РУКОН ЦЕЛЬ
МНОГОПРОФИЛЬНЫЙ ЦЕНТР КВАЛИФИКАЦИЙ

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

УТВЕРЖДАЮ
Директор АНО ДПО «МЦК «Цель»

О. В. Самоварова

Приказ № 12п/2023-БО
от «16» июня 2023 г.

Одобрена на заседании
педагогического совета
Протокол № 4 от «15» июня 2023 г.

Дополнительная общеобразовательная

Общеразвивающая программа

«Этичный хакинг на Python: The Art of Exploitation»

(148 акад. час.)

Автор-составитель:

Сойманова Светлана Викторовна, методист

г. Санкт-Петербург, 2023 г.

Дополнительная общеобразовательная общеразвивающая программа технической направленности

«Этичный хакинг на Python: The Art of Exploitation»

1. Об организации

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

Контакты ответственного за программу. Должность	Методист
Контакты ответственного за программу. Телефон	+7(962)3450600
Контакты ответственного за программу. E-mail	mckcel@cifrosfera.ru

2. Пояснительная записка

Наименование поля	**Значение поля (примеры)**
Название программы (курса)	Этичный хакинг на Python: The Art of Exploitation
Описание программы	Язык программирования Python сегодня весьма популярен. В условиях современных реалий цифровой экономики использование этого языка программирования для обеспечения информационной безопасности является перспективным IT направлением. Этичный хакинг - это выстраивание эффективной защиты на основе глубинного понимания методов и инструментов действиям злоумышленников. Специалисты по кибербезопасности (этичные хакеры) моделируют взломы систем безопасности, проводят тесты на уязвимости придумывают новые способы проверки и защиты, используя для этого язык программирования Python.

	«The Art of Exploitation» с англ. «искусство эксплуатации». Данное название дополнительно подчеркивает продвинутый уровень Программы, так как подходы к обеспечению кибербезопасности фактически преподносятся как «искусство», то есть требуют творческого и креативного подхода. Данная программа поможет учащимся примерить на себя роль этичного хакера, позволит научиться использовать язык программирования Python для решения задач обеспечения информационной безопасности, поможет в профессиональном самоопределении относительно профессии специалиста по информационной безопасности. Обучаться по этой программе могут учащиеся 8-11 классов и учреждений среднего профессионального образования, владеющие основами программирования (основные концепции и структуры данных, работа с переменными, условиями и циклами, функции и модули в Python); имеющими базовые знания сетей; владеющими основными функциями и командами операционной системы (Windows или Linux); умеющими устанавливать программы и работать с файловой системой; имеющими первичное понимание принципов безопасности информации и основных угроз; владеющими основами веб-разработки. Обучение осуществляется очно с применением дистанционных образовательных технологий. Программа рассчитана на нормативную трудоемкость обучения – 148 академических часов, включая все виды аудиторной (теоретические и практические занятия) и внеаудиторной (самостоятельной) работы учащихся. Программа состоит из 4 модулей по 36 академических часов. Прохождение каждого модуля завершается промежуточной аттестацией в форме выполнения практических учебных задач. Программа носит практико-ориентированный характер, 57% времени отводится на отработку практических навыков и умений на практических занятиях под руководством опытных преподавателей, и в рамках самостоятельной работы, которая реализуется согласно инструкциям, гайдам, чек-листам и проч.

	Программа реализуется на русском языке. В результате обучения учащиеся освоят в углубленном формате язык программирования Python и научатся его применять в целях обеспечения информационной безопасности на предпрофессиональном уровне
Аннотация программы	Программа «Этичный хакинг на Python: The Art of Exploitation» разработана в рамках проекта "Код будущего". **#Этичный хакинг#Хакинг#Информационная безопасность#Защита данных** Программа имеет техническую направленность и адресована учащимся 8–11 классов и учреждений среднего профессионального образования, заинтересованным в углубленном изучении языка программирования Python, и в его применении для предотвращения угроз информационной безопасности. Для освоения программы необходимо: иметь базовые знания сетей; владеть основами программирования, основными функциями и командами операционной системы Windows или Linux, основами веб-разработки; уметь устанавливать программы и работать с файловой системой. Почти 57 % учебного времени отводится на отработку практических навыков и умений. В результате обучения участники программы освоят в углубленном формате навыки разработки на языке Python, научатся использовать этот язык программирования для защиты информационных систем от кибератак на предпрофессиональном уровне.
Цель программы	Освоение специализированных знаний и навыков в области программирования на языке Python для обеспечения информационной безопасности и поиска уязвимостей информационных систем на предпрофессиональном уровне.
Актуальность	Актуальность программы обусловлена неуклонным повышением значимости безопасной эксплуатации и защиты данных систем от угроз. При этом основная задача состоит не только в обеспечении отказоустойчивости систем, но и в сохранении данных, которые эти системы накапливают и используют. Сегодня компании, правительства и отдельные граждане хранят

	и обрабатывают огромные объемы конфиденциальной информации. Утечка такой информации может привести к серьезным последствиям, поэтому различные отрасли все больше нуждаются в квалифицированных специалистах в области информационной безопасности. Для обеспечения такой безопасности (из-за различной специфики защищаемых объектов) приходится использовать весь арсенал доступных языков и технологий. Однако наиболее распространенным инструментом в этом арсенале является язык программирования Python. Простота синтаксиса, огромное количество готовых библиотек и модулей, опыт сообщества разработчиков, - все это не только позволяет специалистам в области информационной безопасности автоматизировать процессы, связанные с обеспечением безопасности информационных систем, но и обусловливает возможность освоения этого языка для данных целей старшеклассниками и учащимися учреждений среднего профессионального образования. Освоение навыков компьютерной безопасности позволит учащимся эффективно защищать личную информацию и компьютерные системы, расширит общее понимание ими процессов технологического мира, поможет сделать первые шаги к профессии специалиста по информационной безопасности.
Дополнительная информация	**Дополнительная общеобразовательная программа разработана с учетом требований актуальных нормативно-правовых актов:** • Федеральный закон от 29 декабря 2012 г. № 273 «Об образовании в Российской Федерации»; • Приказ Министерства просвещения Российской Федерации от 27 июля 2022 г. № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»; • Приказ Министерства образования и науки Российской Федерации от 23 августа 2017 г. № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных

	образовательных технологий при реализации образовательных программ»; • Постановление Главного государственного санитарного врача Российской Федерации от 28 сентября 2020 г. № 28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодёжи»; • Письмо Министерства просвещения Российской Федерации от 20 марта 2023 г. № 05-848 «О направлении информации» (вместе с Методическими рекомендациями по реализации профориентационного минимума в общеобразовательных организациях Российской Федерации). Общеразвивающий характер программы предполагает, что в рамках образовательной деятельности учащихся решаются три типа задач ***Обучающие:*** • формирование базовых знаний и умений в области программирования на языке Python; • знакомство с механизмами по обеспечению информационной безопасности; • формирование представлений о потенциальных угрозах информационной безопасности, способах их выявления и устранения при использовании информационных систем; • обучение приемам работы со средствами разработки, инструментами анализа сетевого трафика, системами по автоматизации поиска уязвимостей. ***Развивающие:*** • 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 проч.,

	• развитие технических способностей обучающегося, внимания, мышления, памяти, воображения, мотивации к дальнейшему изучению программирования; • развитие творческих способностей. ***Воспитательные:*** • создание условий для формирования готовности к работе в команде для решения учебных задач; • создание условий для формирования у учащихся самостоятельности, ответственности, социальной активности; • создание условия для профессионального самоопределения учащихся.
Формат обучения	Очная форма с применением дистанционных образовательных технологий, в том числе, с применением средств электронного обучения
Уровень сложности	Продвинутый
Срок освоения образовательной программы	148 ак. ч.
Объем каждого модуля в ак.ч.	36
Объем часов в неделю в ак.ч.	4
Количество занятий	116

Направленность программы	Современные языки программирования
Язык программирования	Python
Дополнительная общеобразовательная программа не представлена для участия в иных федеральных проектах, направленных на дополнительное образование граждан, кроме федерального проекта «Развитие кадрового потенциала ИТ- отрасли»	Не представлена
Дополнительная общеобразовательная программа не была реализована до начала отбора и/или не реализовывается в период отбора на безвозмездной основе	Не реализована
Категория обучающихся по программе	Учащиеся 8 класса Учащиеся 9 класса Учащиеся 10 класса Учащиеся 11 класса Обучающиеся по программам среднего профессионального образования
Описание планируемых результатов обучения	В результате освоения программы **Вы будете знать:** • основные принципы работы с декораторами, множественного наследования • понятие дескрипторов • потоки, однопоточное и многопоточное исполнение • параллельное вычисление суммы элементов

	• основы использования GUI в программах • виды графических библиотек для Python • понятие уязвимостей в сетевых протоколах и их классификация • основные уязвимости и способы их эксплуатации, техники анализа уязвимостей, инструменты и программы для анализа уязвимостей • методы защиты от уязвимостей в сетевых протоколах. • автоматизация действий на Python • расширенные методы перехвата и анализа сетевого трафика. • роль сниффинга в сетевых атаках. • принципы работы протокола ARP. • ARP-атаки: ARP-отравление (ARP poisoning) и ARP-перехват (ARP spoofing) • методы обнаружения и предотвращения сетевых атак • основные уязвимости веб-приложений, инструменты и методы обнаружения и эксплуатации уязвимостей веб-приложений • SQL-инъекции, методы защиты от SQL-инъекций; • принципы сессий и механизмов аутентификации, виды атак на сессии • методы безопасной аутентификации, стандарты безопасности связанные с сессиями и аутентификацией; • форензика и судебная экспертиза в контексте информационной безопасности, методы и инструменты форензики, правовые и этические аспекты форензики • социальная инженерия и фишинг, типичные сценарии социальной инженерии, виды фишинга • методы, инструменты и программы для проведения анализа и обхода защиты системы • основные аспекты разработки безопасных приложений и систем **Вы будете уметь:** • использовать принципы работы с декораторами для изменения поведения функций и классов • создавать и использовать генераторы в Python • использовать контекстный менеджер with.

	• создавать базу данных SQLite и таблицы в ней • разрабатывать графические приложения с использованием выбранной библиотеки • анализировать и фильтровать сетевой трафик • разрабатывать программы для перехвата и анализа сетевого трафика; • изучать протокол DNS и его уязвимости • использовать инструменты для сниффинга и проведения ARP-атак. • разрабатывать программы для проведения ARP-атак и анализа сетевого трафика. • настраивать и управлять брандмауэр • разрабатывать программы для настройки VPN-соединения с использованием протокола IPsec. • 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 • разрабатывать методы защиты от социальной инженерии и фишинга • разрабатывать методы защиты от атак и повышения безопасности системы • создавать инструмент на Python для автоматического поиска и эксплуатации уязвимостей • проектировать механизмы аутентификации и авторизации
Ссылка на лендинг Образовательной программы	https://xn----btbkcarrtg5c1as4d.xn--p1ai/programs/security/ethic-exploit
Ссылка на LMS	https://www.odin.study

Страница обучения на курсе	https://www.odin.study/ru/EducationalProgram/Info/7600 (Тестовый доступ. **Логин:** teacher@fortest.ru, **Пароль:** forTest123)

3. Аттестация

Количество академических часов	8
Формы контроля	решение учебной практической задачи
Диагностические инструменты	задание для практической учебной задачи, содержащее пошаговую инструкцию ее выполнения. требуемое время - 2 академических часа
Показатели и критерии оценивания	• учебная задача не выполнена или выполнена с грубыми ошибками (0 баллов) • учебная задача выполнена с подсказкой преподавателя, при этом допущены существенные ошибки в выборе средств и инструментов реализации задания (1 балл) • учебная задача выполнена верно, но с подсказкой преподавателя и наличием ошибок, осложняющие работу пользователя (2 балла) • учебная задача выполнена верно, но с подсказкой преподавателя и наличием ошибок, не осложняющих работу пользователя (3 балла) • учебная задача выполнена верно и без ошибок, но с подсказкой преподавателя (4 балла) • учебная задача выполнена верно без подсказок преподавателя (5 баллов)
Примеры заданий	**Задание для аттестации по модулю 3** Разработать защиту от SQL-инъекций для веб-страницы.

	1. Создайте простую базу данных с использованием SQLite. Определите таблицу "Users" со следующими полями: "ID" (целое число, автоинкремент), "Username" (строка), "Password" (строка). 2. Создайте веб-страницу с формой, где пользователь может ввести имя пользователя и пароль. Убедитесь, что форма отправляет данные на сервер. 3. Напишите серверный код на языке Python, который будет принимать данные из формы и сохранять их в базе данных. Однако, вам необходимо защитить код от SQL-инъекций. 4. Используйте параметризацию запросов или подготовленные выражения для выполнения SQL-запросов в вашем коде. Убедитесь, что данные, введенные пользователем, не вставляются непосредственно в SQL-запросы. 5. Проверьте работоспособность вашей защиты от SQL-инъекций. Попробуйте ввести специальные символы или SQL-код в поля формы и убедитесь, что они не влияют на выполнение SQL-запросов. 6. Напишите краткий отчет о том, как вы защитили ваш код от SQL-инъекций и почему выбрали определенный метод защиты. 7. Дополнительно: Если вы хотите продемонстрировать свои знания еще больше, попробуйте использовать инструмент sqlmap для автоматизированной атаки на свою базу данных. Попытайтесь обнаружить и устранить любые уязвимости, которые могут быть обнаружены. **Задание для аттестации по модулю 4** Генерация фишингового электронного письма 1. Напишите скрипт на языке Python, который будет генерировать фишинговое электронное письмо. 2. Используйте стандартные библиотеки Python для создания HTML-шаблона письма. 3. Включите элементы социальной инженерии в письмо, такие как представление от имени известной организации или создание чрезвычайной ситуации, требующей

	срочных действий от получателя. 4. Сохраните сгенерированное письмо в виде HTML-файла.
Шкала оценивания, нижнее значение	0
Шкала оценивания, верхнее значение	5
Шкала оценивания, минимальный проходной балл	3
ИТОГОВАЯ АТТЕСТАЦИЯ	
Количество академических часов	4
Формы контроля	Защита итогового проекта
Диагностические инструменты	Оценка итогового проекта осуществляется в соответствии с системой критериев. Каждый критерий оценивается по следующим рубрикаторам: • не соответствует критерию (о баллы) • скорее соответствует, чем не соответствует критерию (1 балл) • скорее соответствует, чем не соответствует критерию (2 балла) • полностью соответствует критерию (3 балла) Максимально возможное количество баллов за итоговый проект: 30 баллов В рамках процедуры оценивания технические баллы переводятся в следующую шкалу оценки:

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

4. Преподаватели

ФИО	Наименование основного места работы	Должность	Высшее образование или среднее профессиональ ое образование по направлению «Образование и педагогически	Высшее образование или среднее профессиональное образование по иному направлению соответствующим направленности ДОП	Ссылка на веб-страницы с портфолио	Информация о курсах повышения квалификац ии по профилю преподаваем ой дисципли	Пройдена промежуточная аттестация не менее чем за два года обучения по образовательным программам высшего образования по специальностям и направлениям	Отметка о полученном согласии на обработку персональных данных

			е науки»			**ны (за последние 3 года)**	**подготовки, соответствующим направленности ДОП**	
Бердашкевич Артём Эдуардович	АО «Диалог»	Руководитель направления информационной безопасности	нет	да	https://xn----btbkcarrtg5c1as4d.xn--p1ai/experts/berdashkevich	Программирование Python. Продвинутый уровень, 36 час., ООО Институт Повышения Квалификации и Дополнительного профессионального образования, 2023 г.	нет	да
Лукьянцев Игорь Сергеевич	АО «Диалог»	Специалист по информационной безопасности	нет	да	https://xn----btbkcarrtg5c1as4d.xn--p1ai/experts/lukiantzev	Программирование Python. Продвинутый уровень, 36 час., ООО Институт Повышения Квалификации	нет	да

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

5. Рабочая программа с описанием каждого модуля

Модуль 1. Программирование на Python Данный модуль посвящен изучению специализированных знаний по современному языку программирования Python: основных принципов работы с декораторами; принципов множественного наследования; понятия дескрипторов; потоков, однопоточное и многопоточное исполнение; синхронизацию потоков; параллельных вычислений; основ использования GUI в	**Тема 1.1 Обзор продвинутых возможностей Python**	Генераторы: создание и использование генераторов, выражения-генераторы. Декораторы: основные принципы работы с декораторами, использование декораторов функций и классов. Метаклассы: понятие метаклассов, создание и использование метаклассов. Множественное наследование: принципы множественного наследования, разрешение конфликтов. Дескрипторы: понятие дескрипторов, использование дескрипторов для управления доступом к атрибутам класса.	теоретические занятия	2
		Реализация декоратора timer, который измеряет время выполнения функции и выводит результат в консоль. Создание генератора, который выводит последовательность чисел Фибоначчи до определенного предела.	практические занятия	5

программах; видов графических библиотек для Python. В качестве практики осваиваются навыки использовать принципы работы с декораторами для изменения поведения функций и классов; создавать и использовать генераторы в Python; работать с файлами (открытие, чтение, запись и закрытие файлов в Python); использовать контекстный менеджер with; создавать базу данных SQLite и таблицы в ней; добавлять новую запись в таблицу; создавать и управлять потоками; разрабатывать графические приложения с использованием выбранной библиотеки.		Создание генератора, который выводит последовательность простых чисел до определенного предела.	самостоятельная работа	1
	Тема 1.2 Работа с файлами и базами данных	Работа с файлами: открытие, чтение, запись и закрытие файлов; использование контекстного менеджера with для автоматического закрытия файла; перемещение указателя файла; чтение и запись текстовых и бинарных данных. Работа с базами данных: введение в базы данных, основные понятия (таблицы, поля, записи); подключение к базе данных; выполнение SQL-запросов (создание таблиц, вставка, обновление, удаление данных); чтение данных из базы данных; закрытие соединения с базой данных.	теоретические занятия	2
		Создание файла data.txt и запись в него строк. Чтение содержимого файла data.txt и вывод его в консоль. Создание базы данных SQLite и таблицу users с полями id, name и email.. Добавление новой записи в таблицу users.	практические занятия	5

		Создание таблицы products в базе данных, содержащую поля id, name, price и quantity. Заполнение таблицы несколькими товарами.	самостоятельная работа	1
	Тема 1.3 Многопоточное программирование и параллельные вычисления	Понятие потоков: однопоточное и многопоточное исполнение; преимущества и недостатки многопоточности. Создание и управление потоками: использование модуля threading; создание потоков; запуск и остановка потоков; ожидание завершения потоков. Синхронизация потоков: проблемы совместного доступа к данным; блокировки (Lock); условные переменные (Condition); семафоры (Semaphore); очереди (Queue). Параллельные вычисления: использование модуля multiprocessing; создание и запуск процессов; обмен данными между процессами; пул процессов (Pool); распределенные вычисления.	теоретические занятия	2
		Создание потока, который выводит числа от 1 до 10 с задержкой в 1 секунду между выводом каждого числа. Реализация программы, которая создает 3 потока и каждый поток	практические занятия	5

		выводит свое имя 5 раз.		
		Реализация программы, которая параллельно вычисляет сумму элементов в двух списках и выводит общую сумму. Написание программы, которая создает пул процессов и параллельно считает факториалы чисел от 1 до 10.	самостоятельная работа	1
	Тема 1.4 Разработка интерфейсов с использование м графических библиотек	Основные понятия GUI (графический интерфейс пользователя): окна, виджеты, события. Виды графических библиотек для Python: PyQt, Kivy. Разработка графических приложений с использованием выбранной библиотеки: создание главного окна приложения, размещение виджетов, обработка событий, стилизация интерфейса. Интеграция функциональности: работа с базами данных, файловой системой, сетевыми запросами. Оптимизация и улучшение интерфейса: многопоточность, асинхронные операции, анимация.	теоретические занятия	2

		Разработка приложения с использованием PyQt, которое позволяет пользователю вводить текст в поле ввода и выводит его в метке при нажатии кнопки. Создание интерфейса с использованием Kivy, который отображает список элементов и позволяет пользователю добавлять новые элементы в список.	практические занятия	6
		Разработка графического приложения с использованием выбранной графической библиотеки, которое позволяет пользователю создавать, сохранять и открывать файлы.	самостоятельная работа	2
	Аттестация по итогам модуля	Выполнение учебной практической задачи		2
				Объем в ак.ч. / **Объем в %**
			теоретические занятия	8 / 22
		ИТОГО ПО МОДУЛЮ:	практические занятия	21 / 58
			самостоятельная работа	5 / 14
			аттестация	2
			Всего:	**36**

Модуль 2. Сетевые атаки и защита В данном модуле осуществляется знакомство с понятием уязвимостей в сетевых протоколах и их классификации; с техникой анализа уязвимостей; с инструментами и программами для анализа уязвимостей; с методами защиты от уязвимостей в сетевых протоколах; с автоматизацией действий на Python; с расширенными методами перехвата и анализа сетевого трафика; с с ролью сниффинга в сетевых атаках; с принципами работы протокола ARP; с ARP-атаками; с методами обнаружения и предотвращения сетевых атак. В рамках модуля осваиваются навыки анализировать и фильтровать сетевой трафик; использовать инструменты для	**Тема 2.1 Анализ уязвимостей в сетевых протоколах**	Правовые основы информационной безопасности. Ответственность за противоправные действия. В каких случаях хакинг считается этичным. Международные стандарты, нормы отечественного законодательства (PCI DSS, 149-ФЗ, 187-ФЗ, 152-ФЗ). Как организована деятельность этичного хакера и как тренировать навыки информационной безопасности не нарушая закон. Понятие уязвимости в сетевых протоколах и их классификация. Техники анализа уязвимостей: сканирование портов, перехват и анализ сетевого трафика, исследование уязвимостей конкретных протоколов. Инструменты и программы для анализа уязвимостей: Nmap, Wireshark, Nessus, Metasploit. Понимание основных уязвимостей и способов их эксплуатации: отказ в обслуживании (DoS), переполнение буфера, подделка данных, атаки на протоколы аутентификации. Методы защиты от уязвимостей в сетевых протоколах: обновление программного обеспечения, настройка брандмауэра, использование шифрования, применение протоколов безопасности.	теоретические занятия	2

сниффинга и проведения ARP-атак; разрабатывать программ для проведения ARP-атак и анализа сетевого трафика; настраивать и управлять брандмауэром; разрабатывать программы для настройки VPN-соединения с использованием протокола IPsec; разрабатывать программы для фильтрации сетевого трафика на основе правил доступа.		Использование инструмента Nmap, для выполнения сканирования портов в локальной сети и нахождение открытых портов на определенных узлах. Перехват и анализ сетевого трафика для протокола HTTP и извлечение полезной информации, такой как заголовки запросов и ответов. Автоматизация приведенных действий на Python в контексте информационной безопасности. Правовые аспекты использования этих инструментов	практические занятия	5
		Написание программы на Python, которая сканирует указанный диапазон IP-адресов и определяет открытые порты и доступные сервисы на каждом узле	самостоятельная работа	1
	Тема 2.2 Продвинутые методы перехвата и анализа трафика	Обеспечение информационной безопасности и расширенные методы перехвата и анализа сетевого трафика. Использование снифферов для перехвата пакетов на сетевом уровне. Изучение протоколов на прикладном уровне: HTTP, FTP, DNS, SMTP. Анализ и фильтрация сетевого трафика с использованием специализированных инструментов, таких как Wireshark или tcpdump. Распознавание и анализ	теоретические занятия	2

		зашифрованного трафика с применением SSL/TLS. Идентификация и анализ сетевых атак, включая атаки типа Man-in-the-Middle, ARP-отравление, DNS-отравление.		
		Реализация программы, которая перехватывает сетевой трафик на локальной машине и ищет подозрительную активность, такую как повышенное количество запросов на определенный порт или аномальный размер пакетов. Перехват зашифрованного сетевого трафика с использованием протокола HTTPS и анализ передаваемых данных в открытом виде, используя инструмент sslstrip, в контексте информационной безопасности. Правовые аспекты	практические занятия	5
		Изучение протокола DNS (Domain Name System) и его уязвимостей. Написание программы, которая перехватывает DNS-запросы и анализирует их содержимое, выявляя подозрительные запросы или изменения DNS-ответов.	самостоятельная работа	1

	Тема 2.3 Сниффинг и ARP-атаки	Сниффинг и обеспечение информационной безопасности. Роль сниффинга в сетевых атаках. Принципы работы ARP (Address Resolution Protocol) и его уязвимости. ARP-атаки, включая ARP-отравление (ARP poisoning) и ARP-перехват (ARP spoofing). Использование инструментов для сниффинга и проведения ARP-атак. Защитные меры от ARP-атак и обнаружение подмененных ARP-записей. Вопросы правомерности и этичности.	теоретические занятия	2
		Для понимания сути обеспечения информационной безопасности, разработка программы, которая проводит ARP-отравление в локальной сети, подменяя MAC-адреса между двумя узлами. Вывод информации о перехватываемых пакетах и измененных ARP-записях. Написание программы, которая перехватывает и анализирует сетевой трафик в локальной сети, используя инструмент scapy. Вывод информации о принятых пакетах, идентификация ARP-пакетов и определение изменений в ARP-таблице. Вопросы правомерности и этичности действий.	практические занятия	5

		Разработка инструмента для мониторинга ARP-таблицы и обнаружения подмененных записей. Программа должна регулярно сканировать ARP-таблицу и оповещать администратора о возможной подмене MAC-адресов.	самостоятельная работа	1
	Тема 2.4 Противодействие атакам и защита сетевых ресурсов	Основные принципы защиты сетевых ресурсов. Методы обнаружения и предотвращения сетевых атак, включая брандмауэры, системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS). Защита от атак типа отказ в обслуживании (DoS) и распределенных атак отказа в обслуживании (DDoS). Использование сетевых политик и фильтров для ограничения доступа к сетевым ресурсам. Протоколы безопасности, такие как IPsec и SSL/TLS, для защиты сетевых коммуникаций.	теоретические занятия	2
		Написание программы для настройки и управления брандмауэром на компьютере. Реализация возможности блокировки входящего и исходящего сетевого трафика на основе определенных правил. Создание программы, которая настраивает VPN-	практические занятия	6

		соединение с использованием протокола IPsec. Программа должна запрашивать необходимые параметры (адрес сервера VPN, аутентификационные данные и т. д.) и устанавливать защищенное соединение.		
		Разработка программы для фильтрации сетевого трафика на основе определенных правил. Программа должна позволять настраивать правила доступа для различных IP-адресов, портов и протоколов.	самостоятельная работа	2
	Аттестация по итогам модуля	Выполнение учебной практической задачи		2
				Объем в ак.ч. / **Объем в %**
			ИТОГО ПО МОДУЛЮ: теоретические занятия	8 / 22
			практические занятия	21 / 58
			самостоятельная работа	5 / 14
			аттестация	2
			Всего:	**36**

Модуль 3. Веб-приложения и безопасность В данном модуле в фокусе внимания - веб-приложения. Изучаются основные уязвимости веб-приложений; инструменты и методы обнаружения и эксплуатации уязвимостей веб-приложений; SQL-инъекции; методы защиты от SQL-инъекций; принципы сессий и механизмов аутентификации; виды атак на сессии; методы безопасной аутентификации; стандарты безопасности, связанные с сессиями и аутентификацией; основные методы защиты от атак. Осваиваются навыки разрабатывать скрипты на Python для поиска и эксплуатации уязвимостей; разрабатывать систему фильтрации и санитизации пользовательского ввода;	**Тема 3.1 Уязвимости веб-приложений и их эксплуатация**	Информационная безопасность и уязвимость веб-приложений. Обзор основных уязвимостей веб-приложений, таких как инъекции SQL, кросс-сайтовый скриптинг (XSS), кросс-сайтовая подделка запроса (CSRF). Механизмы эксплуатации уязвимостей, включая получение несанкционированного доступа к данным, выполнение произвольного кода и подмену сеансов. Понятие белого и черного ящиков в контексте анализа уязвимостей. Инструменты и методы для обнаружения и эксплуатации уязвимостей веб-приложений, включая сканеры уязвимостей и прокси-серверы для перехвата и изменения трафика. Правовые аспекты.	теоретические занятия	2
		Разработка скрипта на Python для автоматизированного поиска уязвимостей XSS на веб-сайте. Написание программы для эксплуатации уязвимости SQL-инъекции на веб-сайте.	практические занятия	5
		Разработка системы фильтрации и санитизации пользовательского ввода для защиты от уязвимостей XSS. Создание модуля, который будет	самостоятельная работа	1

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		проверять и очищать входные данные от потенциально опасных символов и скриптов перед их выводом на веб-страницу.		
	Тема 3.2 SQL-инъекции и защита баз данных	Обзор SQL-инъекций и их принципов работы. Различные типы SQL-инъекций, включая ошибки в SQL-синтаксисе, временные задержки и возвращение ошибок, бандл-инъекции и многое другое. Практические методы защиты от SQL-инъекций, такие как параметризация запросов, использование подготовленных выражений, ограничение прав доступа к базе данных и правильное санитизация и валидация пользовательского ввода.	теоретические занятия	2
		Создание простой базы данных с использованием SQLite и разработка программы на Python, которая позволит пользователям выполнять запросы к базе данных. Защита запросов от SQL-инъекций, используя параметризацию и подготовленные выражения.	практические занятия	5
		Анализ кода веб-приложения и выявление уязвимости SQL-инъекций. Попытка эксплуатации этих уязвимостей. Предложения по	самостоятельная работа	1

		реализации мер по устранению этих уязвимостей.		
	Тема 3.3 Атаки на сессии и механизмы аутентификации	Основные принципы сессий и механизмов аутентификации в веб-приложениях. Сессии используются для установления и поддержания состояния между взаимодействиями клиента и сервера, а механизмы аутентификации проверяют подлинность пользователей. Различные виды атак на сессии, такие как перехват сессионных данных, подмена и подбор идентификаторов сессий, фиксация сессии и многое другое. Принципы безопасной аутентификации, включая использование сильных паролей, двухфакторной аутентификации, ограничение попыток входа и другие меры.	теоретические занятия	2
		Разработка простой системы аутентификации на основе сессий веб-приложения с использованием фреймворка Flask. Защита сессионных данных от перехвата путем использования шифрования и подписи сессионных файлов. Изучение различных методов безопасной аутентификации, такие как	практические занятия	5

		двухфакторная аутентификация, включая использование одноразовых паролей или мобильных приложений аутентификации.		
		Изучение стандартов безопасности, связанных с сессиями и аутентификацией в веб-приложениях, таких как OWASP Top 10.	самостоятельная работа	1
	Тема 3.4 Защита веб-приложений и противодействие атакам	Основные методы защиты веб-приложений от атак, включая защиту от инъекций, кросс-сайтового скриптинга (XSS), подделки запросов межсайтовой подделки (CSRF) и других распространенных уязвимостей. Использование валидации данных и фильтрации входных параметров для предотвращения инъекций, таких как SQL-инъекции и командные инъекции. Применение контрмер CSRF, таких как генерация и проверка токенов CSRF при выполнении запросов, а также использование HTTP-заголовков, таких как SameSite и X-Frame-Options. Защита от XSS-атак путем эскейпинга и санитизации пользовательского ввода, а также использование контекстуальной безопасности при вставке данных в HTML-страницы.	теоретические занятия	2

		Разработка веб-приложения с использованием фреймворка Django и применение необходимых меры безопасности для защиты от инъекций и XSS-атак. Включение валидации и фильтрации данных, проверки типов и длины параметров, использование безопасных ORM-запросов и эскейпинг или санитизации пользовательского ввода при отображении на странице.	практические занятия	6
		Изучение стандартов и рекомендаций по безопасности веб-приложений, таких как OWASP Top 10 и CWE/SANS Top 25 Most Dangerous Software Errors. Составление отчета о наиболее важных мероприятиях по защите веб-приложений и противодействию распространенным атакам.	самостоятельная работа	2
	Аттестация по итогам модуля	Выполнение учебной практической задачи		2
			Объем в ак.ч.	**Объем в %**
		ИТОГО ПО МОДУЛЮ:	теоретические занятия	8	22
			практические занятия	21	58
			самостоятельная работа	5	14

			аттестация	2
			Всего:	**36**
Модуль 4. Продвинутые методы этичного хакинга Этот модуль посвящен освоению методов и инструментов, правовых и этических аспектов форензики; социальной инженерии и фишинга; типичных сценариев социальной инженерии; видов фишинга; методов анализа и обхода защиты системы; инструментов и программ для проведения анализа и обхода защиты системы; принципов безопасного проектирования систем; основных аспектов разработки безопасных приложений и систем. В качестве практических навыков осваивается практики создавать отчеты	**Тема 4.1 Форензика и судебная экспертиза**	Определение форензики и судебной экспертизы в контексте информационной безопасности. Роль форензики в обнаружении, сборе и анализе цифровых доказательств, связанных с компьютерными преступлениями. Применение методов и инструментов форензики для извлечения данных, восстановления удаленных файлов, анализа системных журналов и метаданных, а также идентификации следов деятельности злоумышленников. Правовые и этические аспекты форензики и предоставления цифровых доказательств в судебном процессе.	теоретические занятия	2
		Создание отчета об анализе цифровых доказательств. Рассмотрение конкретного случая компьютерного преступления и разработка детального отчета, включающего информацию о методах анализа, найденных следах и рекомендации по предотвращению подобных	практические занятия	5

об анализе цифровых доказательств; составлять планы действий и процедур в случае инцидентов информационной безопасности; разрабатывать методы защиты от социальной инженерии и фишинга; разрабатывать методы защиты от атак и повышения безопасности системы; создавать инструмент на Python для автоматического поиска и эксплуатации уязвимостей; проектировать механизмы аутентификации и авторизации		инцидентов.		
		Составление плана действий и процедур для проведения анализа в случае инцидента информационной безопасности, такого как взлом системы или утечка данных. Описание шагов, которые необходимо выполнить для сбора и анализа цифровых доказательств, а также для восстановления нормальной работы системы.	самостоятельная работа	1
	Тема 4.2 Социальная инженерия и фишинг	Определение социальной инженерии и фишинга в контексте информационной безопасности. Понимание принципов и методов социальной инженерии, которые используются для манипуляции людьми и получения конфиденциальной информации. Анализ типичных сценариев социальной инженерии, включая подборка информации, маскировку под легитимные лица, создание чрезвычайных ситуаций и другие тактики. Изучение различных видов фишинга, включая письма-	теоретические занятия	2

		перехватчики, фишинговые сайты, фишинговые звонки и другие формы атак. Разработка методов защиты от социальной инженерии и фишинга, включая обучение сотрудников, использование технических мер безопасности и мониторинг подозрительной активности.		
		С целью понимания механизмов действия злоумышленников для их предотвращения и обеспечения информационной безопасности, написание скрипта на Python для генерации фишингового электронного письма. Включение в письмо элементов социальной инженерии, например, представление от имени известной организации или создание чрезвычайной ситуации, требующей срочных действий от получателя. Сохранение сгенерированного письма в виде HTML-файла и отправка его себе.	практические занятия	5
		Разработка уроков для сотрудников компании, которые включают презентации и задания для проверки знаний по противодействию атакам социальной инженерии.	самостоятельная работа	1

	Тема 3.3 Анализ и обход защиты системы	Обзор методов анализа и обхода защиты системы с целью выявления уязвимостей и повышения безопасности. Изучение различных типов атак, включая брутфорс, словарные атаки, обход аутентификации и другие техники. Ознакомление с инструментами и программами, используемыми для проведения анализа и обхода защиты системы. Разработка методов защиты от атак и повышения безопасности системы.	теоретические занятия	2
		Разработка инструмента на Python, используя библиотеку Metasploit, для автоматического поиска и эксплуатации уязвимостей в системе. Создание скрипта для обхода аутентификации на веб-сайте путем перебора пользовательских и паролей, используя библиотеку requests.	практические занятия	5
		Создание собственной уязвимой системы и тестирование ее на безопасность с использованием различных изученных методов и инструментов.	самостоятельная работа	1

	Тема 4.4 Проектирование и реализация безопасных систем	Принципы безопасного проектирования систем, включая защиту от атак и уязвимостей. Основные аспекты разработки безопасных приложений и систем. Проектирование механизмов аутентификации и авторизации. Реализация механизмов шифрования и обеспечения конфиденциальности данных.	теоретические занятия	2	
		Разработка системы управления пользователями, которая обеспечивает безопасность паролей, храня их в хэшированном виде. Создание приложения для обмена зашифрованными сообщениями между пользователями с использованием асимметричного шифрования.	практические занятия	6	
		Разработка механизм безопасной передачи файлов по сети, используя протокол SSH и симметричное шифрование.	самостоятельная работа	2	
	Аттестация по итогам модуля	Выполнение учебной практической задачи		2	
				Объем в ак.ч.	**Объем в %**

ИТОГО ПО МОДУЛЮ:	теоретические занятия	8	22
	практические занятия	21	58
	самостоятельная работа	5	14
	аттестация	2	
	Всего:	**36**	
ИТОГОВАЯ АТТЕСТАЦИЯ (защита итогового проекта)		**4**	
		Объем в ак.ч.	**Объем в %**
ИТОГО ПО ПРОГРАММЕ:	теоретические занятия	32	22
	практические занятия	84	57
	самостоятельная работа	20	13
	аттестация	12	
	Всего:	148	

6. Календарно-тематическое планирование

№	Тема и № модуля	Тема занятия	Кол-во занятий*	Кол-во часов	Дата
1	Модуль 1. Программирование на Python	Тема 1.1 Обзор продвинутых возможностей Python	7	2 2 2 2	29.10.2023 05.10.2023 09.10.2023 12.10.2023
2		Тема 1.2 Работа с файлами и базами данных	7	2 2 2 2	16.10.2023 19.10.2023 23.10.2023 26.10.2023
3		Тема 1.3 Многопоточное программирование и параллельные вычисления	7	2 2 2 2	30.10.2023 02.11.2023 06.11.2023 09.11.2023
4		Тема 1.4 Разработка интерфейсов с использованием графических библиотек	8	2 2 2 4	13.11.2023 16.11.2023 20.11.2023 23.11.2023
5	Аттестация			2	27.11.2023
6	Модуль 2. Сетевые атаки и защита	Тема 2.1 Анализ уязвимостей в сетевых протоколах	7	2 2 2 2	30.11.2023 04.12.2023 07.12.2023 11.12.2023
7		Тема 2.2 Продвинутые методы перехвата и анализа трафика	7	2 2 2 2	14.12.2023 18.12.2023 21.12.2023 25.12.2023

8		Тема 2.3 Сниффинг и ARP-атаки	7	2 2 4	28.12.2023 11.01.2024 16.01.2024
9		Тема 2.4 Противодействие атакам и защита сетевых ресурсов	8	2 2 2 4	18.01.2024 22.01.2024 23.01.2024 25.01.2024
10	Аттестация			2	29.01.2024
11	Модуль 3. Веб-приложения и безопасность	Тема 3.1 Уязвимости веб-приложений и их эксплуатация	7	2 2 2 2	01.02.2024 05.02.2024 08.02.2024 12.02.2024
12		Тема 3.2 SQL-инъекции и защита баз данных	7	2 2 2 2	15.02.2024 19.02.2024 22.02.2024 26.02.2024
13		Тема 3.3 Атаки на сессии и механизмы аутентификации	7	2 2 2 2	29.02.2024 04.03.2024 06.03.2024 11.03.2024
14		Тема 3.4 Защита веб-приложений и противодействие атакам	8	2 2 2 2 2	14.03.2024 18.03.2024 21.03.2024 25.03.2024 28.03.2024
15	Аттестация			2	29.03.2024

16	Модуль 4. Продвинутые методы этичного хакинга	Тема 4.1 Форензика и судебная экспертиза	7	2 2 2 2	01.04.2024 04.04.2024 08.04.2024 11.04.2024
17		Тема 4.2 Социальная инженерия и фишинг	7	2 2 2 2	15.04.2024 18.04.2024 22.04.2024 25.04.2024
18		Тема 3.3 Анализ и обход защиты системы	7	2 2 4	29.04.2024 06.05.2024 13.05.2024
19		Тема 4.4 Проектирование и реализация безопасных систем	8	2 4 4	16.05.2024 20.05.2024 23.05.2024
20	Аттестация			2	27.05.2024
21	Итоговая аттестация			4	30.05.2024

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

7. Учебно-методические материалы

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

Методы, формы и технологии	Образовательная деятельность учащихся предусматривает следующие виды учебных занятий: лекции, практические занятия и самостоятельную работу, определенные учебным планом. При реализации Программы используются групповая и фронтальная формы организации учебного процесса, различные образовательные технологии: технология «перевернутого класса», геймификация, технология проектного обучения, онлайн-конференция.	Образовательная деятельность учащихся предусматривает следующие виды учебных занятий: лекции, практические занятия и самостоятельную работу, определенные учебным планом. При реализации Программы используются групповая и фронтальная формы организации учебного процесса, различные образовательные технологии: технология «перевернутого класса», геймификация, технология проектного обучения, онлайн-конференция.	Образовательная деятельность учащихся предусматривает следующие виды учебных занятий: лекции, практические занятия и самостоятельную работу, определенные учебным планом. При реализации Программы используются групповая и фронтальная формы организации учебного процесса, различные образовательные технологии: технология «перевернутого класса», геймификация, технология проектного обучения, онлайн-конференция.	Образовательная деятельность учащихся предусматривает следующие виды учебных занятий: лекции, практические занятия и самостоятельную работу, определенные учебным планом. При реализации Программы используются групповая и фронтальная формы организации учебного процесса, различные образовательные технологии: технология «перевернутого класса», геймификация, технология проектного обучения, онлайн-конференция.
Методические разработки	реализация модуля предусматривает авторские разработки лекционных материалов (рабочих листов, презентаций,	реализация модуля предусматривает авторские разработки лекционных материалов (рабочих листов, презентаций,	реализация модуля предусматривает авторские разработки лекционных материалов (рабочих листов, презентаций,	реализация модуля предусматривает авторские разработки лекционных материалов (рабочих листов, презентаций,

	конспектов); заданий, видеоинструкций, скринкастов, гайдов для организации и реализации практических занятий и самостоятельной работы.	конспектов); заданий, видеоинструкций, скринкастов, гайдов для организации и реализации практических занятий и самостоятельной работы.	конспектов); заданий, видеоинструкций, скринкастов, гайдов для организации и реализации практических занятий и самостоятельной работы.	конспектов); заданий, видеоинструкций, скринкастов, гайдов для организации и реализации практических занятий и самостоятельной работы.
Материалы модуля	материалы модуля - это учебно-методическое обеспечение освоения программы, размещенное в LMS: презентации и конспекты лекции, записи эфиров лекционных занятий, видеоролики, задания для практикумов с пошаговыми инструкциями, видеоинструкциями и скринкастами, критериями для формирующего оценивания; задания, инструкции, видеоинструкции для самостоятельной работы учащихся, критерии качества	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	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	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	работы, тестовые задания для промежуточного контроля и итоговой аттестации, список основной и дополнительной литературы, электронных информационных и образовательных ресурсов по теме модуля	работы, тестовые задания для промежуточного контроля и итоговой аттестации, список основной и дополнительной литературы, электронных информационных и образовательных ресурсов по теме модуля	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	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	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	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.,

	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.	/ 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»).	"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»).	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»).

8. Материально-технические условия реализации программы

Наименование поля	Значение полей	Значение полей	Значение полей	Значение полей

Порядковый номер модуля	1	2	3	4
Наименование требуемого оборудования	Компьютер или ноутбук со свободным объемом на жестком диске 30+ Гб. CPU: от 2,2 Мгц, Оперативная память: от 4Гб; Выход в интернет со скоростью 2+ мбит/сек	Компьютер или ноутбук со свободным объемом на жестком диске 30+ Гб. CPU: от 2,2 Мгц, Оперативная память: от 4Гб; Выход в интернет со скоростью 2+ мбит/сек	Компьютер или ноутбук со свободным объемом на жестком диске 30+ Гб. CPU: от 2,2 Мгц, Оперативная память: от 4Гб; Выход в интернет со скоростью 2+ мбит/сек	Компьютер или ноутбук со свободным объемом на жестком диске 30+ Гб. CPU: от 2,2 Мгц, Оперативная память: от 4Гб; Выход в интернет со скоростью 2+ мбит/сек
Наименование требуемого программного обеспечения	Операционная система Windows/MacOS Интерпретатор Python, интегрированная среда разработки (IDE), библиотеки Python, браузер для работы с веб-приложениями, ПО Oracle Virtualbox или VMware Workstation для работы с виртуальными машинами, дистрибутивы Linux (bWAPP, DVWA, Kali Linux) Любой браузер	Операционная система Windows/MacOS Интерпретатор Python, интегрированная среда разработки (IDE), библиотеки Python, браузер для работы с веб-приложениями, ПО Oracle Virtualbox или VMware Workstation для работы с виртуальными машинами, дистрибутивы Linux (bWAPP, DVWA, Kali Linux) Любой браузер	Операционная система Windows/MacOS Интерпретатор Python, интегрированная среда разработки (IDE), библиотеки Python, браузер для работы с веб-приложениями, ПО Oracle Virtualbox или VMware Workstation для работы с виртуальными машинами, дистрибутивы Linux (bWAPP, DVWA, Kali Linux) Любой браузер	Операционная система Windows/MacOS Интерпретатор Python, интегрированная среда разработки (IDE), библиотеки Python, браузер для работы с веб-приложениями, ПО Oracle Virtualbox или VMware Workstation для работы с виртуальными машинами, дистрибутивы Linux (bWAPP, DVWA, Kali Linux) Любой браузер
Электронные информационные ресурсы	Selectel — ведущий в России провайдер облачной инфраструктуры и услуг дата-центров.	Selectel — ведущий в России провайдер облачной инфраструктуры и услуг дата-центров.	Перехват и анализ сетевого трафика. Общество с ограниченной	Лучшие дистрибутивы для тестирования на проникновение. АО "Синклит" Официальный

	Общество с ограниченной ответственностью «Сеть дата-центров «Селектел» Официальный сайт - URL: https://selectel.ru Санкт-Петербург, (дата обращения: 14.06.2023) - 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: 14.06.2023) - Текст: электронный. Сбер — крупнейший банк в России. Сбертех, АО Официальный сайт - URL: https://sbertech.ru/ Санкт-Петербург, (дата обращения: 14.06.2023) - Текст: электронный. Лучшие книги по Python 2021-2022 года: для	Общество с ограниченной ответственностью «Сеть дата-центров «Селектел» Официальный сайт - URL: https://selectel.ru Санкт-Петербург, (дата обращения: 14.06.2023) - 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: 14.06.2023) - 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: 14.06.2023) - Текст: электронный.	ответственностью "Аудит-Новые Технологии" Официальный сайт - URL: https://newtechaudit.ru/ Санкт-Петербург, (дата обращения: 14.06.2023) - 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: 14.06.2023) - Текст: электронный.	сайт - URL: https://owasp.org/www-chapter-moscow/.- Москва, (дата обращения: 14.06.2023) - 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: 14.06.2023) - Текст: электронный.

	новичков и профи. Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/companies/sberbank/articles/679852/ (дата обращения: 14.06.2023) - 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: 14.06.2023) - 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: 14.06.2023) - Текст: электронный. Отмена пользовательских паролей. Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/compani		

		es/selectel/articles/112794/ (дата обращения: 14.06.2023) - Текст: электронный.		
Электронные образовательные ресурсы	Сайт pythonchik.ru — обучение основам Python - Москва. - URL: https://pythonchik.ru/osnovy/_(дата обращения: 14.06.2023) - Текст: электронный. Простым языком об HTTP. Блог о кибербезопасности "Habr". Positive Technologies: официальный сайт. - Москва. - URL: https://habr.com/ru/post/215117/(дата обращения: 13.06.2023) - 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: 13.06.2023) - Текст: электронный. Практическое задание в Cisco Packet Tracer. http://ncti.ru/files/studentu/Olimpiada/zadanie_II_.pdf (дата обращения: 13.06.2023) - Текст: электронный. Easy-Network - обучающий курс по сетевым технологиям. Лабораторные работы по Cisco CCNA. URL: https://easy-network.ru/zadaniya.html (дата обращения: 13.06.2023) - Текст: электронный.	PortSwigger: официальный сайт. - URL: https://portswigger.net/web-security (дата обращения: 14.06.2023) - Текст: электронный. TryHackMe - тренинг по кибербезопасности: официальный сайт. - Лондон. - URL: https://tryhackme.com/(дата обращения: 13.06.2023) - Текст: электронный. HACKTHEBOX URL: https://www.hackthebox.com/_(дата обращения: 13.06.2023) - Текст: электронный.	TryHackMe - тренинг по кибербезопасности: официальный сайт. - Лондон. - URL: https://tryhackme.com/(дата обращения: 14.06.2023) - Текст: электронный. Блог “NetSkills” URL: http://blog.netskills.ru/ (дата обращения: 14.06.2023) - Текст: электронный.

		Форум информационной безопасности - CODEBY.NET. URL: https://codeby.net/threads/cisco-ccna-1-2019-zadanija-v-cisco-packet-tracer.69507/ (дата обращения: 13.06.2023) - Текст: электронный.		