Индивидуальный предприниматель Селендеева О.Н.

УТВЕРЖДАЮ

Индивидуальный предприниматель

_____/Селендеева О.Н.//

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
ДОПОЛНИТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА
«ЭТИЧНЫЙ ХАКЕР»

Москва, 2022

Оглавление

Оглавление

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1. Общая характеристика программы

Данный документ описывает комплекс основных характеристик образования (объем, содержание, планируемые результаты) и организационно-педагогических условий, который представлен в виде учебного плана, календарного учебного графика, рабочих программ учебных предметов, модулей, иных компонентов, а также оценочных и методических материалов общеобразовательной общеразвивающей программы "Этичный хакер".

В ходе дополнительной общеобразовательной общеразвивающей программы "Этичный хакер" обучающиеся познакомятся с основными понятиями и практическими подходами информационной безопасности, получат базовое представление о языке Python и его применением в прикладных задачах этичного хакинга, познакомятся с основами профессии специалиста по кибербезопасности.

Выдача обучающимся документов о дополнительном образовании (сертификат установленного образца) осуществляется при условии успешного прохождения итоговой аттестации.

Программа разработана на основе следующих **нормативных документов:**

- Федеральный закон от 29 декабря 2012 г. №273-ФЗ «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";
- Постановление Главного государственного санитарного врача РФ от 28.09.2020 № 28 «Об утверждении санитарных правил СП 2.4.3648-20 "Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи" (вместе с "СП 2.4.3648-20. Санитарные правила...")» (Зарегистрировано в Минюсте России 18.12.2020 № 61573).

Направленность (профиль) программы: техническая

Актуальность программы, соответствие государственному, социальному заказу/запросам.

В современном мире умение находить ошибки в системах безопасности и устранять их является **ценным и востребованным навыком**, который все больше и больше ценится на рынке, особенно сегодня, в условиях ограниченных ресурсов и повышенных расходов. В результате прохождения обучения слушатель получит представление об угрозах и опасностях, подстерегающих в интернете, познакомится с различными аспектами информационной безопасности на практике, научится надежно защищать свои личные данные и секретную информацию. Обучающимся будут созданы оптимальные условий для всестороннего

удовлетворения потребностей и развития их индивидуальных склонностей и способностей, появится мотивация личности к познанию и творчеству.

Отличительные особенности программы: по окончании обучения учащиеся с помощью полученных на курсе знаний и навыков выйдут на продвинутый уровень владения компьютером и смогут защитить себя, свою семью и друзей от киберопасностей. В процессе освоения программы обучающиеся смогут в раннем возрасте получить профессиональную ориентацию - обучение по данной программе будет полезно для тех, кто интересуется развитием в области научно-технической направленности, будущих программистов, специалистов в области кибербезопасности.

Срок обучения: программа реализуется в объеме 96 академических часов, 36 недель (9 месяцев).

Режим занятий: 2-4 академических часа в неделю.

Продолжительность академического часа – 45 минут.

Занятия начинаются не ранее 9.00 часов утра и заканчиваются не позднее 20.00 часов. Для обучающихся в возрасте 16-18 лет допускается окончание занятий в 21.00 часов.

Продолжительность занятий в учебные дни - не более 3-х академических часов в день, в выходные и каникулярные дни - не более 4 академических часов в день. После 30-45 минут теоретических занятий организуется перерыв длительностью не менее 10 мин.

Адресат программы и примерный портрет слушателя курсов: программа разработана для учащихся от 12 до 16 лет, которых интересует направление информационной безопасности. К освоению дополнительной общеобразовательной программы – дополнительной общеразвивающей программы допускаются: лица без предъявления требований к уровню образования.

По завершении реализации программы, как правило, проводится анкетирование обучающихся с целью изучения мнения по вопросу эффективности и информативности проведенного обучения, уровню организации учебного процесса, удовлетворенности учебно-методическим материалом, работниками образовательной организации проводится анализ высказанных предложений и пожеланий.

1.2. Цели и задачи программы

1. **Цель программы** – познакомиться с основными понятиями и практическими подходами информационной безопасности, получить базовое представление о языке Python и его применении в прикладных задачах этичного хакинга, познакомиться с основами профессии специалиста по кибербезопасности.

Задачи программы:

1. Дать представление об угрозах и опасностях, подстерегающих в интернете;
2. Познакомить с различными аспектами информационной безопасности на практике;
3. Научить находить уязвимости, защищать различные программы и системы;
4. Показать, как обходить системы защиты
5. Научить надежно защищать свои личные данные и секретную информацию

6. Дать полное представление о профессиях в сфере информационной безопасности.
7. Сформировать интерес к увлечению программированием и раскрытию своих способностей в сфере IT-технологий.
8. Научить создавать свой проект и презентовать его.

1.3. Планируемые результаты обучения

По итогам освоения дополнительной общеобразовательной программы - дополнительной общеразвивающей программы "Этичный хакер" обучающиеся должны будут овладеть следующими знаниями, умениями и навыками:

Знать:

- Понятие этичного хакинга и его роль в обеспечении информационной безопасности.
- Правила безопасной работы в интернете.
- Роль специалиста по информационной безопасности.
- Понятие "инцидент" в информационной безопасности.
- Понятия "конфиденциальность", "целостность", "доступность"
- Приемы защиты паролей учетных записей.
- Основные виды вирусов.
- Основные виды атак в сети и их сценарии.
- Понятие "социальная инженерия".
- Понятие “фишинг”.
- Основы языка Python и его применение в кибербезопасности.
- Виды сетевых атак.
- Стек протоколов OSI.
- Основы шифрования сообщений.
- Принципы атак Dos и Ddos.
- Принципы языков гипертекстовой разметки (HTML и CSS).
- Основы языка программирования JavaScript.
- Принципы написания функций на языке JavaScript.
- Понятия и принципы работы сетевых протоколов.
- Основы межсайтового скриптинга.
- Принципы работы локальных, глобальных, частных и публичных сетей.
- Отличия в подходах к защите безопасности в ОС Windows и Linux.

Уметь:

- Создавать программы для шифрования сообщений с использованием изученных конструкций языка Python.
- Создавать базы данных на основе файлов для хранения и проверки логинов и паролей пользователей.
- Проверять и устранять уязвимости в коде сайта.
- Писать программы шифрования и расшифровки сообщения.
- На практике применять подходы JavaScript, включая циклы, функции и события.
- На практике применять подходы межсайтового скриптинга (XSS).
- Обнаруживать и создавать сайты-фишеры.
- Создание прототипов веб-сайтов с использованием полученных знаний в HTML, CSS и JavaScript.
- Писать сайты с уязвимостью XSS.

- Записывать команды в командной строке Windows.
- Защита проектов от сетевых атак и уязвимостей.
- Создавать и защищать свои проекты.

Владеть навыками в области:

- Анализа безопасности и обнаружения уязвимостей.
- Применения программирования в практике специалиста по кибербезопасности.
- Сетевой безопасности и защиты данных.
- Реагирования на киберинциденты.
- Подготовки презентаций и защиты технических проектов.

2. УЧЕБНЫЙ ПЛАН ПРОГРАММЫ

В процессе преподавания курса "Этичный хакер" используются как классические методы обучения (лекции), так и различные виды практической работы обучающихся по заданию преподавателя, которые направлены на развитие навыков использования механизмов защиты информации и предотвращения сетевых атак, и на поощрение интеллектуальных инициатив учащихся.

Формы организации образовательного процесса (индивидуальные, групповые и т.д.) и другие виды занятий по программе определяются содержанием программы. Образовательная деятельность обучающихся предусматривает следующие виды учебных занятий и учебных работ: лекции, практические и семинарские занятия, мастер-классы, тренинги, семинары по обмену опытом, проведение открытых занятий, консультации и другие виды учебных занятий и методической работы, определенные учебным планом.

№	*Наименование дисциплины/раздела/ Темы*	*Количество академических часов*				*Форма аттестации /контроля*
		Всего	*в т.ч. аудиторных*		*СРС*	
			теория	*практич. занятия*		
1	Понятие этичного хакинга. Роль специалиста по информационной безопасности	**2**	1	1	0	Практическое задание
2	Роль этичного хакера. Сценарии работы	**2**	1	1	0	Практическое задание
3	Основные виды атак в сети	**2**	1,5	0,5	0	Практическое задание
4	Социальная инженерия	**3**	1	2	0	Практическое задание, Контрольные вопросы.
5	Знакомство с Python. Понятие "Криптография"	**2**	1	1	0	Практическое задание
6	Операторы if и else. Способы шифрования сообщений. Часть 1	**2**	1	1	0	Практическое задание
7	Операторы for и while. Способы шифрования сообщений. Часть 2	**2**	1	1	0	Практическое задание
8	Написание программы шифрования сообщения	**2**	1	1	0	Практическое задание
9	Шифрование сообщения с помощью картинки	**3**	0,5	1,5	1	Практическое задание,

						Контрольные вопросы.
10	Знакомство с хешированием	**2**	1	1	0	Практическое задание
11	Классы в Python. Программа для хеширования пароля	**3**	1	1	1	Практическое задание
12	Создание базы данных логинов и паролей пользователей	**2**	1	0,5	0,5	Практическое задание
13	Виды сетевых атак. Знакомство с языком HTML	**2**	1	0,5	0,5	Практическое задание, Контрольные вопросы.
14	Сетевые атаки. Brute force	**2**	1	1	0	Практическое задание
15	Каскадные таблицы CSS	**3**	1	1,5	0,5	Практическое задание
16	Написание полноценной страницы сайта. Сайты фишеры	**3**	1	1	1	Практическое задание
17	Основы языка программирования JavaScript	**2**	1	1	0	Практическое задание, Контрольные вопросы.
18	Циклы в JavaScript и принципы работы с ними	**3**	1	1	1	Практическое задание
19	Функции и события в JavaScript	**3**	1	1,5	0,5	Практическое задание
20	Межсайтовый скриптинг XSS	**3**	0,5	1	1,5	Практическое задание
21	Создание базы данных	**3**	0,5	1,5	1	Практическое задание, Контрольные вопросы.
22	Базы данных. Команды для работы с БД	**2**	1	1	0	Практическое задание
23	Взаимодействие базы данных с сайтом	**3**	1	2	0	Практическое задание,
24	Способы защиты от SQL уязвимостей	**4**	1	1	2	Практическое задание
25	Устройство сети Интернет. Изучение стека OSI	**2**	**1**	**1**	**0**	Практическое задание, Контрольные вопросы.

26	Изучение стека TCP/IP	**3**	**0,5**	**1,5**	**1**	Практическое задание
27	Протоколы и сферы их применения	**2**	**0,5**	**0,5**	**1**	Практическое задание
28	Протокол http. Локальные, глобальные, частные и публичные сети	**4**	**1**	**1**	**2**	Практическое задание
29	Знакомство с командной строкой Windows	**3**	**1**	**1**	**1**	Практическое задание, Контрольные вопросы.
30	Новые команды и фишки командной строки Windows	**3**	**1**	**2**	**0**	Практическое задание
31	Знакомство с ОС Linux	**4**	**1**	**1**	**2**	Практическое задание,
32	Знакомство с понятиями "IP" и "порт". Сравнение ОС Windows и Linux	**2**	**1**	**1**	**0**	Практическое задание
33	Знакомство и практика работы с VPN	**3**	**1**	**2**	**0**	Практическое задание, Контрольные вопросы.
34	Знакомство и практика работы с FTP	**3**	**1**	**2**	**0**	Практическое задание
35	Знакомство и практика работы с протоколом SMB	**3**	**1**	**2**	**0**	Практическое задание
36	Прохождение испытаний. Challenge 4. Redeemer. Презентация проектов курса	**4**	**0**	**0**	**4**	Практическое Задание, Контрольные вопросы. Защита проекта
	ИТОГО	**96**	**33**	**41,5**	**21,5**	

3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Календарный учебный график формируется при осуществлении обучения в течение всего календарного года. По мере набора групп слушателей по программе составляется календарный график, учитывающий объемы лекций, практики, самоподготовки, другие формы организации занятий.

Темы / недели	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**Итого часов**
1. Понятие этичного хакинга. Роль специалиста по информационной безопасности	2																																				**2**
2. Роль этичного хакера. Сценарии работы		2																																			**2**
3. Основные виды атак в сети			2																																		**2**
4. Социальная инженерия				2,5																																	**2,5**
Промежуточный контроль				0,5																																	**0,5**
5. Знакомство с Python. Понятие "Криптография"					2																																**2**
6. Операторы if и else. Способы шифрования сообщений. Часть 1						2																															**2**
7. Операторы for и while. Способы шифрования сообщений. Часть 2							2																														
8. Написание программы шифрования сообщения								1,5																													**1,5**
Промежуточный контроль								0,5																													**0,5**
9. Шифрование сообщения с помощью картинки									3																												**3**
10. Знакомство с хеширование										2																											**2**
11. Классы в Python. Программа для хеширования пароля											3																										**3**

12. Создание базы данных логинов и паролей пользователей												1,5																												**1,5**
Промежуточный контроль												0,5																												**0,5**
13. Виды сетевых атак. Знакомство с языком HTML													2																											**2**
14. Сетевые атаки. Brute force														2																										**2**
15. Каскадные таблицы CSS															3																									**3**
16. Написание полноценной страницы сайта. Сайты фишеры																2,5																								**2,5**
Промежуточный контроль																0,5																								**0,5**
17. Основы языка программирования JavaScript																	2																							**2**
18. Циклы в JavaScript и принципы работы с ними																		3																						**3**
19. Функции и события в JavaScript																			3																					**3**
20. Межсайтовый скриптинг XSS																				2,5																				**2,5**
Промежуточный контроль																				0,5																				**0,5**
21. Создание базы данных																					3																			**3**
22. Базы данных. Команды для работы с БД																						2																		**2**
23. Взаимодействие базы данных с сайтом																							3																	**3**
24. Способы защиты от SQL уязвимостей																								3,5																**3,5**
Промежуточная аттестация																								0,5																**0,5**
25. Устройство сети Интернет. Изучение стека OSI																									2															**2**
26. Изучение стека TCP/IP																										3														**3**
27. Протоколы и сферы их применения																											2													**2**

28. Протокол http. Локальные, глобальные, частные и публичные сети																													3,5													**3,5**
Промежуточная аттестация																													0,5													**0,5**
29. Знакомство с командной строкой Windows																														3													**3**
30. Новые команды и фишки командной строки Windows																															3												**3**
31. Знакомство с ОС Linux																																4											**4**
32. Знакомство с понятиями "IP" и "порт". Сравнение ОС Windows и Linux																																	1,5										**1.5**
Промежуточная аттестация																																	0,5										**0,5**
33. Знакомство и практика работы с VPN																																		3									**3**
34. Знакомство и практика работы с FTP																																			3								**3**
35. Знакомство и практика работы с протоколом SMB																																				3							**3**
36. Прохождение испытаний. Challenge 4. Redeemer. Презентация проектов курса																																					3						**3**
Итоговая аттестация																																						1					**1**
ИТОГО	**2**	**2**	**2**	**3**	**2**	**2**	**2**	**2**	**3**	**2**	**3**	**2**	**2**	**2**	**3**	**3**	**2**	**3**	**3**	**3**	**3**	**2**	**3**	**4**	**2**	**3**	**2**	**4**	**3**	**3**	**4**	**2**	**3**	**3**	**3**	**4**	**96**					

4. РАБОЧАЯ ПРОГРАММА

1. Понятие этичного хакинга. Роль специалиста по информационной безопасности

- Задачи этичного хакинга;
- Структура отдела информационной безопасности;
- Законы и правила, по которым работает специалист по информационной безопасности;
- Правила безопасной работы в интернет.

Практическое задание: обсуждение и закрепление правил безопасного пребывания в интернете.

2. Роль этичного хакера. Сценарии работы

- Знакомство с понятиями "конфиденциальность", "целостность", "доступность";
- Понятие инцидента;
- Принципы построения сценариев атак и защиты против злоумышленников.

Практическое задание: разделиться на команды по 2-3 человека и продумать свою стратегию атаки или защиты.

3. Основные виды атак в сети

- Знакомство с понятиями SIEM, SOAR, IRP;
- Изучение основных видов атак;
- Практика - просмотр системы анализа инцидентов.

Практическое задание: провести анализ видов атак в порядке их вредоносности.

4. Социальная инженерия

- Изучение понятия "социальная инженерия";
- Рейтинги атак. Знакомство с OWASP Top 10;
- Практика - разработка сценария социальной инженерии.

Практическое задание: работа в командах - продумать сценарии взлома, основанный на социальной инженерии..

5. Знакомство с Python. Понятие "Криптография"

- Написание первой программы на языке Python;
- Изучение арифметических и логических операторов;
- Знакомство с понятием “Криптография”.

Практическое задание: создание первых программ на языке Python.

6. Операторы if и else. Способы шифрования сообщений. Часть 1

- Операторы if и else в Python;
- Знакомство с подходами шифрования сообщений;
- Практика - написание программ с использованием условий.

Практическое задание: написание программы с использованием операторов if и else, ручное шифрование сообщений.

7

. Операторы for и while. Способы шифрования сообщений. Часть 2

- Операторы for и while в Python;
- Более сложные методы шифрования сообщений;
- Практика - написание программ с использованием операторов for и while.

Практическое задание: написание программы с использованием операторов for и while, ручное шифрование сообщений.

8. Написание программы шифрования сообщения

- Изучение понятия "строки" в Python;
- Написание программы шифрования и расшифровки сообщения.

Практическое задание: создание программы на Python для шифрования сообщений с использованием изученных конструкций языка.

9. Шифрование сообщения с помощью картинки

- Изучение функций в Python;
- Способы шифрования с помощью картинки;
- Написание программы для шифрования сообщения внутри картинки.

Практическое задание: создание программы для шифрования сообщения в картинку.

10. Знакомство с хешированием

- Изучение функций в Python - продолжение;
- Знакомство с понятием хеширование;
- Применение хеширования в практике программирования.

Практическое задание: написание программы с использованием функций Python.

11. Классы в Python. Программа для хеширования пароля

- Понятие классов;
- Классы в Python;
- Практика - написание программы для хеширования пароля.

Практическое задание: написание программы с применением классов для хеширования паролей.

12. Создание базы данных логинов и паролей пользователей

- Основы работы с файлами в Python;
- Создание базы данных на основе файлов для хранения логинов и паролей пользователей.

Практическое задание: создание программы по хранению и проверке логинов и паролей с использованием изученных конструкций языка Python.

13. Виды сетевых атак. Знакомство с языком HTML

- Изучение принципа работы сетевой атаки “Отказ в обслуживании”;
- Изучение атак Dos и Ddos
- Базовые элементы языка HTML.

Практическое задание: создание программы по принципу атаки “Отказ в обслуживании”.

14. Сетевые атаки. Brute force

- Углубление в изучение языка гиперразметки HTML;
- Создание простого сайта с помощью HTML;
- Изучение принципов атаки Brute force;
- Проверка и устранение уязвимостей в коде сайта.

Практическое задание: написали свой первый небольшой сайт и научились выявлять уязвимости, связанные с кодом сайта.

15. Каскадные таблицы CSS

- Изучение основ каскадных таблиц CSS;
- Подходы к подбору пароля;
- Практика - написание программы для подбора пароля с помощью техники Brute force.

Практическое задание: создание программы для подбора пароля Brute force.

16. Написание полноценной страницы сайта. Сайты фишеры

- Знакомство с понятием “Фишинг”;
- Практика - создание сайтов с использованием полученных знаний;
- Создание сайта фишера.

Практическое задание: написание своего собственного сайта-фишера.

17. Основы языка программирования JavaScript

- Знакомство с языком программирования JavaScript;
- Переменные в JavaScript;
- Операторы if и else;
- Практика программирования - решение задач на языке
- программирования JavaScript.

Практическое задание: решение практических задач на JavaScript.

18. Циклы в JavaScript и принципы работы с ними

- Циклы в JavaScript и принципы работы с ними;
- Цикл While, понятие бесконечного цикла;
- Цикл For, конечные циклы;
- Практика программирования - решение задач на языке программирования JavaScript

Практическое задание: написали свой первый небольшой сайт.

19. Функции и события в JavaScript

- Принцип написания функций на языке JavaScript;
- Написание программы с использованием функций;
- Изучение понятия “Событие".

Практическое задание: создание программы на JavaScript с использованием функций и обработчиков событий.

20. Межсайтовый скриптинг XSS

- Знакомство с межсайтовым скриптингом;
- Написание сайта с уязвимостью XSS;
- Методики исправления уязвимости XSS.

Практическое задание: написание полноценно рабочего сайта с формами, устранение уязвимости XSS.

21. Создание первой базы данных

- Знакомство с понятием “База данных”;
- Изучение первых команд на языке MySQL;
- Написание первой БД.

Практическое задание: создание своей первой базы данных с применением языка MySQL

22. Базы данных. Команды для работы с БД

- Изучение языка MySQL;
- Изучение команд для взаимодействия с БД;
- Создание базы данных пользователей сайта.

Практическое задание: создали базу данных пользователей для дальнейшей работы

23. Взаимодействие базы данных с сайтом

- Изучение основных методов взаимодействия с базой данных с помощью языка программирования JS и php
- создание программы для авторизации пользователя.

Практическое задание: создание программы для авторизации пользователя.

24. Способы защиты от SQL уязвимостей

- Знакомство с понятием “SQL-инъекция”;
- Изучение методов защиты от SQL-инъекций;
- Практика - изучение и правка кода для защиты от SQL-инъекций.

Практическое задание: исправление допущенных в коде ошибок для защиты от SQL-инъекций.

25. Устройство сети Интернет. Изучение стека OSI

- Изучение понятий “Интернет”, “Компьютерная сеть”, “Сервер”;
- Изучение уровней стека OSI;
- Знакомство с понятием “Протокол”.

Практическое задание: практический разбор работы модели OSI при вводе запроса пользователя на странице сайта.

26. Изучение стека TCP/IP

- Изучение понятий “Маршрутизатор”, “Шлюз”, “Браузер”;
- Изучение уровней стека TCP/IP;
- Обсуждение различий между протоколами OSI и TCP/IP.

Практическое задание: практический разбор применения протоколов TCP/IP.

.

27. Протоколы и сферы их применения

- Изучение различных протоколов;
- Расположение протоколов относительно модели TCP/IP.

Практическое задание: расположить протоколы по соответствующим уровням.

28. Протокол http. Локальные, глобальные, частные и публичные сети

- Изучение основных header протокола http;
- Изучение основных методов протокола http;
- Плюсы и минусы протокола http;
- Изучение принципов работы локальных, глобальных, частных и публичных сетей.

Практическое задание: практический разбор принципа работы http протокола для запроса сайта.

29. Знакомство с командной строкой Windows

- Преимущества Windows;
- Знакомство с функциями командной строки Windows;
- Практика - запись команд в командной строке Windows.

Практическое задание: создание папки и файлов с помощью командной строки.

30. Новые команды и фишки командной строки Windows

- Изучение различных протоколов;
- Расположение протоколов относительно модели TCP/IP.- Изучение новых команд командной строки Windows;
- Использование различных фишек командной строки;
- Практика - запись новых команд в командной строке Windows.

Практическое задание: изменение интерфейса рабочего стола с помощью командной строки.

31. Знакомство с ОС Linux

- Знакомство с протоколом SSH;
- Установка дополнительных приложений;
- Знакомство с ОС Linux и первыми командами.

Практическое задание: запись команд для работы с файлами и папками с помощью командной строки.

32. Знакомство с понятиями "IP" и "порт". Сравнение ОС Windows и Linux

- Знакомство с дополнительными командами Linux;
- Знакомство с понятиями "IP" и "порт";
- Сравнение двух ОС Windows и Linux.

Практическое задание: сравнительный анализ двух ОС, определение плюсов и минусов каждой.

33. Знакомство и практика работы с VPN

- Знакомство с понятием VPN;
- Установка VPN сервера;
- Решение практических задач на работу с VPN.

Практическое задание: прохождение испытания Meow в команде.

34. Знакомство и практика работы с FTP

- Знакомство с протоколом FTP;
- Решение практических задач на выявление уязвимостей, связанных настройками службы FTP.

Практическое задание: прохождение испытания Fawn в команде.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контроль знаний, умений и навыков

Формой подведения итогов реализации дополнительной образовательной программы выступает текущая, промежуточная и итоговая аттестация.

Образовательный процесс осуществляется на основании учебного плана и регламентируется расписанием занятий для каждой учебной группы.

В целях оценки показателей знаний, умений и навыков обучающихся по дополнительной образовательной общеразвивающей программе "Этичный хакер" проводится текущий и промежуточный контроль знаний, а также итоговая аттестация.

Виды текущего контроля:

- устный ответ на поставленный вопрос;
- проверка результатов выполнения практических заданий.

Виды промежуточного контроля:

- тестирование устное/письменное/с помощью электронных форм;
- проверка результатов выполнения практических работ/проектов по итогам учебного модуля.

Тестирование - это форма измерения знаний обучающихся, основанная на применении тестов. Материалы для промежуточного и итогового тестирования предоставляются вместе с комплектом учебно-методических материалов к программе.

Итоговая аттестация

Итоговая аттестация проводится с целью установления уровня знаний обучающихся с учетом прогнозируемых результатов обучения и требований к результатам освоения образовательной программы.

Итоговая аттестация обучающихся осуществляется в форме защиты проекта с демонстрацией результатов – личного цифрового портфолио в по тематике информационной и кибербезопасности, которое сопровождается презентацией. Презентация – это электронный документ, предназначенный для визуальной демонстрации выполненной работы. Как правило, презентация имеет сюжет, сценарий и структуру, созданную для удобного восприятия информации.

Выдача обучающимся документов о дополнительном образовании (сертификат о прохождении курса) осуществляется при условии успешного прохождения итоговой аттестации.

5.2. Критерии оценивания освоения программы при проведении различных форм контроля:

Тестирование (Приложение 1. Примерные вопросы для промежуточного тестирования). Процент результативности (правильных ответов при выполнении тестовых заданий):

Выполнение теста	**Итоговая оценка**
70% и более правильных ответов	"Зачтено"
Менее 70% правильных ответов	"Не зачтено"

Проверка выполнения практических работ (Приложение 2. Примерные задания для проверки усвоения качества учебного материала). Система оценивания:

"Зачтено" – необходимый уровень выполнения задания достигнут, обучающийся демонстрирует хорошее знание теоретической и практической части материала занятия/учебного модуля, достигнуты промежуточные и/или итоговые результаты работы над заданием.
"Не зачтено" - необходимый результат/уровень освоения не достигнут, обучающийся не усвоил теоретические основы и/или изученные практические приемы и инструменты в сфере информационной безопасности, не достиг промежуточных и итоговых результатов при выполнении задания.

Проверка результатов создания проекта на итоговой аттестации:

Критерии оценки цифрового портфолио	**БАЛЛЫ**
Полнота содержания портфолио	0-3 балла
Участие в командных проектах	0-2 балла
Инновационность решений	0-4 балла
Глубина анализа уязвимостей	0-5 балла
Реализуемость технических решений	0-5 балла
Коммуникативные навыки	0-3 балла
Самостоятельность работы над проектом	0-2 балла
Компетентность докладчика (ответы на вопросы)	0-2 балла
Итоговая оценка: «Не зачтено» «Зачтено»	 **0-17 баллов** **18-26 баллов**

6. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ (УЧЕБНИКИ, РАЗДАТОЧНЫЕ МАТЕРИАЛЫ, МЕТОДИЧЕСКИЕ УКАЗАНИЯ, ПЛАКАТЫ, СЛАЙДЫ, ИНТЕРНЕТ-РЕСУРСЫ)

6.1. Информационные и учебно-методические условия реализации программы

Учебно-методический комплект

Для реализации целей и задач обучения по используется общеобразовательной общеразвивающей программы "Этичный хакер" используется комплект материалов преподавателя, который включает:

1. Текстовое методическое пособие с описанием целей, результатов каждого занятия, теоретического материала и практических работ.
2. Видеоурок для преподавателя с методическими указаниями и порядком объяснения учебного материала.
3. Раздаточный материал для учащихся - описание дополнительной самостоятельной работы учащихся по каждому занятию с примерами и рекомендациями по выполнению.
4. Описание мероприятий по контролю знаний – тестовые вопросы, практические задания.
5. Рекомендации по проведению итоговой аттестации и защиты проектов.
6. Дополнительные материалы – презентации по тематике занятий, материалы по работе с дополнительными источниками.
7. Дополнительные материалы – инструкции по установке необходимого программного обеспечения, описание технических требований к компьютерному оборудованию.

Материалы преподавателя размещаются на учебном портале преподавателей, размещенном на сервере информационно-телекоммуникационной сети "Интернет", и доступны по ссылке для всех преподавателей курса. Материалы обучающихся раздаются в печатном виде или рассылаются преподавателем индивидуально каждому обучающемуся.

6.2. Рекомендованная литература для обучающихся

Основная:

1. Наместникова, М. С. Информационная безопасность, или На расстоянии одного вируса : 7—9-е классы : учебное пособие / М.С. Наместникова — 5-е изд., стер. — Москва : Просвещение, 2023. —79 с.
2. Цветкова, М.С., Хлобыстова, И.Ю. Информационная безопасность. Кибербезопасность. 7–9 класс. Учебное пособие. Москва: БИНОМ. Лаборатория знаний, 2023.
3. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с.
4. Информатика. Начало программирования на языке Python : 8-9-е классы : дополнительные главы к учебникам / Л.Л. Босова, Н.А. Аквилянов, И.О. Кочергин [и др.] — 4-е изд., стер. — Москва : Просвещение, 2023, — 96 с.

Дополнительная:

5. Python для детей. Самоучитель по программированию / Дж. Бриггс; пер. с англ. С. Ломакин ; [науч. ред. Д. Абрамова]. — М.: Манн, Иванов и Фербер, 2017. — 320 с.
6. Уитни, Д.. Программирование для детей. Учимся создавать сайты, приложения и игры. HTML, CSS и JavaScript. пер. с англ. Рузмайкина И., ред. Римицан Н. М: Питер, 2022. — 208 с
7. Социальная инженерия и этичный хакинг на практике / пер. с англ. В. С. Яценкова. – М.: ДМК Пресс, 2023. – 226 с
8. Треволт, Д. Защита и укрепление Linux. / пер. Слинкин А. А. М: ДМК-Пресс, 2023. — 618 с.

6.3. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", рекомендованных для освоения программы

9. https://safety.google/families/ - Безопасный интернет от компании Google.
10. http://www.ligainternet.ru/ — крупнейшая и наиболее авторитетная в России организация, созданная для противодействия распространению опасного контента во всемирной сети.
11. https://myttk.ru/ — детский онлайн-конкурс по безопасному использованию Интернета. Советы детям, педагогам и родителям, полезные ссылки.
12. https://rocit.ru/ — Ваш помощник в Интернете. Для детей старшего школьного возраста и родителей. Общественная организация, объединяющая активных интернет-пользователей России.
13. https://xn----otbbaj8ai.xn--p1ai/ — обучающая игра «И-риски.рф».
14. https://skillbox.ru/media/code/test-naskolko-khorosho-ty-razbiraeshsya-v-virusakh-i-kiberatakakh/ — тест “Насколько хорошо ты разбираешься в вирусах и кибератаках?”

7. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

7.1. Материально-техническая и ресурсная база

Для реализации программы предполагается использование учебных аудитории для проведения занятий лекционного типа, занятий семинарского типа, выполнения проектных работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации:

- Компьютерные классы, обеспечивающие доступ в Интернет, и оснащенные мультимедиа проектором или иными средствами визуализации учебного материала, магнитной доской или флипчартом.
- Электронный информационно-образовательный портал, размещенный на сервере в информационно-телекоммуникационной сети "Интернет".
- Специальное программное обеспечение для веб-разработки, необходимое для реализации образовательных задач курса.
- Стандартное программное обеспечение для работы над разработкой учебно-методических материалов.
- Мастерские и аудитории для проведения открытых занятий.
- Специальных помещений, предполагающих наличие какого-либо специального оборудования для реализации данной программы, не предусматривается.

7.2. Кадровое обеспечение программы

Образовательный процесс по программе осуществляется педагогом дополнительного образования с профильным высшим или средним профессиональным образованием.
К занятию педагогической деятельностью по дополнительной общеобразовательной программе также допускаются лица, обучающиеся по образовательным программам высшего образования по специальностям и направлениям подготовки, соответствующим направленности дополнительных общеобразовательных программ, и успешно прошедшие промежуточную аттестацию не менее чем за два года обучения.
Реализация дополнительной общеобразовательной (общеразвивающей) программы обеспечивается руководящими и педагогическими работниками организации, а также лицами, привлекаемыми к реализации программы на условиях гражданско-правового договора.
У педагогического работника, реализующего дополнительную общеобразовательную программу, должны быть сформированы основные компетенции, необходимые для обеспечения успешного достижения обучающимися планируемых результатов освоения программы, в том числе умения:

- обеспечивать условия для успешной деятельности, позитивной мотивации, а также самомотивирования обучающихся;
- осуществлять самостоятельный поиск и анализ информации с помощью современных информационно-поисковых технологий;
- разрабатывать программы учебных предметов, выбирать учебники и учебно-методическую литературу, рекомендовать обучающимся дополнительные источники информации, в том числе Интернет-ресурсы;
- реализовывать педагогическое оценивание деятельности обучающихся;
- работать с текстовыми редакторами, электронными таблицами, электронной почтой и браузерами, мультимедийным оборудованием.

Приложения

Приложение 1. Примерные вопросы для промежуточного тестирования

1. **Кто такой хакер?**
   - Очень хороший программист
   - IT-шник высшего класса, Психолог, Программист
   - Человек, который умеет взламывать системы
   - Программист, вставший против законов

2. **Как работает алгоритм?**
   - Каждый алгоритм в программировании реализуется по крайней мере в три шага
   - Включение. Выводы
   - Получение данных. Выполнение вычислений. Вывод результата.
   - Включение. Проверка кода. Выводы

3. **Какой дистрибутив Linux самый хакерский?**
   - Kali Linux
   - Yellow Dog
   - Xubuntu
   - CrunchBang

4. **Как специалист по информационной безопасности, какое точное определение вы дадите понятию “конфиденциальная информация”?**
   - То же самое, что корпоративная информация
   - Логин и пароль пользователя
   - Закрытая информация о товаре, которая должна быть известна только сотрудникам организации
   - Информация, которая должна быть защищена от несанкционированного доступа и использования

5. **К какой команде можно отнести этичного хакера?**
   - Blue Team
   - Red Team
   - Команда аудита
   - Команда информационной безопасности

6. **Кто такой пентестер?**
   - специалист, который создает правила работы с информацией в организации и обучает этим правилам других сотрудников
   - взломщик корпоративной компьютерной сети
   - крутой программист, который умеет писать программы по взлому пароля
   - то же самое, что “черный хакер”
   - специалист, которые проверяет уязвимости в информационной системе компании

7. **Как называются атаки, которые основаны на обмане, например, злоумышленник посылает электронное письмо, которым намеревается вас встревожить или заинтриговать?**
   - Брут-форс атаки
   - Подмена данных
   - Фишинг
   - DDos атаки

8. **Какое из следующих понятий обозначает одно и то же, что "сетевая атака"?**
   - Незаконное подключение
   - Кибератака
   - Киберугроза
   - Канал утечки информации
   - Кибербезопасность

9. **Что такое инцидент в информационной безопасности?**
   - сотрудник или отдел, который следит за безопасностью информационной системы
   - случай нарушения безопасности информационной системы
   - специальная программа, которую используют злоумышленники для взлома сети
   - срочное сообщение от пользователя о том, что он не может попасть в систему

10. **Правильная система реагирования на инциденты начинается с …**
    - быстрого наказания виновного в нарушении безопасности
    - запрета соцсетей и игр на рабочих местах
    - частой смены своих паролей
    - подготовки и отслеживания работы информационной системы

11. **Что такое “компрометация учетных данных”?**
    - вирусная атака на сервер
    - ответ на сообщение от неизвестного источника
    - ситуация, когда пользователь со своим паролем получает доступ к закрытым корпоративным данным
    - ситуация, когда злоумышленник проник в систему с паролем легального пользователя

12. Что такое аутентификация?

- получение от пользователя логина и пароля
- проверка логина и пароля пользователя на совпадение с логином и паролем из базы данных
- окошко для ввода логина и пароля при входе в компьютер
- окошко для ввода логина и пароля при входе в личный кабинет пользователя на сайте

13. Что такое шифрование?

- Замена символов звездочками при вводе пароля
- кодирование информации с помощью шифра - ключа
- передача информации по защищенному каналу
- создание сложных паролей для пользователей

14. Можно ли написать в Python знак плюс (“+”), чтобы сложить две текстовые строки?

- да можно, получится единая строка
- нет, нельзя, сложить можно только данные числового типа
- можно, если предварительно преобразовать строки с помощью операции str.

15. Что делает закон 159-ФЗ?

- Защищает персональные данные
- Регулирует использование электронных подписей
- Защищает корпоративную информацию
- Обеспечивает бесплатный доступ к интернету во всех школах

Приложение 2. Примерные задания для оценки качества освоения учебного материала

Задание 1.

На сайте HTML-academy пройти главу «Знакомство с формами». Глава находится в разделе «Основы HTML». В сервисе присутствуют объяснения к каждому заданию, следуя которым довольно просто выполнить все задания.

Задание 2.

Просмотрите видео на тему фишинга: https://www.youtube.com/watch?v=8rKsGYOhtUQ

Ответьте на вопросы:

- Что такое фишинг?
- Что такое фишинговый сайт?
- Как можно определить, что сайт является фишинговым?

Задание 3.

Установите на свой компьютер программу Bitvise. Подсказка по установке: https://www.youtube.com/watch?v=1uxlogd22Ic Выполните и сделайте скриншот выполнения следующих заданий (Скриншот можно сделать с помощью клавиши ***prtscr***):

a. Создать папку со своим именем (команда: mkdir ‘Название папки’)
b. Перейти в неё (команда: cd ‘Название папки’)
c. Создать файл с любым название (команда: touch ‘Название файла’)
d. Перейти в файл, написать в нём какую-либо фразу (команда: vi ‘название файла’)
e. Сохранить изменения (внутри команды vi выполнить команду ‘:wq’)
f. Вывести содержимое файла на экран (команда: cat ‘название файла’)
g. Отобразить текущий каталог (команда: ls)
h. Удалить файл (команда: rm ‘Название файла’)

Задание 4.

Загрузите 3 страницы авторизации любых сайтов. Например: steam, Instagram, facebook. (Для того чтобы загрузить страницу, необходимо нажать сочетание клавиш ***Ctrl + S***).

Задание 5.

Самостоятельно выполните задания 1-11 с сайта Overthewire. Для решения задач можете воспользоваться сайтом с решением: https://rundata.wordpress.com/2013/03/21/overthewire-bandit-wargame-solutions-1-24/

Задание 6.

1) Определите верность IP-адресов:
127.0.0.1, 12.3.3.3.1, 132.132.132.132, 10.10.8.8
(IP-адрес должен состоять из 4-ех чисел, разделённых точкой, каждое число должно быть в диапазоне от 0 до 255)

2) Переведите числа из двоичной системы в десятичную: 111, 1010, 111001

3) Переведите числа из десятичной системы в двоичную: 5, 12, 33

Для решения заданий можно воспользоваться калькулятором в режиме программиста.

Задание 7.

Зашифруйте пословицу «Карл у Клары украл кораллы» 3-мя шифрами:

1) Цезарь

2) Вижинера

3) Квадрат Полибия

Для шифрования можно использовать сайт https://calculatorium.ru/cryptography/

Задание 8.

Напишите программу, в которой пользователь вводит 3 числа, программа должна определить, какое из этих чисел больше.

Задание 9

Напишите программу, в которой пользователь вводит число, программа выводит все делители числа (Делитель – число, на которое делимое делится без остатка. Например для числа 10 делителями являются 10, 5, 2, 1) .

Задание 10.

Напишите программу, в которой пользователь вводит строку, программа должна вывести это слово без первой и последней буквы.