Министерство образования Тульской области
Государственное профессиональное образовательное учреждение Тульской области
«Тульский государственный машиностроительный колледж
Имени Никиты Демидова»

УТВЕРЖДАЮ
Директор ГПОУ ТО
«ТГМК им. Н. Демидова»
_____ Салищев В.Н.
Приказ № 117/1-А
От «29» августа 2022 г.

Дополнительная образовательная программа

технической направленности

«Школа информационной безопасности. 144 ч.»

Возраст обучающихся: *13 – 17 лет*

Уровень*: базовый*

Срок реализации: 1 год

Автор-составитель:

Подымов Алексей Игоревич,
педагог дополнительного образования

г. Тула, 2022 г.

Содержание

1. Основные характеристики программы 3
1.1. Пояснительная записка 3
1.2. Цель и задачи программы 4
2. Структура программы 5
2.1. Объём программы и виды учебной работы 5
2.2. Учебно-тематический план 5
2.3. Содержание программы 8
3. Комплекс организационно-педагогических условий 12
3.1. Календарно-тематическое планирование 12
3.2. Условия реализации программы 18
3.3. Планируемые результаты освоения программы 19
3.4. Способы и формы проверки результатов освоения программы 19
3.5. Учебно-методическое и информационное обеспечение программы 19

1. Основные характеристики программы

1.1. Пояснительная записка

№ п/п	Наименование пункта	Содержание пункта
1.	Направленность (профиль) программы	Техническая
2.	Актуальность программы	В связи с активным проникновение компьютерных технологий во все сферы общественной и личной жизни понимание основ функционирования информационных систем, угроз информационной безопасности и методов защиты информационных систем являются весьма актуальными направлениями на сегодняшний день
3.	Отличительные особенности программы	Отличительными особенностями данной программы является ее практическая направленность. Также в программе уделено особое внимание методам реализации угроз информационной безопасности для понимания какие структурно-функциональные характеристики информационных систем могут быть уязвимыми.
4.	Адресат программы	Учащиеся общеобразовательных учреждений 7-9 классов
5.	Объем и срок освоения программы	1 уч. год, 144 часа
6.	Формы обучения	Очная
7.	Особенности организации образовательного процесса	В соответствии с индивидуальными учебными планами в объединениях по интересам, сформированных в группы учащихся одного возраста
8.	Режим занятий, периодичность и продолжительность занятий	общее количество часов в год – 144 ч.; количество часов и занятий в неделю – 3 ч./2 занятия в неделю; периодичность и продолжительность занятий – на еженедельной основе, 1,5 ч. – 1 занятие.

1.2. Цель и задачи программы

Целью данной программы является развитие у учащихся понимания основ функционирования информационных систем и отдельных технологий их составляющих. Задачами данной программы является формирование у учащихся навыков использования данных технологий, в частности:

- навыки построения и администрирования сетей в эмуляторе сетей Cisco Packet Tracer;
- навыки настройки межсетевого экрана (уровня узла, уровня сети);
- навыки анализа заголовков сетевых сообщений, перехваченных снифером Wireshark;
- навыки написания скриптов для командного интерпретатора ОС MS Windows
- навыки установки и настройки дистрибутива CentOS 7;
- навыки анализ сети сканером сетей nmap;
- навыки анализа wi-fi сетей inSSIDer;
- навыки атаки на ПК при физическом доступе при помощи liveUSB;
- навыки использования инструментов пен-тестера дистрибутива KaliLinux для проведения атак на информационные системы;
- навыки работы с различными кодировками, применяемыми в Web-среде;
- знаниями о применяемых web-технологиях (архитектуры сайта, языки программирования);
- знания о применяемых системах управления базами данных;
  навыки написания запросов на языке SQL.

Одной из важных задач данной программы является развитие у учащихся понимания того, какие структурно-функциональные характеристики информационных систем могут быть уязвимы с точки зрения информационной безопасности и использованы злоумышленником при реализации угроз. Для этого необходимо формировать у учащихся практические навыки анализа информационных систем с точки зрения информационной безопасности и проведения атак на информационные системы, в частности:

- методы атак с помощью социальной инженерии, и способы противодействовать таким атакам;
- анализ wi-fi сетей с точки зрения информационной безопасности, методы атак на wi-fi сети и способы защиты;
- анализ web-сайта на наличие уязвимостей;
- навыки работы с ПО, позволяющим перехватывать сетевые запросы.

2. Структура программы

2.1. Объём программы и виды учебной работы

Общий объем программы составляет 144 часа.

Программа включает следующие виды учебной работы: теоретические занятия, практические занятия, проектная деятельность, итоговый экзамен.

2.2. Учебно-тематический план

№ п/п	Название раздела, темы	Количество часов			Форма контроля
		Всего	Теория	Практика	
1.	Введение в информационную безопасность: - Информационная безопасность. - Этичный хакинг. Правовые аспекты	2	2	-	-
2.	Безопасность компьютерных сетей: - Модель OSI. Стек протоколов TCP/IP. - Физический уровень. Канальный уровень. - Протокол Ethernet. - Канальный уровень. - Протокол Wi-Fi. - Сетевой уровень. - Транспортный уровень. - Прикладной уровень.	44	26	18	Успешное выполнение практического занятия
3.	Командный интерпретатор ОС Windows, скрипты	2	1	1	Успешное выполнение практического занятия
4.	Безопасность ОС Linux: - Введение в ОС Linux. Установка. Файловая структура. Командный интерпретатор. - Пользователи и права доступа в ОС Linux. - Настройка сетевых интерфейсов ОС Linux. - Установка программ в ОС Linux. - Дистрибутив Kali Linux с набором утилит для этичного хакинга.	10	5	5	Успешное выполнение практического занятия
5.	Атаки на различные ОС: - Атаки при физическом доступе к ПК.	2	1	1	Успешное выполнение практического занятия

№ п/п	Название раздела, темы	Количество часов			Форма контроля
		Всего	Теория	Практика	
	- Атаки при удаленном доступе к ПК с использованием уязвимостей настройки ОС. - Атаки при удаленном доступе к ПК с использованием уязвимостей ОС и ПО.				
6.	Проектная деятельность: - Проектирование и администрирование сетей на базе протокола TCP/IP. - Скрипт, реализующий защиту ПК от несанкционированного доступа. - Установка и администрирование ОС Linux	6	-	6	Успешное выполнение проектов
7.	Промежуточный зачет	6	-	6	Успешное прохождение зачета
8.	Сбор информации. Изучение сбора информации с помощью интернета. Google dorks.	2	1	1	Выполнение практического задания
9.	Криптография. Виды шифрования.	8	4	4	Выполнение практического задания
10.	Стеганография: - Методы сокрытия информации в текстовых файлах, файлах изображений, аудиофайлах. - Стеганоанализ.	3	2	1	Выполнение практического задания
11.	Социальная инженерия: - Виды атак с помощью социальной инженерии. - Изучение мер предосторожности и противодействия.	2	1	1	Выполнение практического задания
12.	Безопасность Wi-fi Концепция. - Шифрование данных wi-fi (XOR, WEP, WPA, WPA2). - Протокол WPS. Угрозы. - Методология атак на сети wi-fi. Контрмеры.	8	4	4	Выполнение практического задания
13.	Основы WEB-технологий www и Интернет:	12	6	6	Выполнение практического задания

№ п/п	Название раздела, темы	Количество часов			Форма контроля
		Всего	Теория	Практика	
	- Язык разметки HTML. - Протокол HTTP. - Методы передачи данных (POST и GET запросы). - Архитектура WEB-приложений. - Работа с СУБД. MITM-атаки.				
14.	Основы языка SQL: - Основы реляционных баз данных, СУБД. - Синтаксис языка СУБД SQL. Понятие SQL-инъекции.	5	3	2	Выполнение практического задания
15.	WEB-уязвимости: - Исследование WEB-приложения. - DNS/whois. Portscanning. - Анализ http-запросов и ответов. - Кодировка. Раскрытие данных. - Локальное включение файлов. Path Traversal. - Внедрение комманд. SQL-инъекции.	13	8	5	Выполнение практического задания
16.	- Cross-Site Scripting (XSS). - Межсайтовая подделка запроса (CSRF). - Инъекция заголовков и фиксация сессий. Пост-эксплуатация.	7	4	3	Выполнение практического задания
17.	Проект. - Проверка пользователей организации методами социальной инженерии	4	-	4	Составление и защита отчета
18.	Проект. - Исследовать тестовый сайт на наличие уязвимостей.	4	-	4	Составление и защита отчета
19.	Экзамен. Итоговая проверка знаний и навыков учащихся, путем реализации информационных атак на «некую организацию» (тестовая среда, подготовленная преподавателями), и реализация методов защиты данной «организации».	4	-	4	Выполнение задания экзамена.

2.3. Содержание программы

№ п/п	Название раздела, темы	Содержание обучения
1.	Введение в информационную безопасность: - Информационная безопасность. - Этичный хакинг. Правовые аспекты	Основные вопросы курса. Объяснение целей и методов достижения. Объяснение ответственности с точки зрения закона РФ.
2.	Безопасность компьютерных сетей: - Модель OSI. Стек протоколов TCP/IP. - Физический уровень. Канальный уровень. - Протокол Ethernet. - Канальный уровень. - Протокол Wi-Fi. - Сетевой уровень. - Транспортный уровень. - Прикладной уровень.	– Введение в компьютерные сети. Модель OSI. Стэк протоколов TCP/IP. – Канальный уровень – назначение. Место в модели OSI. Понятие MAC-адрес и VLAN. Понятие и назначение протокола STP. Подключение и настройка сетевого коммутатора. Настройка безопасности коммутатора. Настройка работы протокола STP и RSTP. Демонстрация разницы работы между этими двумя протоколами. Настройка 2 VLAN на коммутаторе. – Wi-fi на канальном уровне. Поверхностный анализ wi-fi с помощью программы INSSIDER. Назначение, применение и рекомендации по защите wi-fi сетей. – Исследование протокола ARP в wireshark. Перехват пары логин/пароль, переданных через незашифрованный протокол с помощью сетевого анализатора пакетов wireshark. – Сетевой уровень – назначение. Место в модели OSI и TCP/IP. Назначение. Фрагментация. Маршрутизация. Протокол IP. Сервисы IP. Формат заголовка IP-пакета. IP-адресация. Исследование сетевых пакетов на сетевом уровне с помощью ПО Wireshark. Настройка маршрутизации для сети из нескольких устройств. Настройка DHCP на примере простой сети. – Транспортный уровень – назначение. Место в моделях OSI и TCP/IP. Сервис транспортного уровня. Адреса и порты. Типы портов. Протокол UDP. Протокол TCP. Понятие инкапсуляции и декапсуляции и разъяснение данных процессов. Понятие и цели создания NAT. Внешние и внутренние ip-адреса. Способы трансляции адресов. Понятие и назначение DMZ. Понятие и назначение VPN. Понятие и назначение межсетевых экранов. Исследование протокола TCP с помощью программы wireshark. Анализ портов, установки соединения TCP, инкапсуляции.

№ п/п	Название раздела, темы	Содержание обучения
		Настройка трансляции адресов с перегрузкой. Настройка списка доступов в уже созданной сети. Исследование DNS при помощи wireshark. – Понятие о прикладном уровне сетей. Место в моделях OSI и TCP/IP. Протоколы прикладного уровня. Протокол HTTP. Протокол DNS. Протокол FTP. Протоколы электронной почты. Настройка FTP-сервера. Исследование протокола SMTP, демонстрация атаки на пользователя при помощи данного протокола.
3.	Командный интерпретатор ОС Windows, скрипты	ОС Windows – понятие, история. Файловая система NTFS. Командная строка и основные команды. Написание скриптов для ОС семейства windows.
4.	Безопасность ОС Linux: - Введение в ОС Linux. Установка. Файловая структура. Командный интерпретатор. - Пользователи и права доступа в ОС Linux. - Настройка сетевых интерфейсов ОС Linux. - Установка программ в ОС Linux. - Дистрибутив Kali Linux с набором утилит для этичного хакинга.	ОС Linux – понятие, история. Ядро. Дистрибутивы. Файловая система Linux. Консоль и основные команды. Настройка сети. Создание пользователей. Установка программ. Установка дистрибутива ОС Linux. Настройка сети. Создание учетных записей. Установка программ.
5.	Атаки на различные ОС: - Атаки при физическом доступе к ПК. - Атаки при удаленном доступе к ПК с использованием уязвимостей настройки ОС. - Атаки при удаленном доступе к ПК с использованием уязвимостей ОС и ПО.	– Изучение различных методов атак на информационную систему, с использованием различного ПО и видов доступа. Создание live-usb. Загрузка с live-usb. Подмена экранной клавиатуры на командную строку. – Обфускация вредоносного ПО. Использование ПО keylogers. Изучение ПО hydra по подбору пароля на практике. Сканирование сети nmap. – Демонстрация атак на различные операционные системы с помощью ПО metasploit.
6.	Проектная деятельность: - Проектирование и администрирование сетей на базе протокола TCP/IP. - Скрипт, реализующий защиту ПК от несанкционированного доступа.	– Решение задач по проектированию локальной вычислительной сети. – Написание bat-файла, реализующего функционал средства защиты от несанкционированного доступа. – Администрирование и настройка ОС Linux на практике.

№ п/п	Название раздела, темы	Содержание обучения
	- Установка и администрирование ОС Linux	
7.	Промежуточный зачет	Реализация сетевой атаки на лабораторию, имитирующий офис компании. Цель – экзамена: проведение разведки по изначальным данным, проникновение в сеть предприятия, копирование нужных данных.
8.	Сбор информации. Изучение сбора информации с помощью интернета. Google dorks.	Изучение сбора информации об организации с помощью интернет-ресурсов, включая различные google-запросы. Умение делать выводы из полученной информации.
9.	Криптография. Виды шифрования.	Ассиметричное и симметричное шифрование. Хэш-функции. Кодирование в WEB. SSL/TLS. Криптоанализ.
10.	Стеганография: - Методы сокрытия информации в текстовых файлах, файлах изображений, аудиофайлах. - Стеганоанализ.	Изучение методов сокрытия информации в различных видах файлов, изучение методов и средств для проведения анализа файлов на наличие скрытой информации.
11.	Социальная инженерия: - Виды атак с помощью социальной инженерии. - Изучение мер предосторожности и противодействия.	Изучения атак с помощью социальной инженерии, виды атак, цели. Контрмеры для предотвращения атак подобного рода.
12.	Безопасность Wi-fi Концепция. - Шифрование данных wi-fi (XOR, WEP, WPA, WPA2). - Протокол WPS. Угрозы. - Методология атак на сети wi-fi. Контрмеры.	Изучение шифрования в сетях wi-fi, методологии атак на wi-fi сети и контрмеры от взлома wi-fi сетей.
13.	Основы WEB-технологий www и Интернет: - Язык разметки HTML. - Протокол HTTP. - Методы передачи данных (POST и GET запросы). - Архитектура WEB-приложений. - Работа с СУБД. MITM-атаки.	Изучение основ WEB-технологий, структуры сайтов и языка HTML. Изучение методов и протоколов передачи и получения данных в среде WEB. Изучение работы систем управления базами данных и их интегрированности с сайтами. Изучение атак типа «Человек-по-середине».
14.	Основы языка SQL: - Основы реляционных баз данных, СУБД. - Синтаксис языка СУБД SQL. Понятие SQL-инъекции.	Изучение основных систем управления базами данных, использующих язык SQL. Синтаксис и изучение основ составления запросов на языке SQL. Понятие SQL-инъекции, угрозы и степени риска.
15.	WEB-уязвимости: - Исследование WEB-приложения.	Изучение, анализ и реализация web-уязвимостей. Анализ сайта, сканирование портов, анализ http-

№ п/п	Название раздела, темы	Содержание обучения
	- DNS/whois. Portscanning. - Анализ http-запросов и ответов. - Кодировка. Раскрытие данных. - Локальное включение файлов. Path Traversal. - Внедрение комманд. SQL-инъекции.	запросов и http-ответов. Изучение средств для анализа сайтов.
16.	- Cross-Site Scripting (XSS). - Межсайтовая подделка запроса (CSRF). - Инъекция заголовков и фиксация сессий. Пост-эксплуатация.	Изучение web-уязвимостей со стороны клиента. Анализ действий потенциального злоумышленника после успешно проведенной атаки на сайт. Реализация бэкдора.
17.	Экзамен	Реализация сетевой атаки на лабораторию, имитирующий офис компании. Цель – экзамена: проведение разведки по изначальным данным, проникновение в сеть предприятия, копирование нужных данных.

3. Комплекс организационно-педагогических условий

3.1. Календарно-тематическое планирование

№ п/п	Тема занятия	Форма занятия	Кол-во часов
Введение в информационную безопасность			
1.	Информационная безопасность. Этичный хакинг. Правовые аспекты	занятие-презентация, занятие-демонстрация	2
Безопасность компьютерных сетей			
2.	Модель OSI. Стек протоколов TCP/IP	занятие-презентация, занятие-демонстрация, практическое занятие	4
3.	Физический уровень	занятие-презентация, занятие-демонстрация, практическое занятие	2
4.	Канальный уровень. Протокол Ethernet.	занятие-презентация, занятие-демонстрация, практическое занятие	6
5.	Канальный уровень. Протокол Wi-Fi	занятие-презентация, занятие-демонстрация, практическое занятие	4
6.	Сетевой уровень	занятие-презентация, занятие-демонстрация, практическое занятие	6
7.	Транспортный уровень	занятие-презентация, занятие-демонстрация, практическое занятие	6
8.	Прикладной уровень	занятие-презентация, занятие-демонстрация, практическое занятие	8
Командный интерпретатор ОС Windows, скрипты			
9.	Командный интерпретатор ОС Windows, скрипты	занятие-презентация, занятие-демонстрация, практическое занятие	4
Безопасность ОС Linux			
10.	Введение в ОС Linux. Установка. Файловая структура. Командный интерпретатор	занятие-презентация, занятие-демонстрация, практическое занятие	2

№ п/п	Тема занятия	Форма занятия	Кол-во часов
11.	Пользователи и права доступа в ОС Linux	занятие-презентация, занятие-демонстрация, практическое занятие	2
12.	Настройка сетевых интерфейсов ОС Linux	занятие-презентация, занятие-демонстрация, практическое занятие	2
13.	Установка программ в ОС Linux	занятие-презентация, занятие-демонстрация, практическое занятие	2
14.	Дистрибутив Kali Linux с набором утилит для этичного хакинга	занятие-презентация, занятие-демонстрация, практическое занятие	2
Атаки на различные ОС			
15.	Атаки при физическом доступе к ПК	занятие-презентация, занятие-демонстрация, практическое занятие	2
16.	Атаки при удаленном доступе к ПК с использованием уязвимостей настройки ОС	занятие-презентация, занятие-демонстрация, практическое занятие	2
17.	Атаки при удаленном доступе к ПК с использованием уязвимостей ОС и ПО	занятие-презентация, занятие-демонстрация, практическое занятие	2
Проектная деятельность			
18.	Проектирование и администрирование сетей на базе протокола TCP/IP	практическое занятие, занятие-соревнование	4
19.	Скрипт, реализующий защиту ПК от несанкционированного доступа	практическое занятие, занятие-соревнование	2
20.	Установка и администрирование ОС Linux	практическое занятие, занятие-соревнование	2
Зачет			
21.	Зачет	практическое занятие, занятие-соревнование	6
Сбор информации.			
22	Изучение сбора информации с помощью интернета. Google dorks.	занятие-презентация, занятие-демонстрация	1

№ п/п	Тема занятия	Форма занятия	Кол-во часов
23	Использование google dorks на практике	занятие-демонстрация, практическое занятие	1
	Криптография.		
22.	Ассиметричное и симметричное шифрование. Хэш-функции	занятие-презентация, занятие-демонстрация, практическое занятие	2
23.	Кодирование в WEB.	занятие-презентация, занятие-демонстрация, практическое занятие	2
24.	SSL/TLS	занятие-презентация, занятие-демонстрация, практическое занятие	2
25.	Криптоанализ.	занятие-презентация, занятие-демонстрация, практическое занятие	2
	Стеганография		
26.	Методы сокрытия информации в текстовых файлах, файлах изображений, аудио-файлах. Стеганоанализ	занятие-презентация, занятие-демонстрация	2
27.	Практика сокрытия информации в различных файлах.	занятие-презентация, занятие-демонстрация, практическое занятие	1
	Социальная инженерия		
28.	Виды атак с помощью социальной инженерии. Контрмеры.	занятие-презентация, занятие-демонстрация	1
29.	Реализация фишинговой рассылки с предварительной подготовкой.	практическое занятие	1
	Безопасность wi-fi		
30.	Концепция wi-fi.	занятие-презентация, занятие-демонстрация	1
31.	Шифрование данных в wi-fi сетях. Протокол WPS.	занятие-презентация, занятие-демонстрация, практическое занятие	1
32.	Угрозы. Методология атак. Контрмеры.	занятие-презентация, занятие-демонстрация	2
33.	Изучение и реализация различных типов атак на сети wi-fi.	занятие-презентация, занятие-	4

№ п/п	Тема занятия	Форма занятия	Кол-во часов
		демонстрация, практическое занятие	
	Основы WEB-технологий		
34.	WWW и Интернет. Язык разметки HTML	занятие-презентация, занятие-демонстрация	1
35.	MITM-атаки	занятие-презентация, занятие-демонстрация	1
36.	Протокол передачи данных HTTP.	занятие-презентация, занятие-демонстрация	1
37.	Методы передачи данных (POST и GET запросы).	занятие-презентация, занятие-демонстрация, практическое занятие	1
38.	Архитектура WEB-приложений.	занятие-презентация, занятие-демонстрация	1
39.	Работа с СУБД	занятие-презентация, занятие-демонстрация, практическое занятие	1
40.	Практическое применение HTML	занятие-презентация, занятие-демонстрация, практическое занятие	2
41.	Изучение и работа с ПО BurpSuite. Практика по методам передачи данных. Практическое изучение протокола HTTP.	занятие-презентация, занятие-демонстрация, практическое занятие	2
42.	Реализация атаки «Человек-по-середине»	занятие-презентация, занятие-демонстрация, практическое занятие	2
	Основы языка SQL		
43.	Основы реляционных баз данных. Системы управления базами данных.	занятие-презентация, занятие-демонстрация, практическое занятие	1
44.	Синтаксис языка SQL. Понятие об SQL-инъекции	занятие-презентация, занятие-демонстрация, практическое занятие	2
45.	Практическое написание SQL-запросов	занятие-презентация, занятие-демонстрация, практическое занятие	2
	WEB-уязвимости. Часть 1		
46.	Исследование WEB-приложения. DNS/WHOIS. Portscanning.	занятие-презентация, занятие-	1

№ п/п	Тема занятия	Форма занятия	Кол-во часов
		демонстрация, практическое занятие	
47.	Анализ http-запросов и ответов.	занятие-презентация, занятие-демонстрация, практическое занятие	1
48.	Кодировка	занятие-презентация, занятие-демонстрация, практическое занятие	1
49.	Раскрытие данных	занятие-презентация, занятие-демонстрация, практическое занятие	1
50.	Локальное включение файлов. Path traversal.	занятие-презентация, занятие-демонстрация, практическое занятие	1
51.	Внедрение команд	занятие-презентация, занятие-демонстрация, практическое занятие	1
52.	SQL-инъекции	занятие-презентация, занятие-демонстрация, практическое занятие	2
53.	Практика анализа http-запросов и ответов	занятие-презентация, занятие-демонстрация, практическое занятие	1
54.	Разбор распространенных кодировок и использование он-лайн декодеров.	занятие-презентация, занятие-демонстрация, практическое занятие	1
55.	Практическая реализация локальной загрузки файлов и уязвимости типа «Path traversal».	занятие-презентация, занятие-демонстрация, практическое занятие	1
56.	Реализация SQL-инъекции	занятие-презентация, занятие-демонстрация, практическое занятие	2
	WEB-уязвимости. Часть 2		
57.	Cross-Site Scripting (XSS). Межсайтовая подделка запроса (CSRF).	занятие-презентация, занятие-демонстрация, практическое занятие	2
58.	Инъекция заголовков и фиксация сессий	занятие-презентация, занятие-	1

№ п/п	Тема занятия	Форма занятия	Кол-во часов
		демонстрация, практическое занятие	
59.	Пост-эксплуатация	занятие-презентация, занятие-демонстрация, практическое занятие	1
60.	Поиск и реализация XSS.	занятие-презентация, занятие-демонстрация, практическое занятие	2
61.	Реализация бэкдора, как пост-эксплуатация успешной атаки.	занятие-презентация, занятие-демонстрация, практическое занятие	1
Проекты и экзамены			
62.	Проверка пользователей организации методами социальной инженерии	практическое занятие, занятие-соревнование	4
63.	Исследование тестового сайта на наличие уязвимостей.	практическое занятие, занятие-соревнование	4
64.	Экзамен. Итоговая проверка знаний и навыков учащихся, путем реализации информационных атак	практическое занятие, занятие-соревнование	4

3.2. Условия реализации программы

№ п/п	Условия реализации программы	Характеристика условий реализации программы
1.	Материально-техническое обеспечение	Изучение материала программы ориентировано на работу в компьютерном классе на 14 рабочих мест. Учебный класс оснащен интерактивной панелью для показа презентаций. Каждое рабочее место должно быть оснащено необходимым программным обеспечением и иметь одинаковые технические характеристики. Технические характеристики компьютера: - Процессор: Intel Core i7 4790, 3600 МГц; - Оперативная память: 16384 Мб. - Видеокарта: GeForce GTX 980 4096 Мб. Программное обеспечение для каждого компьютера: - ОС Windows 8.1; - Офисный пакет Office 2016 Prof; - Среда виртуализации Oracle Virtual Box; - ОС MS Windows 7 Prof, MS Windows Server 2012 R2, дистрибутив CentOS 7, дистрибутив KaliLinux; - Среда эмуляции сети Cisco Packet Tracer; - САЗ Kaspersky Total Security
2.	Информационное обеспечение	Презентации (в MS PowerPoint); Подготовленные стенды для практических и проектных заданий (в Oracle Virtual Box, Cisco Packet Tracer); Подготовленный стенд для экзамена
3.	Кадровое обеспечение	Педагоги имеют высшее профессиональное образование в сфере информационной безопасности или информационных технологий, а также проходили курсы повышения квалификации по обеспечению безопасности ОС, сетей, этичному хакингу, анализу веб-уязвимостей. Педагоги имеют опыт работы в сфере информационной безопасности более 5 лет.

3.3. Планируемые результаты освоения программы

Результатом освоения данной программы является развитие у учащихся понимания основ функционирования информационных систем и отдельных технологий их составляющих и соответствующие навыки применения полученных знаний, в частности:

- навыки построения и администрирования сетей в эмуляторе сетей Cisco Packet Tracer;
- навыки настройки межсетевого экрана (уровня узла, уровня сети);
- навыки анализа заголовков сетевых сообщений, перехваченных снифером Wireshark;
- навыки написания скриптов для командного интерпретатора ОС MS Windows;
- навыки установки и настройки дистрибутива CentOS 7.

Также результатом освоения данной программы является понимание того, какие структурно-функциональные характеристики информационных систем могут быть уязвимы с точки зрения информационной безопасности и использованы злоумышленником при реализации угроз, а также практических навыком реализации отдельных информационных технологий и методов проведения атак на информационные системы, в частности:

- анализ сети сканером сетей nmap;
- анализ wi-fi сетей inSSIDer;
- атаки на ПК при физическом доступе при помощи liveUSB;
- навыки использования инструментов пен-тестера дистрибутива KaliLinux для проведения атак на информационные системы.

3.4.Способы и формы проверки результатов освоения программы

Проверка результатов проходит в форме:

- выполнения практических заданий,
- выполнения проектных заданий,
- прохождения экзамена.

3.5.Учебно-методическое и информационное обеспечение программы

Литература для учителя и ученика

1. М.Фленов «Linux глазами хакера»;
2. Daniel Robbins, Chris Houser, Aron Griffis «Основы Linux от основателя Gentoo»;
3. Марк Руссинович и др. «Внутреннее устройство Microsoft Windows»;
4. Шон Харрис «Подготовка к CISSP»;
5. Е.Ольков «Архитектура корпоративных сетей»;
6. Е.Ольков «Практическая безопасность сетей»

Интернет-ресурсы

1. https://www.kali.org/;
2. https://www.ptsecurity.com/ru-ru/research/analytics/;
3. https://www.asozykin.ru/courses/networks;
4. https://habrahabr.ru/company/pentestit/;
5. курс «Linux для начинающих. Базовый курс» (Online Network School “Netskills”);
6. курс «Анализ безопасности веб-проектов» (Online Network School «Stepic»);
7. курс «Web-технологии» (Online Network School «Stepic»);
8. курс «Курс молодого бойца. Практический курс с использованием cisco packet tracer» (Online Network School “Netskills”).