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 № 044/1-У

От «27» августа 2020 г.

Дополнительная образовательная программа технической направленности «Информационная безопасность. 72 ч.»

Возраст обучающихся: 14-18 лет

Уровень: многоуровневая модульная образовательная программа

Автор-составитель: Подымов Алексей Игоревич

Тула
2020 г.

Содержание

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.

№ п/п	Наименование пункта	Содержание пункта
4.	Адресат программы	Учащиеся общеобразовательных учреждений 8-10 классов
5.	Объем и срок освоения программы	1 уч. год, 72 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 – 72 ч.; количество часов и занятий в неделю – 2 ч; .

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.

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.

2. Структура программы

2.1.Объём программы и виды учебной работы

Общий объем программы составляет 72 часа. Программа включает следующие виды учебной работы: теоретические занятия, практические занятия, проектная деятельность, итоговый экзамен.

№ п/п	Название раздела, темы	Количество часов			Форма контроля
		Всего	Теория	Практика	
1.	**Раздел:** Введение в информационную безопасность **Темы:** Информационная безопасность. Этичный хакинг. Правовые аспекты	2	2	-	-
2.	**Раздел:** Безопасность компьютерных сетей **Темы:** – 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

№ п/п	Название раздела, темы	Количество часов			Форма контроля
		Всего	Теория	Практика	
3.	**Раздел:** командный интерпретатор ОС Windows, скрипты **Темы:** командный интерпретатор ОС Windows, скрипты	2	1	1	Успешное выполнение практического занятия
4.	**Раздел:** Безопасность ОС Linux **Темы:** – 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.	12	5	5	Успешное выполнение практического занятия
5.	**Раздел:** Атаки на различные ОС. **Темы:** – 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.	**Раздел:** проектная деятельность **Темы:** – Проектирование и администрирование сетей на базе протокола TCP/IP. – Скрипт, реализующий защиту ПК от несанкционированного доступа. – Установка и администрирвоание ОС Linux	6	-	6	Успешное выполнение проектов
7.	**Раздел:** экзамен	6	-	6	Успешное прохождение экзамена
	Итого	***72***	***35***	***37***	

2.2.Содержание программы

№ п/п	Название раздела, темы	Содержание обучения
1.	**Раздел:** Введение в информационную безопасность **Темы:** Информационная безопасность. Этичный хакинг. Правовые аспекты	Основные вопросы курса. Объяснение целей и методов достижения. Объяснение ответственности с точки зрения закона РФ.
2.	**Раздел:** Безопасность компьютерных сетей **Темы:** – Модель OSI. Стек протоколов TCP/IP. – Физический уровень. Канальный уровень. – Протокол Ethernet. – Канальный уровень. – Протокол Wi-Fi. – Сетевой уровень. – Транспортный 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.

№ п/п	Название раздела, темы	Содержание обучения
	– Прикладной уровень.	– 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

№ п/п	Название раздела, темы	Содержание обучения
		экранов. Исследование протокола TCP с помощью программы wireshark. Анализ портов, установки соединения TCP, инкапсуляции. 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.	**Раздел:** командный интерпретатор ОС Windows, скрипты **Темы:** командный интерпретатор ОС Windows, скрипты	ОС Windows – понятие, история. Файловая система NTFS. Командная строка и основные команды. Написание скриптов для ОС семейства windows.
4.	**Раздел:** Безопасность ОС Linux **Темы:**	ОС Linux – понятие, история. Ядро. Дистрибутивы. Файловая система Linux. Консоль и основные команды. Настройка сети. Создание пользователей. Установка

№ п/п	Название раздела, темы	Содержание обучения
	– 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.	программ. Установка дистрибутива ОС Linux. Настройка сети. Создание учетных записей. Установка программ.
5.	**Раздел:** Атаки на различные ОС. **Темы:** – Атаки при физическом доступе к ПК.	– 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.

№ п/п	Название раздела, темы	Содержание обучения
	– Атаки при удаленном доступе к ПК с использованием уязвимостей настройки ОС. – Атаки при удаленном доступе к ПК с использованием уязвимостей ОС и ПО.	– 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.	**Раздел:** проектная деятельность **Темы:** – Проектирование и администрирование сетей на базе протокола TCP/IP. – Скрипт, реализующий защиту ПК от несанкционированного доступа. – Установка и администрирвоание ОС Linux	– 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
7.	**Раздел:** 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	6
3.	Физический уровень	занятие-презентация, занятие-демонстрация, практическое занятие	6
4.	Канальный уровень. Протокол Ethernet.	занятие-презентация, занятие-демонстрация,	6

№ п/п	Тема занятия	Форма занятия	Кол-во часов
		практическое занятие	
5.	Канальный уровень. Протокол Wi-Fi	занятие-презентация, занятие-демонстрация, практическое занятие	6
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			

№ п/п	Тема занятия	Форма занятия	Кол-во часов
9.	Командный интерпретатор ОС Windows, скрипты	занятие-презентация, занятие-демонстрация, практическое занятие	2
Безопасность ОС Linux			
10.	Введение в ОС Linux. Установка. Файловая структура. Командный интерпретатор	занятие-презентация, занятие-демонстрация, практическое занятие	2
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,	2

№ п/п	Тема занятия	Форма занятия	Кол-во часов
		занятие-демонстрация, практическое занятие	
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,	2

№ п/п	Тема занятия	Форма занятия	Кол-во часов
		практическое занятие	
Проектная деятельность			
18.	Проектирование и администрирование сетей на базе протокола TCP/IP	практическое занятие, занятие-соревнование	2
19.	Скрипт, реализующий защиту ПК от несанкционированного доступа	практическое занятие, занятие-соревнование	2
20.	Установка и администрирование ОС Linux	практическое занятие, занятие-соревнование	2
Экзамен			
21.	Экзамен	практическое занятие, занятие-соревнование	6

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").