена данными и распределенных вычислений.	Теоретическая подготовка	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	1
		Текущий контроль по теме "Основы параллельных вычислений и многопоточного программирования".	Текущий контроль	1
	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.	Теоретическая подготовка	2
		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

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.		Разработка с помощью ИИ графического приложения на выбранной библиотеке, позволяющего пользователю создавать, сохранять и открывать файлы.	Самостоятельная работа	1
		Текущий контроль по теме "Создание графических интерфейсов на Python и применению ИИ для разработки программ".	Текущий контроль	1
	Промежуточная аттестация	Тестирование 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.	Промежуточная аттестация	1
Модуль 2 Защита от сетевых атак с применением ИИ 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 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	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).	Теоретическая подготовка	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
			Самостоятельная работа	0
		Текущий контроль по теме "Уязвимости сетевых протоколов и их анализ с помощью ИИ".	Текущий контроль	1
	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).	Теоретическая подготовка	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
			Самостоятельная работа	0
		Текущий контроль по теме "Анализ и перехват трафика с применением ИИ".	Текущий контроль	1
	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.	Теоретическая подготовка	2

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: 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 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
		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	1
		Текущий контроль по теме "ARP-атаки и сниффинг".	Текущий контроль	1
	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.	Теоретическая подготовка	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	1
		Текущий контроль по теме "Защита сетевых ресурсов с применением ИИ".	Текущий контроль	1
	Промежуточная аттестация	Тестирование 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.	Промежуточная аттестация	1
Модуль 3 Безопасность веб-приложений с применением ИИ 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	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).	Теоретическая подготовка	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 целью несанкционированного доступа или изменения данных.	Практические занятия	5

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. Цель модуля: 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			Самостоятельная работа	0
		Текущий контроль по теме "Эксплуатация уязвимостей веб-приложений с помощью ИИ".	Текущий контроль	1
	Защита баз данных с применением ИИ	Рассматриваются SQL-инъекции, их принципы работы и типы (синтаксические ошибки, временные задержки, бандлинъекции), а также методы защиты: параметризация запросов, подготовленные выражения, ограничение прав доступа и санитизация ввода.	Теоретическая подготовка	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
			Самостоятельная работа	0
		Текущий контроль по теме "Защита баз данных с применением ИИ".	Текущий контроль	1
	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.	Теоретическая подготовка	2
		Разработка с помощью ИИ системы аутентификации на основе сессий в Flask, обеспечивающей защиту данных через шифрование и подпись сессий, а так-же изучение методов безопасной аутентификации, включая двухфакторную авторизацию с одноразовыми паролями или мобильными приложениями.	Практические занятия	5
		Рассмотрение стандартов безопасности сессий и аутентификации в веб-приложениях, включая OWASP Top 10, и применение возможностей ИИ для проведения аудита безопасности.	Самостоятельная работа	1

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 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		Текущий контроль по теме "Аутентификация и атаки на сессии с применением ИИ".	Текущий контроль	1
	Защита 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.	Теоретическая подготовка	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	1
		Текущий контроль по теме "Защита и противодействие атакам на веб-приложения с помощью ИИ".	Текущий контроль	1
	Промежуточная аттестация	Тестирование 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.	Промежуточная аттестация	1
Модуль 4 Комплексная безопасность информационных систем с применением ИИ 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	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.	Теоретическая подготовка	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
			Самостоятельная работа	0

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 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		Текущий контроль по теме "Цифровая экспертиза с применением ИИ".	Текущий контроль	1
	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.	Теоретическая подготовка	2
		Разработка с помощью ИИ скрипта на Python для создания фишингового письма, включающего элементы 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.	Практические занятия	5
			Самостоятельная работа	0
		Текущий контроль по теме "Манипулятивные атаки с применением ИИ".	Текущий контроль	1
	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.	Теоретическая подготовка	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	1
		Текущий контроль по теме "Обход системы защиты и противодействие этому с помощью ИИ".	Текущий контроль	1
	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.	Теоретическая подготовка	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
		Разработка с помощью ИИ механизма безопасной передачи файлов по сети с использованием протокола SSH и симметричного шифрования.	Самостоятельная работа	1
		Текущий контроль по теме "Безопасные системы с применением ИИ".	Текущий контроль	1

авторизации, реализация шифрования данных и обеспечение конфиденциальности, а также составление отчетов по анализу уязвимостей и рекомендаций по повышению уровня защищенности информационных систем.	Промежуточная аттестация	Тестирование 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.	Промежуточная аттестация	1
Итоговый контроль/аттестация	Итоговый контроль/аттестация по ДОП	Представление итогового проекта 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)	Итоговый контроль/аттестация	4.00

		Объем в ак.ч.	**Объем в %**
ИТОГО ПО ПРОГРАММЕ:	Теоретическая подготовка	32,00	21,62
	Практическая работа	84,00	56,76
	Самостоятельная работа	8,00	5,41
	Текущий контроль	16,00	10,81
	Промежуточная аттестация	4,00	2,70
	Итоговый контроль/аттестация	4.00	2,70
	Всего:	**148**	

ИТиСИ	Часы ИТиСИ не входят в общую трудоемкость ДОП, но участие в ИТиСИ обязательно для всех успешно прошедших итоговый контроль/аттестацию по ДОП

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	2025-09-22	1	2025-09-22	69	2026-05-29
				2	2025-12-01	64	
				3	2026-02-03	56	
				4	2026-03-30	61	

Сведения об условиях реализации ДОП (в том числе материально-техническое, информационное, кадровое обеспечение)

Материально-технические и информационные условия реализации ДОП

Наименование поля	Значение полей	Значение полей	Значение полей	Значение полей
Порядковый номер модуля	1	2	3	4
Перечень требований к оснащению площадки (для офлайн-формата)	«Не заполняется»	«Не заполняется»	«Не заполняется»	«Не заполняется»
Наименование требуемого оборудования (для онлайн-формата)	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 (для онлайн-формата)	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).

Информационные условия реализации ДОП (заполняется по каждому модулю):

Наименование поля	Значение полей	Значение полей	Значение полей	Значение полей
Порядковый номер модуля	1	2	3	4

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 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: 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. 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. - 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.	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 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.	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 кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/articles/276477/ (дата обращения: 05.07.2025) - Текст: электронный.

Наименование поля	Значение полей	Значение полей	Значение полей	Значение полей
Порядковый номер модуля	1	2	3	4

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 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.	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.

Кадровое обеспечение

Сведения о работниках, привлекаемых к реализации и разработке ДОП

ФИО	Роль	Наименование основного места работы	Должность	Ученая степень	Ученое звание	Ссылка на веб-страницы с портфолио	Образование. Наименование учебного заведения	Образование. Год окончания учебного заведения	Образование. Полученная специальность	Стаж работы в данной (аналогичной) должности	Основание для привлечения к реализации ДОП (трудовой договор, договор ГПХ, иное)	Информация о курсах повышения квалификации по профилю преподаваемой дисциплины (за последние 3 года)	Опыт работы в сфере ИТ (в области программирования, робототехники, искусственного интеллекта)	Отметка о полученном согласии на обработку персональных данных
строка	строка	строка	строка	строка	строка	каждая ссылка с новой строки	строка	числовое значение	строка	числовое значение	строка	строка	строка	строка
Сойманова Светлана Викторовна	Разработчик	РУКОН Цель	Методист			https://цель-обучение.рф/experts/soymanova	Пермский государственный университет	2002	Географ. Преподаватель. по специальности "География"	10	Трудовой договор	Вопросы применения средств криптографической защиты информации (СКЗИ), 72 час., Автономная некоммерческая организация дополнительного профессионального образования «Центр профессионального развития ПРОФИ», 2024 г.		Да

Зигуля Андрей Сергеевич	Разработчик	ООО «Дилибриум»	Генеральный директор ООО «Дилибриум»			https://цель-обучение.рф/experts/zigulya	Сумской техникум пищевой промышленности	2002	Специальность "Обслуживание компьютерных и интеллектуальных систем и сетей"	10	Договор ГПХ	Проектно-образовательный интенсив «Архипелаг 2024»	Опыт работы: 21 год. Работа в составе экспертной группы проекта «Масштабирование на региональном уровне модели кадрового обеспечения внедрения передовых производственных технологий» Агентство по развитию человеческого капитала в Северо-Западном федеральном округе и Фонда инфраструктурных и образовательных программ (группа РОСНАНО), сотрудничество в области инновационного развития с ОАО «РЖД», направленного на внедрение высокотехнологичных инновационных решений предусматривающих использование технологий, процессов или продуктов, ранее не применявшихся ОАО «РЖД», Aquamatica – роботизированные аквафермы (действующий резидент Сколково), участие в круглых столах Государственной Думы РФ посвященных информационной безопасности. Выступление в Государственной Думе РФ с докладом «Манипуляция общественным сознанием посредством интернет технологий». Финалист конкурса Архипелаг 20.35. Автор учебных курсов «Цифровая трансформация бизнеса» совместно с Санкт-Петербургским Государственным Университетом,	Да

													образовательная платформа Coursera, «Цифровая трансформация в государственном управлении» совместно с Российской Академией Народного Хозяйства и Государственной Службы при Президенте РФ.	
Почаевец Андрей Андреевич	Преподаватель	РУКОН Цель	Программный директор АНО ДПО МЦК "Цель", преподаватель линейки программ 1С. Эксперт в области программирования в 1С и управления командой разработчиков.			https://цель-обучение.рф/experts/pochaevets	Государственное образовательное учреждение высшего профессионального образования "Архангельский государственный технический университет"	2007	Инженер по специальности "Информационные системы и технологии"	4	Трудовой договор		Опыт работы в сфере IT более 15 лет. Участие в проектах цифровизации бизнес-процессов и внедрения ERP-решений в компаниях различных отраслей. Опыт автоматизации от продаж и маркетинга до комплексных систем управления предприятиями. Основное направление деятельности – внедрение и адаптация 1С для решения задач управленческого учета, бюджетирования и контроля проектов. Опыт внедрения таких решений как 1С:ERP, 1С:Комплексная автоматизация, 1С:CRM и настройка их интеграцию с другими бизнес-системами. Успешная практика реализации проектов в строительной сфере, тяжелом машиностроении, производстве, энергетике и гостиничном бизнесе. Участие в разработке и проведении обучающих программ по работе с 1С. Подготовка более 2000 аналитиков и программистов. А также опыт работы в международных проектах и работе с крупными промышленными предприятиями, где требуется комплексный подход к цифровой трансформации.	Да

Волков Александр Георгиевич	Преподаватель, Разработчик	Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»	Директор Института развития квалификаций	Кандидат технических наук	Доцент	https://цель-обучение.рф/experts/volkov	Мордовский ордена Дружбы народов госуниверситет им. Н.П. Огарева	1983	Промышленная электроника	21	Трудовой договор			Да
Рыбалёва Ирина Александровна	Разработчик	РУКОН Цель	Руководитель образовательного процесса	Кандидат педагогических наук		https://цель-обучение.рф/experts/rybaleva	Комсомольский-на-Амуре государственный педагогический институт (учитель русского языка и литературы	1994	Учитель русского языка и литературы	15	Договор об оказании услуг с индивидуальным предпринимателем	Развитие инфраструктуры авиационных систем на современном этапе, 72 час., АНО ДПО "МЦК "Цель", 2024 г.		Да
Пантелеев Сергей Владимирович	Преподаватель, Разработчик	Филиал НИТУ МИСиС г. Выкса	Доцент кафедры БД	Кандидат технических наук	Доцент	https://цель-обучение.рф/futurecode/panteleev	Владимирский государственный университет	1999	Инженер по специальности "Проектирование и технология радиоэлектронных средств"	26	Договор об оказании услуг с самозанятым лицом	Интенсив от университета Зерокодинга: AI-ассистент, интегрированный в Telegram, 2025 г.	Преподавание IT-дисциплин (Муромский институт ВлГУ, Выксунский металлургический техникум, Выксунский филиал НИТУ МИСиС) Программирование, системное администрирование с 2012 года (АО "Выксаэнерго", Нижновэнерго). Разработка сайтов с 2005 года (ООО "Виртуальная Выкса", самозанятость) к.т.н по искусственному интеллекту, специальность 05.13.01 "Системный анализ, управление и обработка информации", тема диссертации "Разработка, исследование и применение нейросетевых алгоритмов идентификации и управления динамическими системами". Преподаватель курсов «Технология программирования» (на Python), «Вычислительные машины, системы и сети», «Протоколы сетей», «Интернет-технологии» (HTML, CSS, PHP, Python, JavaScript, Jquery, MySQL, CMS).	Да

Кротов Александр Викторович	Разработчик	Код Грин Инжиниринг	Генеральный директор			https://цель-обучение.рф/experts/krotov	ФГБОУ ВПО "Санкт-Петербургский государственный электротехнический университет"ЛЭТИ" им. В.И. Ульянова (Ленина), 2012	2012	Инженер по специальности "Электронные приборы и устройства"	9	Договор ГПХ		Опыт работы в сфере IT - 8 лет. Компании: ЦНИИ РТК, ООО "НИЦ Радиотехники", Код Грин Инжиниринг.	Да

Формы аттестации и оценочные материалы (комплект контрольно-измерительных материалов, позволяющих определить достижение Получателями поддержки планируемых результатов)

Наименование поля	Значение полей
Текущий контроль	
Модуль 1, Продвинутое программирование на Python с ИИ, Инструменты Python для решения сложных задач	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Напишите ближайшее к 100 простое число. 2. Что такое генератор в Python? 3. Что делает ключевое слово «yield» в Python? 4. Какой метод необходимо определить в классе, чтобы он стал метаклассом? 5. Что такое дескриптор в Python? 6. Какой из следующих вариантов является примером множественного наследования? 7. Какой из следующих декораторов применяется для создания методов, которые не требуют экземпляра класса? 8. Какой метод создаёт экземпляр нового класса? 9. Какой из следующих вариантов является корректным способом создания генератора? 10. Какой из следующих вариантов является примером использования метакласса? 11. Какой из следующих вариантов является правильным способом создания последовательности чисел Фибоначчи с использованием генератора? 12. Какой из следующих методов используется для проверки, является ли число простым? 13. Какой из следующих вариантов является правильным способом создания генератора для последовательности простых чисел? 14. Как называется надстройка над функцией, которая принимает другую функцию и расширяет её поведение без изменения исходного кода. 15. Возможен ли механизм множественного наследования в Python? (да/нет)
Модуль 1, Продвинутое программирование на Python с ИИ, Базы данных и обработка файлов на Python	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.

Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Как называется простая база данных, для которой не нужен сервер, так как она работает на файлах? 2. Какой метод используется для открытия файла в Python в режиме чтения? 3. Что делает контекстный менеджер with при работе с файлами? 4. Какой модуль Python используется для работы с базой данных SQLite? 5. Какой SQL-запрос используется для создания таблицы в базе данных? 6. Какой метод используется для выполнения SQL-запроса в SQLite через Python? 7. Какой режим открытия файла позволяет добавлять данные в конец файла? 8. Что происходит, если попытаться открыть несуществующий файл в режиме 'r'? 9. Какой метод используется для получения всех строк из результата SQL-запроса? 10. Какой тип данных используется для поля `id` в таблице базы данных, если оно является первичным ключом? 11. Какой метод используется для закрытия соединения с базой данных SQLite? 12. Какой метод используется для записи данных в файл? 13. Какой параметр используется в методе `open()` для указания кодировки файла? 14. Какой SQL-запрос используется для изменения данных в таблице? 15. Какой метод используется для чтения всего содержимого файла в одну строку?
Модуль 1, Продвинутое программирование на Python с ИИ, Основы параллельных вычислений и многопоточного программирования	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Как называется модуль Python для многопроцессорных вычислений? 2. Что такое поток (thread) в контексте многопоточного программирования? 3. Какой механизм синхронизации используется для обеспечения доступа только одного потока к ресурсу одновременно? 4. Что делает объект Condition в модуле threading? 5. Какой объект из модуля threading позволяет ограничить количество одновременно работающих потоков? 6. Какой метод используется для запуска нового потока в Python? 7. Какой метод в модуле multiprocessing создает новый процесс? 8. Какой объект из модуля multiprocessing используется для обмена данными между процессами? 9. Какой код создаст поток, который выводит числа от 1 до 10 с задержкой в 1 секунду? 10. Какой код реализует три потока, каждый из которых выводит свое имя 5 раз? 11. Какой код правильно использует пул процессов для вычисления факториалов чисел от 1 до 10? 12. Что такое GIL (Global Interpreter Lock) в Python? 13. Какой метод используется для ожидания завершения потока в Python? 14. Что такое "пул процессов" (Process Pool)? 15. Какой из перечисленных модулей поддерживает как многопоточность, так и многопроцессность?
Модуль 1, Продвинутое программирование на Python с ИИ, Создание графических интерфейсов на Python и применению ИИ для разработки программ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.

Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Как называется кроссплатформенная библиотека Python, работающая в том числе и на Android? 2. Что такое GUI в контексте программирования? 3. Какой из перечисленных виджетов используется для отображения текста в PyQt? 4. Что такое событие в контексте GUI-приложений? 5. Какой метод в PyQt используется для запуска главного цикла приложения? 6. Что такое многопоточность в контексте GUI-приложений? 7. Какой метод в Kivy используется для добавления элементов в список? 8. Какой из следующих типов ИИ специализируется на обработке естественного языка? 9. Какой из следующих способов позволяет взаимодействовать с ИИ? 10. Какой из перечисленных методов PyQt используется для получения текста из поля ввода? 11. Какой из следующих подходов помогает оптимизировать интерфейс при работе с сетью? 12. Какой из следующих инструментов можно использовать для объяснения кода с помощью ИИ? 13. Какой из перечисленных методов Kivy используется для обработки событий нажатия кнопки? 14. Какой из следующих форматов данных чаще всего используется для сохранения файлов в GUI-приложениях? 15. Какой из следующих примеров является преимуществом использования ИИ для разработки кода?
Модуль 2, Защита от сетевых атак с применением ИИ, Уязвимости сетевых протоколов и их анализ с помощью ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какой максимальный номер порта в протоколе TCP/IP? 2. . Какой из перечисленных методов используется для обнаружения открытых портов на удалённом сервере? 3. Какой инструмент наиболее часто применяется для сканирования портов в сети? 4. Что такое DoS-атака? 5. Какой протокол считается уязвимым к атакам типа "перехват трафика" без использования шифрования? 6. Какой инструмент используется для анализа сетевого трафика? 7. Какие данные можно извлечь из HTTP-заголовков с помощью анализа трафика? 8. Какая из перечисленных уязвимостей связана с переполнением буфера? 9. Какой метод анализа трафика позволяет выявить аномалии в поведении сети с использованием ИИ? 10. Как называется процесс, при котором злоумышленник отправляет большее количество данных, чем может обработать буфер? 11. Какой из перечисленных методов защиты помогает предотвратить атаки типа "переполнение буфера"? 12. Какой из следующих инструментов используется для эксплуатации уязвимостей? 13. Какой протокол используется для безопасной передачи файлов? 14. Какой из следующих методов помогает защитить сеть от атак типа "межсайтовый скриптинг" (XSS)? 15. Какой из перечисленных методов автоматизации можно использовать для сканирования диапазона IP-адресов с помощью Python?

Модуль 2, Защита от сетевых атак с применением ИИ, Анализ и перехват трафика с применением ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. На каком порту работает сервис DNS? 2. Какой протокол является основным для передачи веб-страниц? 3. Что такое ARP-отравление? 4. Как называется атака, при которой злоумышленник разрывает соединение между двумя сторонами? 5. Какой фильтр в Wireshark позволяет отфильтровать только HTTP-трафик? 6. Какой метод шифрования обеспечивает защиту HTTPS-трафика? 7. Какое событие может быть признаком ARP-атаки? 8. Для чего используется sslstrip? 9. Какой алгоритм ИИ может использоваться для выявления аномалий в сетевом трафике? 10. Какие данные можно анализировать в зашифрованном трафике без дешифрования? 11. Какой протокол используется для отправки электронной почты? 12. Какой тип атаки может изменить DNS-ответы, чтобы перенаправить пользователя на фишинговый сайт? 13. Какой инструмент можно использовать для анализа SSL/TLS-трафика? 14. Какой порт используется для HTTPS-трафика? 15. Какой метод защиты помогает предотвратить ARP-отравление?
Модуль 2, Защита от сетевых атак с применением ИИ, ARP-атаки и сниффинг	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.

	1. В каком месте находится ARP-таблица в операционных система Linux? 2. Что такое сниффинг в контексте сетевой безопасности? 3. Какую основную функцию выполняет протокол ARP? 4. Какая уязвимость протокола ARP делает возможным проведение ARP-атак? 5. Как называется атака, при которой злоумышленник подменяет MAC-адрес в ARP-таблице? 6. Какой инструмент часто используется для проведения ARP-атак? 7. Что такое ARP-спуфинг? 8. Какой метод защиты помогает предотвратить ARP-атаки? 9. Какие пакеты анализируются при обнаружении ARP-атак? 10. Какой метод может использоваться для автоматического обнаружения подмены ARP-записей? 11. Что такое ARP-таблица? 12. Какой параметр ARP-пакета обычно подменяется при ARP-спуфинге? 13. Какой метод защиты от ARP-атак предполагает использование криптографии? 14. Какой алгоритм ИИ может быть использован для анализа ARP-трафика и выявления аномалий? 15. Какой параметр ARP-пакета остается неизменным при ARP-спуфинге?
Модуль 2, Защита от сетевых атак с применением ИИ, Защита сетевых ресурсов с применением ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Как называется фаервол в операционных система Linux? 2. Какую основную функцию выполняет IDS (система обнаружения вторжений)? 3. Какой метод является эффективным для противодействия DDoS-атакам? 4. Какие протоколы безопасности наиболее часто используются для шифрования данных при передаче? 5. В чем заключается основное преимущество использования ИИ для настройки брандмауэра? 6. Какой тип трафика может быть заблокирован с помощью правил брандмауэра на основе портов? 7. Для чего применяется протокол IPsec? 8. Какой из перечисленных методов используется для фильтрации трафика по IP-адресам? 9. Какая цель реализуется при использовании сетевых политик безопасности? 10. Какую задачу решает IPS (система предотвращения вторжений)? 11. Какое действие рекомендуется предпринять для защиты от DoS-атак? 12. Какой механизм используется для аутентификации участников соединения в IPsec? 13. Какие данные анализируются при фильтрации трафика на основе протоколов? 14. Какой из перечисленных компонентов является частью SSL/TLS-шифрования? 15. Какой из перечисленных методов используется для защиты от несанкционированного доступа к сетевым ресурсам?
Модуль 3, Безопасность веб-приложений с применением ИИ, Эксплуатация уязвимостей веб-приложений с помощью ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.

Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какой тип уязвимости позволяет злоумышленнику внедрить вредоносный SQL-код в запрос к базе данных? 2. Какой метод анализа предполагает изучение исходного кода приложения для поиска уязвимостей? 3. Какой инструмент можно использовать для перехвата и анализа HTTP/HTTPS трафика? 4. Какая библиотека Python может быть использована для работы с HTTP-запросами при тестировании на уязвимости? 5. Какой тип XSS-атаки сохраняет вредоносный скрипт в базе данных, чтобы он выполнялся при каждом обращении к зараженной странице? 6. Какой метод защиты от SQL-инъекций считается наиболее эффективным? 7. Какой механизм защиты помогает предотвратить CSRF-атаки? 8. Какой инструмент можно использовать для автоматического сканирования веб-приложений на наличие уязвимостей? 9. Какой тип уязвимости позволяет злоумышленнику выполнить произвольный код на сервере? 10. Какой метод используется для очистки пользовательского ввода от потенциально опасных символов? 11. Какой тип атаки использует доверие пользователя к веб-сайту для выполнения нежелательных действий? 12. Какой инструмент можно использовать для анализа безопасности веб-приложений с использованием методологии черного ящика? 13. Какой тип XSS-атаки отражает вредоносный скрипт в URL или параметрах запроса? 14. Какой метод защиты от XSS предполагает преобразование специальных символов в их HTML-эквиваленты? 15. Какой инструмент можно использовать для автоматической генерации и отправки вредоносных запросов для тестирования на SQL-инъекции?
Модуль 3, Безопасность веб-приложений с применением ИИ, Защита баз данных с применением ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что такое SQL-инъекция? 2. Какой тип SQL-инъекции эксплуатирует временные задержки для получения информации? 3. Что является основным методом защиты от SQL-инъекций? 4. Какую функцию выполняет подготовленное выражение в SQL? 5. Какой из перечисленных методов НЕ защищает от SQL-инъекций? 6. В каком случае может быть использована слепая SQL-инъекция? 7. Какую задачу решает санитизация ввода в контексте защиты от SQL-инъекций? 8. Какой метод используется в Python для создания параметризованных запросов в SQLite? 9. Какой из следующих примеров является SQL-инъекцией? 10. Какой уровень прав доступа рекомендуется назначать приложениям для работы с базой данных? 11. Какие данные обычно используются для тестирования уязвимости к SQL-инъекциям? 12. Какой из следующих подходов помогает предотвратить слепую SQL-инъекцию? 13. Какой эффект достигается при использовании параметризованных запросов? 14. С каких символов начинается однострочный комментарий в SQL? 15. Какой из следующих подходов НЕ рекомендуется для защиты от SQL-инъекций?
Модуль 3, Безопасность веб-приложений с применением ИИ, Аутентификация и атаки на сессии с применением ИИ	
Количество академических часов	1

Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какой метод атаки на сессии предполагает перехват идентификатора сессии через незащищенное соединение? 2. Какая технология помогает защитить сессию от перехвата при передаче данных? 3. Что такое атака фиксации сессии? 4. Какое свойство сессий может помочь предотвратить атаку фиксации? 5. Какая из следующих практик является наиболее безопасной для хранения идентификаторов сессии? 6. Что такое двухфакторная аутентификация (2FA)? 7. Какой из следующих методов НЕ является фактором двухфакторной аутентификации? 8. Какую роль играет ограничение числа попыток входа в систему? 9. Какие преимущества дает использование подписи сессий в Flask? 10. Какой механизм используется для защиты данных сессии в Flask? 11. Какую роль выполняет флаг Secure в cookies? 12. Какие данные НЕ рекомендуется хранить в сессии? 13. Какую задачу решает одноразовый пароль (OTP) в двухфакторной аутентификации? 14. Что такое brute-force атака? 15. Какую роль играет ИИ в анализе поведения пользователя для выявления подозрительной активности?
Модуль 3, Безопасность веб-приложений с применением ИИ, Защита и противодействие атакам на веб-приложения с помощью ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какой метод защиты веб-приложений наиболее эффективен для предотвращения SQL-инъекций? 2. Что такое XSS-атака? 3. Какой заголовок HTTP помогает защитить веб-приложение от кликджекинга? 4. Какой стандарт безопасности веб-приложений описывает наиболее распространенные уязвимости? 5. Какой метод защиты от CSRF-атак является наиболее надежным? 6. Какой инструмент Django помогает защищать приложение от SQL-инъекций? 7. Какой заголовок HTTP рекомендуется использовать для защиты от MIME-тип атак? 8. Какой метод защиты от XSS-атак рекомендуется использовать в Django? 9. Какой тип XSS-атаки наиболее сложен для обнаружения? 10. Какой параметр HTTP-заголовка SameSite помогает защитить от CSRF-атак? 11. Какой стандарт безопасности веб-приложений фокусируется на программных ошибках? 12. Какой метод защиты рекомендуется использовать для предотвращения атак через загрузку файлов? 13. Какой модуль Django обеспечивает защиту от CSRF-атак? 14. Какой метод защиты рекомендуется использовать для предотвращения атак через URL-параметры? 15. Какой инструмент ИИ может помочь в анализе уязвимостей веб-приложения?
Модуль 4, Комплексная безопасность информационных систем с применением ИИ, Цифровая экспертиза с применением ИИ	

Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Что является основным отличием форензики от судебной экспертизы? 2. Какой метод чаще всего используется для восстановления удаленных файлов? 3. Что из перечисленного НЕ относится к метаданным файла? 4. При составлении отчета об анализе цифровых доказательств с помощью ИИ наиболее важным является: 5. Какой этап должен быть первым при анализе инцидента ИБ? 6. Какие данные считаются наиболее надежными в контексте судебной экспертизы? 7. Что является ключевым требованием к хранению цифровых доказательств? 8. Какую роль играет хэш-функция в цифровой форензике? 9. Что из перечисленного является этическим требованием к эксперту? 10. Какой тип данных чаще всего используется для установления временной шкалы событий? 11. Что из перечисленного является наиболее надежным способом предотвращения повторных инцидентов? 12. Что из перечисленного является наиболее важным при подготовке отчета о компьютерном преступлении? 13. Что является основным фактором при выборе инструментов цифровой форензики? 14. Какой подход наиболее эффективен для предотвращения внутренних угроз? 15. Какой элемент должен быть обязательно включен в рекомендации по предотвращению инцидентов?
Модуль 4, Комплексная безопасность информационных систем с применением ИИ, Манипулятивные атаки с применением ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.

	1. Какой метод социальной инженерии чаще всего используется для получения конфиденциальной информации через электронную почту? 2. Какой тип фишинга предполагает использование поддельных веб-сайтов, имитирующих известные бренды? 3. Какой элемент фишингового письма наиболее эффективен для манипуляции получателем? 4. Какая из перечисленных мер является наиболее эффективной для защиты от фишинга? 5. Какой формат файла чаще всего используется для сохранения фишинговых писем? 6. Какой вид социальной инженерии предполагает использование телефонных звонков для манипуляции жертвой? 7. Какой инструмент ИИ может помочь в создании обучающих материалов для сотрудников? 8. Какой тип атаки социальной инженерии направлен на конкретного человека или организацию? 9. Какой метод защиты от фишинга предполагает использование многофакторной аутентификации? 10. Какой элемент фишингового письма может быть создан с помощью ИИ для повышения его достоверности? 11. Какой тип теста наиболее эффективен для проверки знаний сотрудников о защите от социальной инженерии? 12. Какой метод ИИ может быть использован для автоматического обнаружения фишинговых писем? 13. Какой тип атаки предполагает использование SMS-сообщений для манипуляции жертвой? 14. Какой этап разработки обучающих материалов является наиболее важным для повышения их эффективности? 15. Какой метод защиты от социальной инженерии предполагает регулярное проведение тренингов для сотрудников?
Модуль 4, Комплексная безопасность информационных систем с применением ИИ, Обход системы защиты и противодействие этому с помощью ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.
Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какой метод атаки предполагает систематический перебор комбинаций паролей? 2. Какая библиотека в Python чаще всего используется для отправки HTTP-запросов при тестировании веб-приложений? 3. Что такое словарная атака? 4. Какой инструмент часто используется для автоматизации эксплуатации уязвимостей? 5. Какой метод защиты эффективен против брутфорс-атак? 6. Как называется процесс создания системы с известными уязвимостями для тестирования? 7. Какой метод аутентификации является более защищенным? 8. Какой метод защиты можно использовать для предотвращения перебора логинов и паролей? 9. Какой инструмент используется для сканирования сети на наличие открытых портов? 10. Какой метод атаки предполагает использование доверия пользователя к легитимному сайту? 11. Какой механизм защиты может использоваться для предотвращения атак типа "человек посередине" (MITM)? 12. Какой тип уязвимости позволяет злоумышленнику выполнить произвольный код на сервере? 13. Какой метод защиты можно использовать для предотвращения XSS-атак? 14. Какой инструмент можно использовать для анализа и модификации HTTP/HTTPS-трафика? 15. Какой метод защиты помогает предотвратить несанкционированный доступ к системе?
Модуль 4, Комплексная безопасность информационных систем с применением ИИ, Безопасные системы с применением ИИ	
Количество академических часов	1
Формы контроля	Тестовая форма контроля.
Диагностические инструменты	Форма текущего контроля – зачет, который проводится в форме тестирования, состоящего из 15 вопросов. Перечень вопросов составляется на основе изученного в процессе обучения материала по теме модуля. Время прохождение тестирования составляет 1 академический час.

Показатели и критерии оценивания	По результатам прохождения тестирования выставляются отметки по двухбалльной системе («зачтено», «не зачтено») с учетом следующих критериев: отметка «зачтено» – 60% и более правильных ответов; отметка «не зачтено» – менее 60% правильных ответов.
	1. Какой метод хранения паролей считается наиболее безопасным в системах управления пользователями? 2. Какой алгоритм хэширования рекомендуется использовать для хранения паролей? 3. Что такое асимметричное шифрование? 4. Какой протокол обеспечивает безопасную передачу файлов по сети? 5. Что такое "соль" в контексте хэширования паролей? 6. Какой из перечисленных методов является наиболее безопасным для аутентификации пользователей? 7. Какой тип шифрования используется в протоколе SSH для передачи файлов? 8. Что такое авторизация в системе безопасности? 9. Какой из перечисленных методов НЕ относится к защитным механизмам при разработке безопасных приложений? 10. Что такое цифровая подпись? 11. Какой из перечисленных методов используется для обеспечения конфиденциальности данных? 12. Что такое сертификат SSL/TLS? 13. Какой из перечисленных методов является наиболее эффективным для защиты от brute-force атак? 14. Что такое принцип наименьших привилегий? 15. Какой из перечисленных методов используется для обеспечения целостности данных?
Промежуточная аттестация (по модулям)	
Продвинутое программирование на Python с ИИ, Модуль 1	
Количество академических часов	1
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.

Варианты заданий (представлены в качестве приложения к ДОП)	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
	2. Какой оператор используется для получения значения из генератора?
	3. Для чего используется __metaclass__?
	4. Какой метод закрывает соединение с БД?
	5. Что предотвращает «Lock» в модуле threading?
	6. Какой виджет используется для ввода текста в PyQt?
	7. Что означает «GPT»?
	8. Какой метод дескриптора вызывается при присвоении значения?
	9. Как добавить обработчик нажатия кнопки в Kivy?
	10. Какое ключевое слово обозначает асинхронную функцию?
	11. Как создать генераторное выражение?
	12. Как применить декоратор к функции?
	13. Что гарантирует «with open(...)»?
	14. Что вернет «list(gen())»?
	def gen():
	 for i in range(3):
	  yield i * 2
	15. Как выполнить SQL-запрос в SQLite?
	16. С помощью какой функции достигается синхронизация доступа к общим ресурсам?
	17. Какой виджет в PyQt отображает текст?
	18. Как объявить метакласс?
	19. Как создать бесконечный генератор?
	20. Для чего используется «multiprocessing.Pool()»?

Шкала оценивания, нижнее значение	0
Шкала оценивания, верхнее значение	20
Шкала оценивания, минимальный проходной балл	10
Защита от сетевых атак с применением ИИ, Модуль 2	
Количество академических часов	1
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.

Варианты заданий (представлены в качестве приложения к ДОП)	1. Выберите уязвимость протокола DNS:
	2. Инструмент для анализа трафика с графическим интерфейсом:
	3. Цель DoS-атаки:
	4. Для защиты от перехвата трафика используется протокол:
	5. ARP-отравление возможно из-за:
	6. Порт по умолчанию для HTTPS:
	7. Инструмент для эксплуатации уязвимостей:
	8. Как называется атака которая имитирует легитимный сервер для перехвата трафика? (напиши-те аббревиатуру)
	9. IDS предназначена для:
	10. Фильтрация трафика по IP-адресам реализуется через:
	11. На каком уровне модели OSI работает Ipsec? (одним прилагательным)
	12. Протокол для безопасной передачи файлов:
	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
	14. Какой протокол может предотвратить перехват трафика в веб?
	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"
	16. Атаки на какой протокол обнаруживает эта функция?
	17. Для защиты от ARP-спуфинга используется:
	18. SSLstrip атакует путём:
	19. Инструмент для пассивного анализа трафика:
	20. IPS отличается от IDS тем, что:

Шкала оценивания, нижнее значение	0
Шкала оценивания, верхнее значение	20
Шкала оценивания, минимальный проходной балл	10
Безопасность веб-приложений с применением ИИ, Модуль 3	
Количество академических часов	1
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.

Варианты заданий (представлены в качестве приложения к ДОП)	1.Какой тип атаки используется?
	2. Какой метод безопасно выводит пользовательские данные?
	3. Какое условие обязательно для успешной CSRF-атаки?
	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,))
	5. Как подписать сессионные куки в Flask?
	6. Выберите прокси-сервер для перехвата HTTP(S):
	7. Какой HTTP-заголовок блокирует встраивание страницы в <iframe>?
	8. Какой метод используется для подтверждения уязвимости слепой SQL-инъекции?
	9. Какая функция Python преобразует <script> в безопасную строку?
	10. Какая библиотека Python используется для обработки естественного языка в санитизации?
	11. Какой оператор позволяет объединить результаты двух запросов в SQL?
	12. Что такое «фиксация сессии»?
	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)
	14. Какой параметр SameSite блокирует CSRF?
	15. Какая функция Python опасна для выполнения пользовательского ввода?
	16. Какой инструмент OWASP интегрирует ИИ для сканирования?
	17. Какой метод хеширования паролей соответствует стандартам OWASP?
	18. Где происходит выполнение вредоносного кода в DOM-based XSS?
	19. Какая СУБД может работать без сервера?
	20. Ниболее популярный фреймвор для разработки сайтов на Python?

Шкала оценивания, нижнее значение	0
Шкала оценивания, верхнее значение	20
Шкала оценивания, минимальный проходной балл	10
Комплексная безопасность информационных систем с применением ИИ, Модуль 4	
Количество академических часов	1
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.

Варианты заданий (представлены в качестве приложения к ДОП)	1. Цель цифровой форензики:
	2. **МС** (Multiple Choice): Методы извлечения данных:
	3. Цепочка расследования должна фиксировать всех, кто имел доступ к доказательствам? (да/нет)
	4. Этапы анализа доказательств:
	5. Ключевой элемент отчета об инциденте?
	6.ИИ может автоматически генерировать юридически значимые отчеты? (да/нет)
	7. Пример фишинга:
	8. Уязвимость при обходе аутентификации:
	9. Этапы атаки брутфорс:
	10. Функция хэширования пароля:
	import hashlib
	def hash_password(password, salt):
	return hashlib.____(salt.encode() + password.encode()).hexdigest()
	11. SSH использует асимметричное шифрование для установки соединения? (да/нет)
	12. Инструмент анализа метаданных:
	13. Самый опасный тип фишинга:
	14. Признаки уязвимости Broken Authentication
	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
	16. Лучшая защита от MITM-атак:
	17. Обнаружение фишинговых URL:
	def is_phishing(url):
	import re
	return bool(re.search(r'(?:http://|www\.)(?!trusted-domain)', _____))
	18. Какой метод НЕ используется для обхода аутентификации?
	19. Лучшая практика хранения паролей:
	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))

Шкала оценивания, нижнее значение	0
Шкала оценивания, верхнее значение	20
Шкала оценивания, минимальный проходной балл	10

Итоговый контроль / аттестация	
Количество академических часов	4.00
Формы контроля	Представление итогового проекта
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)

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.
Варианты заданий (представлены в качестве приложения к ДОП)	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.)
Шкала оценивания, нижнее значение	0.00
Шкала оценивания, верхнее значение	30.00
Шкала оценивания, минимальный проходной балл	16.00
Дополнительные сведения (предложения по ЕВИ и ИТиСИ)	

Вопросы для ЕВИ	1. Что гарантирует «with open(...)»? - Автоматическое закрытие файла - Шифрование данных - Кэширование записи - Освобождение буфера 2. Сколько раз выполнится цикл: k = 1 while k < 10: k += 2 3. Что вернёт range(1, 5)? - [1, 2, 3, 4] - [1, 2, 3, 4, 5] - [0, 1, 2, 3, 4] - [1, 5] 4. Укажите, какой результат будет выведен на экран после выполнения кода a = 'Привет' b = 'мир' str = f"Привет {b}" print(len(str)) 5. Что произойдёт, если открыть несуществующий файл с режимом 'r'? - Создастся новый файл - Ничего - Произойдёт ошибка - Откроется пустой файл 6. Каков результат данной операции: len({"a": 1, "b": 2})? - 1 - 2 - 0 - Ошибка 7. Какой из этих методов строк удаляет пробелы в начале строки? - strip() - trim() -. lstrip() - startstrip() 8. Напишите число, которое мы увидим на экране после выполнения программы. lst = [1, 2, 3, 4, 5] value = 0

	i = 0
	j = len(lst)
	for r in range(i, j):
	  value = value + lst[r]
	print(value)
	9. Что делает функция round(4.567, 2)?
	- Округляет до целого
	- Округляет до 3 знаков
	- Округляет до двух знаков после запятой
	- Удаляет дробную часть
	10. Как называется исключение, возникающее при попытке деления на ноль?
	11. Что произойдет, если попытаться открыть несуществующий файл без обработки ошибок?
	- Файл создастся
	- Файл проигнорируется
	- Выдаст исключение
	- Возвратится пустая строка
	12. Какой результат у выражения "a" * 3?
	- aaa
	- 3a
	- Error4
	- a3
	13. Укажите, сколько раз будет выведена на экран буква «A» после выполнения кода.
	a = -1
	while a < 10:
	  a += 1
	  if a >= 7:
	  continue
	  print("A")
	14. Какое ключевое слово используется для передачи управления исключению?
	15. Какое ключевое слово используется для объявления цикла, в котором условие проверяется после выполнения тела?
	- do...while
	- while
	- for
	- Нет такого ключевого слова

Вопросы для ИТиСИ	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
	- Результат my_function
	- Функцию wrapper
	- Ошибку
	- None
	2. Для чего используется __metaclass__?
	- Изменение создания классов
	- Обработка исключений
	- Оптимизация памяти
	- Множественного наследования
	3. Что предотвращает «Lock» в модуле threading?
	- Race condition
	- Утечку памяти
	- Deadlock
	- Семафор
	4. Какой метод дескриптора вызывается при присвоении значения?
	- __get__
	- __set__
	- __delete__
	- __upload__
	5. Что вернет «list(gen())»?
	def gen():
	  for i in range(3):
	  yield i * 2
	- [0, 1, 2]
	- [0, 2, 4]
	- [2, 4, 6]
	- [0, 2, 8]
	6. В поле краткого ответа введите результат работы функции boxes, которая будет принимать список весов отдельных товаров (в кг) и возвращать количество коробок, в которые можно упаковать все товары с этими весами при условии, что вместимость коробки 10 кг.
	В списке всегда будет как минимум один элемент. Все веса будут меньше или равны 10 кг. Упаковываться товары должны в том порядке, в котором стоят в списке.
	Тестовый список весов для поля краткого ответа:
	boxes([2, 1, 2, 5, 4, 3, 6, 1, 1, 9, 3, 2])

	7. Как объявить метакласс? - class MyClass(metaclass=Meta) - class MyClass(Meta) - class MyClass with Meta - class MyClass(Meta=metaclass) 8. Как создать бесконечный генератор? - while True: yield - for i in infinity: yield - yield from endless() - while None: yield 9. Имеется математическая последовательность, первый член которой равен 1, а каждый следующий задается по правилу: xi = xi – 1 % 3 + xi – 1 * 2. Найдите сотый член последовательности 10. Для чего используется «multiprocessing.Pool()»? - Создание потоков - Параллельное выполнение функций - Синхронизация процессов - Блокировка общего ресурса 11. Как можно реализовать ARP-спуфинг с помощью Python в локальной сети? - С использованием модуля scapy и отправкой поддельных ARP-ответов - С помощью socket.sendto() и формирования ARP-заголовков вручную - Через DNS-запросы с изменённым источником - Все вышеперечисленное 12. Как в Python можно обнаружить наличие активного MITM (man-in-the-middle) атаки в сети? - Проверяя дублирующиеся MAC-адреса в ARP-ответах - Анализируя TTL значений входящих пакетов - Отслеживая необычную активность на порту 80 - Никак — это невозможно сделать программно 13. Что делает следующая строка кода в контексте scapy? send(IP(dst="192.168.1.1")/TCP(dport=80, flags="S")) - Отправляет TCP-ACK пакет на порт 80 - Выполняет TCP SYN-сканирование порта 80 на целевой машине - Отправляет UDP-запрос на порт 80 - Завершает TCP-соединение с сервером 14. Какой из следующих подходов позволяет выполнять детектирование WAF (Web Application Firewall) с помощью Python? - Анализ HTTP-ответов на запросы с потенциально опасными символами - Использование sqlmap через интерфейс командной строки - Подмена User-Agent в HTTP-запросах
	- Все вышеперечисленные 15. Какой из следующих подходов может быть использован для эмуляции выполнения shellcode на Python без его прямого исполнения в памяти? - Использование библиотеки unicorn для эмуляции CPU и выполнения байт-кода - Простое декодирование base64 и вывод в hex-формате - Отправка shellcode на удалённый сервер для выполнения - Запуск кода через eval() с предварительным преобразованием

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», геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного 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, - технологий «перевернутого класса», геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного 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, - технологий «перевернутого класса», геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного 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, - технологий «перевернутого класса», геймификация, кейс-технология, онлайн-конференция, технология проектного обучения, технология проблемного обучения.
Методические разработки (представлены в качестве приложения к ДОП)	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 (представлены в качестве приложения к ДОП)	Материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, 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.	Материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, 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.	Материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, 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.	Материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, 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, 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.	Black Hat Python: программирование для хакеров и пентестеров. 2-е изд. — СПб.:Питер, 2022. — 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»).	Python. Разработка на основе тестирования. / пер. с англ. Логунов А. В. – М.: ДМК Пресс, 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»).	Искусство тестирования на проникновение в сеть / пер. с анг. В. С. Яценкова. – М.: ДМК 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»).