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 №11п/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: надень «белую шляпу»

(148 акад. час.)

Автор-составитель:

Сойманова Светлана Викторовна, методист

г. Санкт-Петербург, 2023 г.

Дополнительная общеобразовательная общеразвивающая программа технической направленности

«Этичный хакинг на Python: надень «белую шляпу»

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: надень "белую шляпу"
Описание программы	Язык программирования Python сегодня весьма популярен. Использование его для обеспечения информационной безопасности является перспективным IT направлением в условиях современных реалий цифровой экономики. Этичный хакинг - это выстраивание эффективной защиты на основе глубинного понимания методов и инструментов действиям злоумышленников. Специалисты по кибербезопасности (этичные хакеры) моделируют взломы систем безопасности, проводят тесты на уязвимости, придумывают новые способы проверки и защиты, используя для этого язык программирования Python.

	Данная программа поможет школьникам попробовать себя в роли этичного хакера, позволит научиться использовать язык программирования Python для решения различных задач обеспечения информационной безопасности, поможет в профессиональном самоопределении относительно профессии специалиста по информационной безопасности. Обучаться по этой программе могут учащиеся 8-11 классов, владеющие основами программирования (умение писать простые программы на любом языке программирования), основами логики, знающие основные функции и команды операционной системы (например, Windows или Linux), умеющие устанавливать программы и работать с файловой системой, знающие основные принципы работы сетей. 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 специализированные знания и умения языка программирования Python, и научатся его применять в целях обеспечения информационной безопасности

Аннотация программы	Программа «Этичный хакинг на Python: надень «белую шляпу» разработана в рамках проекта «Код будущего». **#Этичный хакинг#Хакинг#Информационная безопасность#Защита данных** Программа имеет техническую направленность и адресована учащимся 8–11 классов, владеющим основами программирования, заинтересованным в изучении языка программирования Python, и в его применении для предотвращения угроз информационной безопасности. Для освоения программы необходимы: базовые умения программирования на любом языке, знание основные функций и команд операционной системы (Windows или Linux), умение устанавливать программы и работать с файловой системой, знать основные принципы работы сетей. Почти 57 % учебного времени отводится на отработку практических навыков и умений. В результате обучения участники программы углубят свои навыки программирования, освоят умения разработки на языке Python, научатся использовать этот язык программирования для защиты информационных систем от кибератак.
Цель программы	Освоение специализированных знаний и умений в области программирования на языке Python для обеспечения информационной безопасности и поиска уязвимостей информационных систем.
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. Освоение навыков компьютерной безопасности позволит учащимся эффективно защищать личную информацию и компьютерные системы, расширит общее понимание ими процессов технологического мира, поможет в профессиональном самоопределении.
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 школьников 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 школьников.
Формат обучения	Очная форма с применением дистанционных образовательных технологий, в том числе, с применением средств электронного обучения
Уровень сложности	Базовый
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: • основы синтаксиса Python • понимание операторов и выражений • условные выражения и операторы, циклы и структуры данных • встроенные функции Python • сущность этичного хакинга и его отличий от нелегальных действий. • виды хакерских атак и их классификации • сертификации в области этичного хакинга • основные методы и инструменты сбора информации и разведки. • принципы и методы анализа уязвимостей, инструменты для обнаружения уязвимостей • принципы эксплуатации и защиты от атак, методы обнаружения атак • основные понятия и протоколы сетевого взаимодействия: IP, TCP, UDP, HTTP, HTTPS.

	• основы анализа сетевого трафика и его роли в обеспечении безопасности • методы защиты сети, методы защиты от DDoS-атак • принципы работы систем IDS и IPS • основные угрозы безопасности Wi-Fi сетей, методы защиты Wi-Fi сетей, виды шифрования Wi-Fi • основные компоненты веб-приложений, методы защиты веб-приложений • протоколы передачи данных в вебе: HTTP и HTTPS • основные уязвимости веб-приложений и методы их защиты • кросс-сайтовый скриптинг (XSS) и его основные принципы работы • типы XSS-атак и их потенциальные последствия, методы предотвращения XSS-атак • инъекции и уязвимости баз данных, методы предотвращения инъекций Вы будете уметь: • писать простые программы с использованием основных синтаксических конструкций языка Python • создавать функции таблицы умножения • работать со списками и модулями • создавать модули math_operations.py, string_operations.py • обрабатывать исключения, работать с путями файлов • писать программы для чтения и записи файлов • разрабатывать скрипты для проверки безопасности сети на языке программирования Python • писать программы на Python для извлечения информации о домене • писать программы на Python для сканирования уязвимостей сети. • использовать инструменты, разрабатывать программы для эксплуатации и защиты • разрабатывать клиент-серверное приложение на Python с использованием TCP протокола • разрабатывать программы на Python для сканирования сети и определения активных устройств • работать с инструментами анализа сетевого трафика, в частности с программой

	Wireshark. • писать программы на Python с использованием библиотеки pcapy для анализа сетевого трафика • писать программы на Python для симуляции фаервола • писать программы на Python для сканирования Wi-Fi сетей и проведения аудита безопасности • проводить исследования безопасности Wi-Fi сети и писать отчет • разрабатывать веб-приложения с использованием фреймворка Flask на Python • разрабатывать и веб-страниц с уязвимостью к XSS-атаке • исследовать различные типы XSS-атак и разрабатывать демонстрационные страницы • разрабатывать веб-страницы с уязвимостью к инъекциям. • разрабатывать и осуществлять аудит безопасности веб-приложений
Ссылка на лендинг Образовательной программы	https://xn----btbkcarrtg5c1as4d.xn--p1ai/programs/security/ethic-whitecap
Ссылка на LMS	https://www.odin.study
Страница обучения на курсе	https://www.odin.study/ru/EducationalProgram/Info/7601 (Тестовый доступ. **Логин:** teacher@fortest.ru, **Пароль:** forTest123)

3. Аттестация

Количество академических часов	8
Формы контроля	решение учебной практической задачи

Диагностические инструменты	задание для практико-ориентированной 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	**Итоговое задание к модулю 2** Разработка программы для сканирования уязвимостей сети 1. Напишите программу на Python, используя библиотеку Scapy, для сканирования уязвимостей сети. Программа должна выполнять следующие действия: • Запросить у пользователя ввод IP-адреса или диапазона IP-адресов для сканирования. • Создать сетевые пакеты, содержащие запросы на определенные службы или устройства, которые часто становятся объектами атак или имеют известные уязвимости. • Отправить созданные пакеты на указанные IP-адреса с использованием библиотеки Scapy. • Анализировать полученные ответы на наличие уязвимостей или нежелательных состояний. 2. Реализуйте функционал для идентификации уязвимых устройств или служб. Вы можете

	использовать известные уязвимости и популярные службы, такие как открытые порты, службы с известными уязвимостями, настройки безопасности и другие показатели. 3. Предоставьте информацию о найденных уязвимостях в удобном формате. Включите в отчет информацию о найденных уязвимых устройствах или службах, их типе, версии, описании уязвимости и рекомендации по устранению уязвимости или повышению безопасности. 4. Протестируйте программу, запустив ее на реальной или виртуальной сети и проверив ее работу на наличие уязвимостей. **Итоговое задание к модулю 3** Анализ сетевого трафика с использованием библиотеки pcapy 1. Установите библиотеку pcapy на свой компьютер. 2. Напишите программу на Python, которая будет анализировать сетевой трафик, захватываемый с помощью библиотеки pcapy. 3. Программа должна запрашивать у пользователя имя сетевого интерфейса для захвата трафика. 4. Захватите сетевой трафик в течение определенного времени (например, 30 секунд). 5. Выведите информацию о каждом захваченном пакете, включая протокол, IP-адрес отправителя и получателя, порты и другие параметры, которые считаете важными.
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 (0 баллов) • скорее соответствует, чем не соответствует критерию (1 балл) • скорее соответствует, чем не соответствует критерию (2 балла) • полностью соответствует критерию (3 балла) Максимально возможное количество баллов за итоговый проект: 30 баллов В рамках процедуры оценивания технические баллы переводятся в следующую шкалу оценки: от 0% до 50% (0-15 баллов) – не зачтено от 51% до 100% (16-30 баллов) - зачтено
Показатели и критерии оценивания	1. Владение технологиями показано на уровне реализаций проектов подобных типов 2. Проект выполнен в соответствии с современными подходами в заявленной тематической области 3. Проект выполнен самостоятельно, без содержательной помощи преподавателя 4. В проекте корректно используется язык программирования Python 5. Требования к стилю кода соблюдены 6. Графические элементы интерфейса отображаются корректно, текстовые элементы не содержат языковых ошибок 7. Используются оптимальные алгоритмы и структура базы данных, а также оптимальные запросы к базе данных

	8. Терминология соответствует решаемой проблеме и используется правильно 9. Интерфейс интуитивно понятен пользователям, удобен в использовании 10. Проект выполнен и представлен на проверку с соблюдением дедлайна

4. Преподаватели

ФИО	Наименование основного места работы	Должность	Высшее образование или среднее профессиональное образование по направлению «Образование и педагогические науки»	Высшее образование или среднее профессиональное образование по иному направлению соответствующим направленности ДОП	Ссылка на веб-страницы с портфолио	Информация о курсах повышения квалификации по профилю преподаваемой дисциплины (за последние 3 года)	Пройдена промежуточная аттестация не менее чем за два года обучения по образовательным программам высшего образования по специальностям и направлениям подготовки, соответствующим направленности ДОП	Отметка о полученном согласии на обработку персональных данных
Бердашкевич Артём Эдуардович	АО «Диалог»	Руководитель направления	нет	да	https://xn----btbkcarrtg5c1as4d.xn--p1ai/experts/	Программирование Python. Продвинут	нет	да

		информационной безопасности			berdashkevich	ый уровень, 36 час., ООО Институт Повышения Квалификации Дополнительного профессионального образования, 2023 г.		
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 Дополнительного профессионального образовани	нет	да

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

5. Рабочая программа с описанием каждого модуля

Модуль 1. Основы Python Данный модуль посвящен изучению специализированных знаний по современному языку программирования Python: основ синтаксиса Python; сущности операторов и выражений; условных выражений и операторов, циклов и структур данных; функций в Python; рекурсии; встроенных функций Python. В качестве практики осваиваются навыки писать простейшие программы; создавать функции таблицы умножения; работать со списками; работать с модулями; создавать модули math_operations.py и	**Тема 1.1 Введение в Python**	Введение в язык программирования Python: история, особенности, применение. Установка и настройка окружения для работы с Python. Синтаксис Python: переменные, типы данных, операторы, условные выражения, циклы. Ввод и вывод данных: работа с консолью, чтение и запись файлов. Функции и модули в Python: создание и использование функций, импорт и использование модулей. Обработка исключений: обработка ошибок и исключительных ситуаций в Python.	теоретические занятия	2
		Написание программы, которая приветствует пользователя и запрашивает его имя. Затем программа выводит приветствие с использованием введенного имени. Написание программы, которая запрашивает у пользователя два числа и выводит их сумму, разность, произведение и частное	практические занятия	5

string_operations.py; обрабатывать исключения; работать с путями файлов; писать программы для чтения и записи файлов.		Создание функции на Python, которая принимает число в качестве аргумента и выводит таблицу умножения для этого числа до 10.	самостоятельная работа	1
	Тема 1.2 Синтаксис и основные конструкции языка	Операторы и выражения: арифметические операторы, операторы сравнения, логические операторы. Условные выражения и операторы: if-else, elif, вложенные условия. Циклы: цикл while, цикл for, операторы break и continue. Структуры данных: списки, кортежи, словари, множества. Индексация и срезы: доступ к элементам списков, кортежей и строк.	теоретические занятия	2
		Написание программы, которая проверяет, является ли введенное пользователем число четным или нечетным. Написание программы, которая выводит все числа от 1 до 10, кроме числа 3. Написание программы, которая запрашивает у пользователя список слов и выводит на экран только те слова, которые начинаются с буквы "a".	практические занятия	5

		Написание программы на Python, которая принимает список чисел и возвращает сумму всех элементов списка. Написание программы, которая запрашивает у пользователя список слов и выводит на экран только те слова, которые начинаются с буквы "о".	самостоятельная работа	1
	Тема 1.3 Функции и модули	Определение функций в Python: синтаксис, аргументы, возвращаемые значения. Локальные и глобальные переменные в функциях. Работа с модулями в Python: импорт модулей, использование функций и переменных из модулей. Создание собственных модулей в Python. Рекурсия: определение рекурсии, примеры рекурсивных функций. Встроенные функции Python: примеры использования встроенных функций.	теоретические занятия	2
		Создание модуля math_operations.py, который содержит функции для выполнения математических операций: сложение, вычитание, умножение и деление. Использование этого модуля в программе для выполнения арифметических операций над двумя числами, введенными пользователем. (работа в парах или группах из 3-х, 4-х	практические занятия	5

		человек)		
		Создание модуля string_operations.py, который содержит функции для работы со строками: подсчет количества символов, поиск подстроки, замена символов и т.д. Написание программы, которая использует функции из этого модуля для выполнения различных операций со строками, введенными пользователем.	самостоятельная работа	1
	Тема 1.4 Работа с файлами и обработка исключений	Открытие и закрытие файлов: функция open(), режимы открытия файлов. Чтение данных из файла: методы .read(), .readline(), .readlines(). Запись данных в файл: метод .write(), .writelines(). Обработка исключений: блок try-except, обработка различных видов исключений. Блок finally: использование для выполнения кода в любом случае. Управление ресурсами с помощью менеджера контекста with. Работа с путями файлов: модуль os.path, получение информации о файле или директории.	теоретические занятия	2

		Написание программы, которая открывает текстовый файл data.txt, считывает его содержимое и выводит на экран. Создание программы, которая запрашивает у пользователя строку и записывает ее в текстовый файл output.txt. Написание программы, которая открывает текстовый файл data.txt, считывает его содержимое построчно и выводит только те строки, которые содержат определенное ключевое слово, введенное пользователем.	практические занятия	6	
		Создание программы, которая копирует содержимое одного текстового файла в другой файл. Имена файлов должны быть заданы пользователем.	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. Основы этичного хакинга В данном модуле осуществляется знакомство с основами этичного хакинга, его отличием от нелегальных действий злоумышленников; с хакерскими атаками; с основными методами и инструментами сбора информации и разведки; с принципами эксплуатации и защиты от атак; с методами обнаружения атак. В рамках модуля осваиваются навыки разработки скриптов для проверки безопасности сети на языке программирования Python; написания программы на Python для извлечения информации о	**Тема 2.1 Основные понятия этичного хакинга**	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. Определение этичного хакинга и его отличие от нелегальных действий. Кодекс этичного хакера и основные принципы. Виды хакерских атак и их классификация. Разрешенные и незаконные действия в рамках этичного хакинга. Сертификации и лицензии в области этичного хакинга.	теоретические занятия	2
		Разработка скрипта для проверки безопасности сети в контексте обеспечения информационной безопасности. Написание скрипта на Python, который будет сканировать указанный IP-адрес или диапазон	практические занятия	5

домене; проведения поисковых запросов и анализ результатов; разработки программ для эксплуатации и защиты.		адресов и проверять открытые порты для принятия решений о методах защиты и обеспечения информационной безопасности.. Скрипт должен выводить информацию о найденных открытых портах и предлагать рекомендации по устранению уязвимостей.		
		Исследование и сравнение различных сертификаций в области этичного хакинга (например, CEH, OSCP, CISSP). Создание информационного доклада, который описывает каждую сертификацию, ее требования и преимущества, правовые аспекты.	самостоятельная работа	1
	Тема 2.2 Сбор информации и разведка	Информационная безопасности и основные методы сбора информации и разведки. Инструменты для сбора информации: поиск в открытых источниках, использование специализированных программ. Основы сетевого сканирования и анализа уязвимостей. Правовые и этические аспекты сбора информации и разведки.	теоретические занятия	2

		Написание программы на Python для извлечения информации о домене, которая будет принимать доменное имя и извлекать различную информацию о нем, такую как IP-адрес, WHOIS-данные, записи DNS и другие. Использование библиотек, таких как socket, python-whois и dnspython, для взаимодействия с соответствующими сервисами в контексте обеспечения информационной безопасности.	практические занятия	5
		Проведение поисковых запросов и анализ результатов. Составление списка заданных поисковых запросов и анализ результатов поиска. Оценка релевантности результатов, применение фильтров и расширенные операторы поиска для получения более точных и специфических результатов. Составление отчета о найденной информации и ее оценка для дальнейшего использования в деле обеспечения информационной безопасности.	самостоятельная работа	1

	Тема 2.3 Анализ уязвимостей	Принципы и методы анализа уязвимостей в сфере информационной безопасности. Инструменты для обнаружения уязвимостей: сканеры уязвимостей, инструменты анализа кода и т. д. Оценка и классификация уязвимостей. Отчетность и документирование уязвимостей. Правовые аспекты.	теоретические занятия	2
		Написание программы на Python для сканирования уязвимостей сети, которая будет сканировать сеть и идентифицировать уязвимые устройства или службы в контексте информационной безопасности. Использование библиотеки scapy для отправки и получения сетевых пакетов и анализа полученных ответов в деле обеспечения информационной безопасности..	практические занятия	5
		Исследование известных уязвимостей и угроз безопасности (выбор уязвимости или угрозы, например, Spectre или WannaCry, и подготовка сообщения, в котором должен быть рассмотрен принцип ее работы, возможные последствия и рекомендации по защите от нее).	самостоятельная работа	1

	Тема 2.4 Эксплуатация и защита от атак	Основы эксплуатации уязвимостей в контексте информационной безопасности. Инструменты и методы эксплуатации. Защитные меры и техники обнаружения атак. Разработка и внедрение политик безопасности. Правовые аспекты.	теоретические занятия	2
		Освоение основных угроз информационной безопасности через разработку скрипта на Python для взлома слабого пароля, который будет использовать словарь паролей для попыток взлома учетных записей с использованием слабых паролей. (работа в парах или группах из 3-х, 4-х человек)	практические занятия	6
		Исследование и анализ известных уязвимостей и методов эксплуатации в контексте информационной безопасности. Изучение списка известных уязвимостей и методов эксплуатации, таких как буферное переполнение, инъекции кода, отказ в обслуживании (DoS) и другие. Создание отчета, с описанием каждой уязвимости, ее влияние на систему защиты от нее.	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. Сетевая безопасность В данном модуле в фокусе внимания - сетевая безопасность. Изучаются основные понятия и протоколы сетевого взаимодействия (IP, TCP, UDP, HTTP, HTTPS); основы анализа сетевого трафика и его роли в обеспечении безопасности; методы защиты сети и	**Тема 3.1 Основы сетевых протоколов**	Основные понятия и протоколы сетевого взаимодействия: IP, TCP, UDP, HTTP, HTTPS и другие в контексте информационной безопасности. Функции и особенности каждого протокола. Основные принципы маршрутизации и пересылки пакетов в сети. Правовые аспекты	теоретические занятия	2	
		Разработка клиент-серверного приложения на Python с использованием TCP протокола, в которой реализован клиент-серверный обмен данных с использованием TCP протокола для понимания вопросов	практические занятия	5	

техники обнаружения атак; принципы работы систем IDS и IPS; методы защиты от DDoS-атак; основные угрозы безопасности Wi-Fi сетей; виды шифрования Wi-Fi. Осваиваются навыки разработки клиент-серверного приложения на Python с использование TCP протокола; разработки программы на Python для сканирования сети и определения активных устройств; работы с инструментами анализа сетевого трафика (Wireshark); написания программы на Python с использованием библиотеки pcapy для анализа сетевого трафика; написания программы на Python для симуляции фаервола; написания программы на Python для сканирования Wi-Fi сетей и проведения аудита безопасности.		обеспечения информационной безопасности в Интернет. (работа в парах, один ученик пишет клиентскую часть, а второй - серверную)		
		Освоение способов обеспечения информационной безопасности в контексте разработки программы на Python, которая будет сканировать сеть и определять активные устройства. Программа должна отправлять ICMP эхо-запросы (ping) на IP адреса в заданном диапазоне и анализировать полученные ответы для определения активных устройств. Выводы о значимости полученных навыков в деле обеспечения информационной безопасности.	самостоятельная работа	1
	Тема 3.2 Анализ сетевого трафика	Основы анализа сетевого трафика и его роли в обеспечении безопасности. Инструменты анализа сетевого трафика, такие как Wireshark. Анализ протоколов на разных уровнях модели OSI (Ethernet, IP, TCP, UDP) и распознавание типичных сетевых пакетов. Идентификация и анализ сетевых атак, таких как атаки отказа в обслуживании (DoS), атаки переполнения буфера и другие.	теоретические занятия	2

		Правовые аспекты использования данных инструментов.		
		Инструмент Wireshark. Установка Wireshark на свой компьютер и проведение анализа сетевого трафика, захват пакетов на сетевых устройствах в контексте обеспечения информационной безопасности. Изучение содержимого пакетов на разных уровнях и анализ данных. Протоколы, адреса отправителей и получателей, порты и другие параметры. Правовые аспекты	практические занятия	5
		Написание программы на Python, которая будет анализировать сетевой трафик, захватываемый с использованием библиотеки pcapy в контексте безопасности. Программа должна просматривать захваченные пакеты и выводить информацию о протоколах, IP адресах отправителей и получателей, портах и других параметрах. Уточнение правовых аспектов.	самостоятельная работа	1

	Тема 3.3 Защита сети и обнаружение атак	Основные методы защиты сети: фаерволы, антивирусные программы, системы обнаружения вторжений (IDS) и предотвращения вторжений (IPS). Техники обнаружения атак: сигнатурный анализ, аномальное поведение, статистический анализ. Принципы работы систем IDS и IPS. Использование сетевых масок для фильтрации трафика. Методы защиты от DDoS-атак.	теоретические занятия	2
		Написание программы на Python, которая симулирует фаервол, принимая сетевой трафик и применяя правила фильтрации для разрешения или блокировки пакетов. Возможна работа в парах или группах из 3-х, 4-х человек. Каждый член команды создает свою функцию или модуль программы, чтобы в дальнейшем объединить их все в общий скрипт на Python.	практические занятия	5
		Методы защиты от DDoS-атак. Разработка плана защиты от DDoS-атак для вымышленной компании, который включает использование специализированных устройств и программного обеспечения.	самостоятельная работа	1

	Тема 3.4 Безопасность Wi-Fi сетей	Основные угрозы безопасности Wi-Fi сетей: перехват трафика, подмена точки доступа, атаки на протоколы аутентификации и шифрования. Методы защиты Wi-Fi сетей: использование безопасных протоколов, настройка сетевых устройств, управление доступом, использование виртуальных частных сетей (VPN). Различные виды шифрования Wi-Fi: WEP, WPA, WPA2, WPA3. Аудит безопасности Wi-Fi сетей и поиск уязвимостей.	теоретические занятия	2
		Написание программы на Python, которая сканирует доступные Wi-Fi сети и выводит информацию о них, включая уровень сигнала, тип шифрования и наличие защищенного пароля в контексте информационной безопасности. Реализация скрипта на Python, который проводит аудит безопасности Wi-Fi сети. Скрипт должен проверять уровень шифрования, наличие уязвимостей и давать рекомендации по улучшению безопасности.	практические занятия	6
		Проведение исследования безопасности Wi-Fi сети в собственном домашнем окружении. Описание	самостоятельная работа	2

		проблем и уязвимостей, которые были обнаружены, и предложение меры по улучшению безопасности сети. Написание отчета, в котором детально описаны найденные уязвимости и предложенные решения для их устранения.		
	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. Веб-безопасность Этот модуль посвящен освоению основных компонентов веб-приложений; протоколов	**Тема 4.1 Основы веб-разработки**	Информационная безопасности и веб-разработка. Основные компоненты веб-приложений: клиентская часть (HTML, CSS, JavaScript) и серверная часть (языки программирования, базы данных). Протоколы передачи данных в вебе: HTTP, HTTPS. Архитектура	теоретические занятия	2

передачи данных в вебе: HTTP и HTTPS; основных уязвимостей веб-приложений и методов их защиты; кросс-сайтового скриптинга (XSS) и его основных принципов работы; различных типов XSS-атак и их потенциальных последствий; инъекций и уязвимостей баз данных; методов предотвращения XSS-атак и инъекций; методов защиты веб-приложений. В качестве практических навыков осваивается практика разработки веб-приложения с использованием фреймворка Flask на Python; разработки веб-страниц с уязвимостью к XSS-атаке; исследования различных типов XSS-атак и разработки демонстрационных страниц; разработки веб-страниц с уязвимостью к		клиент-сервер и взаимодействие между клиентом и сервером в контексте информационной безопасности. Основные уязвимости веб-приложений: недостаточная валидация ввода, недостаточная обработка ошибок, уязвимости баз данных		
		Разработка простого веб-приложение с использованием фреймворка Flask на Python в деле обеспечения информационной безопасности. Приложение должно иметь форму для ввода данных от пользователя, а затем выводить их на веб-странице. Возможна работа в парах или группах из 3-х, 4-х человек. Каждый член команды создает свою функцию или модуль программы, чтобы в дальнейшем объединить их все в общий скрипт на Python.	практические занятия	5
		Овладение методами защиты веб-приложений, такими как фильтрация ввода, санитизация данных и использование подготовленных запросов. Разработка документа с рекомендациями по обеспечению безопасности веб-приложений, включая примеры кода на Python и	самостоятельная работа	1

инъекциям; исследования различных типов инъекций баз данных; разработки и осуществления аудита безопасности веб-приложений.		объяснения их работы.		
	Тема 4.2 Кросс-сайтовый скриптинг (XSS)	Определение кросс-сайтового скриптинга (XSS) и его роль в обеспечении информационной безопасности. Основные принципы работы. Различие между хранимым (stored), отраженным (reflected) и межсайтовым (DOM-based) XSS. Уязвимые точки веб-приложений, которые могут быть использованы для XSS-атак. Виды XSS-атак и их потенциальные последствия. Методы предотвращения XSS-атак.	теоретические занятия	2
		Разработка веб-страницы, на которой имеется уязвимость к XSS-атаке. Создание страницу с формой для ввода данных и выводом этих данных на странице используя Python и фреймворк Flask. Демонстрация, как можно провести XSS-атаку, внедрив вредоносный скрипт, и предложение мер по предотвращению такой атаки.	практические занятия	5
		Исследование различные типы XSS-атак (stored, reflected, DOM-based) и разработка набора демонстрационных страниц, которые иллюстрируют каждый из этих типов атак.	самостоятельная работа	1

		Уточнение, как можно эксплуатировать уязвимости и предложение методов предотвращения каждого типа атаки		
	Тема 4.3 Инъекции и уязвимости баз данных	Введение в инъекции и уязвимости баз данных в контексте обеспечения информационной безопасности. Типы инъекций: SQL-инъекции, командные инъекции, NoSQL-инъекции. Уязвимые точки веб-приложений, которые могут быть использованы для инъекций. Потенциальные последствия инъекций баз данных. Методы предотвращения инъекций, включая использование подготовленных запросов, фильтрацию и санитизацию ввода, ограничение привилегий баз данных.	теоретические занятия	2
		Разработка простой веб-страницы с формой для ввода данных, которые будут использоваться для выполнения SQL-запроса к базе данных. Создание страницы, где пользователь может ввести свои данные и получить результат из базы данных используя Python и фреймворк Flask. Правовые аспекты	практические занятия	5

		Исследование различных типов инъекций баз данных (SQL, командные, NoSQL) и разработка демонстрационных приложений, которые иллюстрируют каждый из этих типов инъекций. Демонстрация, как можно эксплуатировать уязвимости и предложите методы предотвращения каждого типа инъекции.	самостоятельная работа	1
	Тема 4.4 Защита веб-приложений	Введение в защиту веб-приложений и ее важность. Основные угрозы и уязвимости веб-приложений, такие как перехват данных, подделка запросов, межсайтовый скриптинг (XSS), инъекции, утечки информации и другие. Методы защиты веб-приложений: валидация и санитизация ввода, использование безопасных архитектурных подходов, контроль доступа, защита от инъекций и уязвимостей баз данных, шифрование данных, управление сеансами и аутентификация, мониторинг и журналирование событий.	теоретические занятия	2

		Разработка простого веб-приложения с использованием фреймворка Flask. Проведение аудита безопасности приложения и выявление потенциальных уязвимостей. Предложения и реализация мер по усилению безопасности приложения, такие как валидация и санитизация ввода, контроль доступа	практические занятия	6
		Исследование различных методов аутентификации и авторизации веб-приложений, таких как многофакторная аутентификация, токены доступа и JSON Web Tokens (JWT).	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. Основы Python	Тема 1.1 Введение в Python	7	2 2 2 2	29.09.2023 05.10.2023 09.10.2023 12.10.2023
2		Тема 1.2 Синтаксис и основные конструкции языка	7	2 2 2 2	16.10.2023 19.10.2023 23.10.2023 26.10.2023
3		Тема 1.3 Функции и модули	7	2 2 2 2	30.10.2023 02.11.2023 06.11.2023 09.11.2023
4		Тема 1.4 Работа с файлами и обработка исключений	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. Основы этичного хакинга	Тема 2.1 Основные понятия этичного хакинга	7	2 2 2 2	30.11.2023 04.12.2023 07.12.2023 11.12.2023
7		Тема 2.2 Сбор информации и разведка	7	2 2 2 2	14.12.2023 18.12.2023 21.12.2023 25.12.2023
8		Тема 2.3 Анализ уязвимостей	7	2 2 4	28.12.2023 11.01.2024 16.01.2024

9		Тема 2.4 Эксплуатация и защита от атак	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. Сетевая безопасность	Тема 3.1 Основы сетевых протоколов	7	2 2 2 2	01.02.2024 05.02.2024 08.02.2024 12.02.2024
12		Тема 3.2 Анализ сетевого трафика	7	2 2 2 2	15.02.2024 19.02.2024 22.02.2024 26.02.2024
13		Тема 3.3 Защита сети и обнаружение атак	7	2 2 2 2	29.02.2024 04.03.2024 06.03.2024 11.03.2024
14		Тема 3.4 Безопасность Wi-Fi сетей	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. Веб-безопасность	Тема 4.1 Основы веб-разработки	7	2 2 2 2	01.04.2024 04.04.2024 08.04.2024 11.04.2024

17		Тема 4.2 Кросс-сайтовый скриптинг (XSS)	7	2 2 2 2	15.04.2024 18.04.2024 22.04.2024 25.04.2024
18		Тема 3.3 Инъекции и уязвимости баз данных	7	2 2 4	29.04.2024 06.05.2024 13.05.2024
19		Тема 4.4 Защита веб-приложений	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.	Образовательная деятельность учащихся предусматривает следующие виды учебных занятий: лекции, практические занятия и самостоятельную работу, определенные учебным планом.	Образовательная деятельность учащихся предусматривает следующие виды учебных занятий: лекции, практические занятия и самостоятельную работу, определенные учебным планом.	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.	При реализации Программы используются групповая и фронтальная формы организации учебного процесса, различные образовательные технологии: технология «перевернутого класса», геймификация, технология проектного обучения, онлайн-конференция.	При реализации Программы используются групповая и фронтальная формы организации учебного процесса, различные образовательные технологии: технология «перевернутого класса», геймификация, технология проектного обучения, онлайн-конференция.	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, конспектов); заданий, видеоинструкций, скринкастов, гайдов для организации и реализации практических занятий и самостоятельной работы.	реализация модуля предусматривает авторские разработки лекционных материалов (рабочих листов, презентаций, конспектов); заданий, видеоинструкций, скринкастов, гайдов для организации и реализации практических занятий и самостоятельной работы.	реализация модуля предусматривает авторские разработки лекционных материалов (рабочих листов, презентаций, конспектов); заданий, видеоинструкций, скринкастов, гайдов для организации и реализации практических занятий и самостоятельной работы.	реализация модуля предусматривает авторские разработки лекционных материалов (рабочих листов, презентаций, конспектов); заданий, видеоинструкций, скринкастов, гайдов для организации и реализации практических занятий и самостоятельной работы.
Материалы модуля	материалы модуля - это учебно-методическое	материалы модуля - это учебно-методическое	материалы модуля - это учебно-методическое	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	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	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	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	образовательных ресурсов по теме модуля	образовательных ресурсов по теме модуля	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 /	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	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.	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»).

	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.	программиста»).	Гид для разработчиков, программистов и интересующихся. — СПб.: Питер, 2019. — 272 с.: ил. — (Серия «Библиотека программиста»).	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. 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	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".	Перехват и анализ сетевого трафика. Общество с ограниченной 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	Лучшие дистрибутивы для тестирования на проникновение. АО "Синклит" Официальный 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:

	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 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.	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. 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:	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.	официальный сайт. - Москва. - URL: https://habr.com/ru/articles/276477/ (дата обращения: 14.06.2023) - Текст: электронный.

		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/companies/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.	Лабораторная работа в Packet Tracer. Блог о кибербезопасности"Habr". Positive Technologies: официальный сайт.- Москва. - URL: https://habr.com/ru/post/35	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: 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.	0720/ (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. 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.	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.	Блог "NetSkills" URL: http://blog.netskills.ru/ (дата обращения: 14.06.2023) - Текст: электронный.