

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ  
«ГИМНАЗИЯ № 4» города Смоленска**

<b>РАССМОТРЕНО</b> на заседании педагогического совета протокол от 30 мая 2023 года №6	<b>УТВЕРЖДЕНО</b> приказом директора МБОУ «Гимназия № 4» от 31.05.2023 №27-од
--	--

**Образовательная программа внеурочной деятельности  
«Информационная безопасность»**

Возраст обучающихся: 14-18 лет

Уровень: многоуровневая модульная образовательная программа

Составитель  
Горбач И.А.  
методист

## Содержание

<b>1. Основные характеристики программы.....</b>	<b>3</b>
1.1. Пояснительная записка.....	3
1.2. Цель и задачи программы.....	5
<b>2. Структура программы.....</b>	<b>6</b>
2.1. Объём программы и виды учебной работы.....	6
2.2. Содержание программы.....	9
<b>3. Комплекс организационно-педагогических условий.....</b>	<b>15</b>
3.1. Календарно-тематическое планирование.....	15
3.2. Условия реализации программы.....	20
3.3. Планируемые результаты освоения программы.....	23
3.4. Способы и формы проверки результатов освоения программы.....	23
3.5. Учебно-методическое и информационное обеспечение программы.....	24

# 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 проникновением 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 сниффером 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. Объем 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.	<b>Раздел:</b> Введение в информационную безопасность <b>Темы:</b> Информационная безопасность. Этичный хакинг. Правовые аспекты	2	2	-	-
2.	<b>Раздел:</b> Безопасность компьютерных сетей <b>Темы:</b> <ul style="list-style-type: none"><li>- Модель OSI. Стек протоколов TCP/IP.</li><li>- Физический уровень.</li><li>Канальный уровень.</li><li>- Протокол Ethernet.</li><li>- Канальный уровень.</li><li>- Протокол Wi-Fi.</li><li>- Сетевой уровень.</li><li>- Транспортный уровень.</li><li>- Прикладной уровень.</li></ul>	44	26	18	Успешное выполнение практического занятия

№ п/п	Название раздела, темы	Количество часов			Форма контроля
		Всего	Теория	Практика	
3.	<p><b>Раздел:</b> командный интерпретатор ОС Windows, скрипты</p> <p><b>Темы:</b> командный интерпретатор ОС Windows, скрипты</p>	2	1	1	Успешное выполнение практического занятия
4.	<p><b>Раздел:</b> Безопасность ОС Linux</p> <p><b>Темы:</b></p> <ul style="list-style-type: none"> <li>– Введение в ОС Linux. Установка. Файловая структура. Командный интерпретатор.</li> <li>– Пользователи и права доступа в ОС Linux.</li> <li>– Настройка сетевых интерфейсов ОС Linux.</li> <li>– Установка программ в ОС Linux.</li> <li>– Дистрибутив Kali Linux с набором утилит для этичного хакинга.</li> </ul>	12	5	5	Успешное выполнение практического занятия
5.	<p><b>Раздел:</b> Атаки на различные ОС.</p> <p><b>Темы:</b></p> <ul style="list-style-type: none"> <li>– Атаки при физическом доступе к ПК.</li> </ul>	2	1	1	Успешное выполнение практического занятия

№ п/п	Название раздела, темы	Количество часов			Форма контроля
		Всего	Теория	Практика	
	<ul style="list-style-type: none"> <li>– Атаки при удаленном доступе к ПК с использованием уязвимостей настройки ОС.</li> <li>– Атаки при удаленном доступе к ПК с использованием уязвимостей ОС и ПО.</li> </ul>				
6.	<p><b>Раздел:</b> проектная деятельность</p> <p><b>Темы:</b></p> <ul style="list-style-type: none"> <li>– Проектирование и администрирование сетей на базе протокола TCP/IP.</li> <li>– Скрипт, реализующий защиту ПК от несанкционированного доступа.</li> <li>– Установка и администрирование ОС Linux</li> </ul>	6	-	6	Успешное выполнение проектов
7.	<p><b>Раздел:</b> экзамен</p>	6	-	6	Успешное прохождение экзамена
<b>Итого</b>		<b>72</b>	<b>35</b>	<b>37</b>	



## 2.2. Содержание программы

№ п/п	Название раздела, темы	Содержание обучения
1.	<p><b>Раздел:</b> Введение в информационную безопасность</p> <p><b>Темы:</b> Информационная безопасность. Этический хакинг. Правовые аспекты</p>	<p>Основные вопросы курса. Объяснение целей и методов достижения. Объяснение ответственности с точки зрения закона РФ.</p>
2.	<p><b>Раздел:</b> Безопасность компьютерных сетей</p> <p><b>Темы:</b></p> <ul style="list-style-type: none"> <li>– Модель OSI. Стек протоколов TCP/IP.</li> <li>– Физический уровень.</li> <li>Канальный уровень.</li> <li>– Протокол Ethernet.</li> <li>– Канальный уровень.</li> <li>– Протокол Wi-Fi.</li> <li>– Сетевой уровень.</li> <li>– Транспортный уровень.</li> </ul>	<ul style="list-style-type: none"> <li>– Введение в компьютерные сети. Модель OSI. Стек протоколов TCP/IP.</li> <li>– 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.</li> <li>– Wi-fi на канальном уровне. Поверхностный анализ wi-fi с помощью программы INSSIDER. Назначение, применение и рекомендации по защите wi-fi сетей.</li> </ul>

№ п/п	Название раздела, темы	Содержание обучения
	<p>– Прикладной уровень.</p>	<p>– Исследование протокола ARP в Wireshark. Перехват пары логин/пароль, переданных через незашифрованный протокол с помощью сетевого анализатора пакетов Wireshark.</p> <p>– 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.</p> <p>– 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</p>

№ п/п	Название раздела, темы	Содержание обучения
		<p>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.</p> <p>– 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.</p>
3.	<p><b>Раздел:</b> командный интерпретатор ОС Windows, скрипты</p> <p><b>Темы:</b> командный интерпретатор ОС Windows, скрипты</p>	<p>ОС Windows – понятие, история. Файловая система NTFS. Командная строка и основные команды.</p> <p>Написание скриптов для ОС семейства windows.</p>
4.	<p><b>Раздел:</b> Безопасность ОС Linux</p> <p><b>Темы:</b></p>	<p>ОС Linux – понятие, история. Ядро. Дистрибутивы. Файловая система Linux. Консоль и основные команды. Настройка сети. Создание пользователей. Установка</p>

№ п/п	Название раздела, темы	Содержание обучения
	<ul style="list-style-type: none"> <li>– Введение в ОС Linux.</li> <li>– Установка. <ul style="list-style-type: none"> <li>Файловая структура.</li> <li>Командный интерпретатор.</li> </ul> </li> <li>– Пользователи и права доступа в ОС Linux.</li> <li>– Настройка сетевых интерфейсов ОС Linux.</li> <li>– Установка программ в ОС Linux.</li> <li>– Дистрибутив Kali Linux с набором утилит для этичного хакинга.</li> </ul>	<p>программ. Установка дистрибутива ОС Linux. Настройка сети. Создание учетных записей. Установка программ.</p>
5.	<p><b>Раздел:</b> Атаки на различные ОС.</p> <p><b>Темы:</b></p> <ul style="list-style-type: none"> <li>– Атаки при физическом доступе к ПК.</li> </ul>	<p>– 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.</p>

№ п/п	Название раздела, темы	Содержание обучения
	<ul style="list-style-type: none"> <li>– Атаки при удаленном доступе к ПК с использованием уязвимостей настройки ОС.</li> <li>– Атаки при удаленном доступе к ПК с использованием уязвимостей ОС и ПО.</li> </ul>	<ul style="list-style-type: none"> <li>– Обфускация вредоносного ПО. Использование ПО keyloggers. Изучение ПО hydra по подбору пароля на практике. Сканирование сети nmap.</li> <li>– Демонстрация атак на различные операционные системы с помощью ПО metasploit.</li> </ul>
6.	<p><b>Раздел:</b> проектная деятельность</p> <p><b>Темы:</b></p> <ul style="list-style-type: none"> <li>– Проектирование и администрирование сетей на базе протокола TCP/IP.</li> <li>– Скрипт, реализующий защиту ПК от несанкционированного доступа.</li> <li>– Установка и администрирование ОС Linux</li> </ul>	<ul style="list-style-type: none"> <li>– Решение задач по проектированию локальной вычислительной сети.</li> <li>– Написание bat-файла, реализующего функционал средства защиты от несанкционированного доступа.</li> <li>– Администрирование и настройка ОС Linux на практике.</li> </ul>

№ п/п	Название раздела, темы	Содержание обучения
7.	<b>Раздел:</b> 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
<b>Введение в информационную безопасность</b>			
1.	Информационная безопасность. Этичный хакинг. Правовые аспекты	занятие-презентация, занятие-демонстрация	2
<b>Безопасность компьютерных сетей</b>			
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
<b>Командный интерпретатор ОС Windows, скрипты</b>			



№ п/п	Тема занятия	Форма занятия	Кол-во часов
9.	Командный интерпретатор ОС Windows, скрипты	занятие- презентация, занятие- демонстрация, практическое занятие	2
<b>Безопасность ОС Linux</b>			
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
<b>Атаки на различные ОС</b>			
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	
<b>Проектная деятельность</b>			
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
<b>Экзамен</b>			
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	<p>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.</p> <p>Технические характеристики компьютера:</p> <ul style="list-style-type: none"> <li>- Процессор: Intel Core i7 4790, 3600 МГц;</li> <li>- Оперативная память: 16384 Мб.</li> <li>- Видеокарта: GeForce GTX 980 4096 Мб.</li> </ul> <p>Программное обеспечение для каждого компьютера:</p> <ul style="list-style-type: none"> <li>- ОС Windows 8.1;</li> <li>- Офисный пакет Office 2016 Prof;</li> <li>- Среда виртуализации Oracle Virtual Box;</li> <li>- ОС MS Windows 7 Prof, MS Windows Server 2012 R2, дистрибутив CentOS 7, дистрибутив KaliLinux;</li> <li>- Среда эмуляции сети Cisco Packet Tracer;</li> <li>- САЗ Kaspersky Total Security</li> </ul>
2.	Информационное обеспечение	Презентации (в MS PowerPoint);

		<p>Подготовленные стенды для практических и проектных заданий (в Oracle Virtual Box, Cisco Packet Tracer);</p> <p>Подготовленный стенд для экзамена</p>
3.	Кадровое обеспечение	<p>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.</p>

### 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 сниффером 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 навыков 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”).