
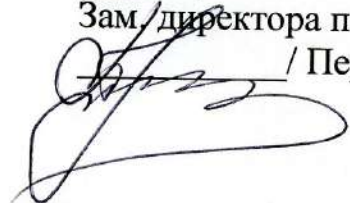


муниципальное бюджетное образовательное учреждение  
«Школа №178» городского округа Самара

Рассмотрено  
на заседании МО  
«математики, физики,  
информатики»  
Протокол № 1 от  
«26» августа 2021 г.  
Председатель МО  
 / Кабанова Е.С.

Проверено  
«28» августа 2021 г.  
Зам. директора по УВР  
 / Перова Т.П.

  
Утверждаю  
Директор школы  
Самаркина Н.П.  
Приказ № 322  
от «1» сентября 2021г.

## РАБОЧАЯ ПРОГРАММА

курса внеурочной деятельности «Интернет и защита пользователя»

**Класс:** 11

**Программу разработали:**

Кисликова Елена Григорьевна — учитель технологии

Цыганова Ксения Ивановна — учитель иностранного языка

## ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая программа «Интернет и защита пользователя» для 10/11 класса соответствует требованиям федерального государственного образовательного стандарта среднего общего образования и разработана на основе: основной образовательной программы среднего общего образования МБОУ Школы № 178 г.о. Самара;

Программа рассчитана на 34 часа (1 час в неделю). Авторская программа реализуется в полном объеме.

**Направление внеурочной деятельности** — общеинтеллектуальное

**Форма организации занятий** — кружок, поисковая деятельность.

**Цель программы:** Учебный курс по профилю «Интернет и защита пользователя» специально разработан для формирования у активных пользователей Интернета компетенций в области обеспечения информационной безопасности, правовых аспектов информационной безопасности, кибербезопасности, а также получения базовых знаний по криптографии и элементам сетевой безопасности, обеспечения информационной безопасности личного пространства.

### ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

*Предметные:*

1. Сформированы знания о безопасном поведении при работе с компьютерными программами, информацией в сети интернет;
2. Сформированы умения соблюдать нормы информационной этики;
3. Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.

*Метапредметные:*

1. Развиваются компьютерная грамотность и информационная культура личности в использовании информационных и коммуникационных технологий;
2. Развиваются умения анализировать и систематизировать имеющуюся информацию;
3. Развиваются познавательная и творческая активность в безопасном использовании информационных и коммуникационных технологий.

*Личностные:*

1. Вырабатывается сознательное и бережное отношение к вопросам собственной информационной безопасности;
2. Формируются и развиваются нравственные, этические, патриотические качества личности;
3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.

# СОДЕРЖАНИЕ ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ

## **Модуль 1. Общие сведения о безопасности ПК и Интернета (5 часов).**

Борьба с использованием Интернета в террористических, сепаратистских и экстремистских целях

Интернет как оружие массового поражения

Опасная информация в сети (сайты азартных игр, сайты о наркотиках, экстремистские, сектантские, террористические и националистические). Социальные последствия безответственного поведения в интернете

Угрозы для IOS-устройств. Угрозы для Android-устройств

## **Модуль 2. Техника безопасности и экология (2 часов).**

ПК и ЗОЖ. Организация рабочего места

## **Модуль 3. Проблемы Интернет-зависимости (2 часа).**

Классификация интернет-зависимостей

## **Модуль 4. Методы обеспечения безопасности ПК и Интернета.**

### **Вирусы и антивирусы (12 часов).**

Основные меры кибербезопасности. Безопасность приложений, серверов, конечных пользователей

Защита от атак, повышение готовности

Аппаратная защита ПО и сети (электронные ключи, аппаратные брандмауэры)

Защита ПК на этапе загрузки. Параметры безопасности ПК. Обновления

Защита файловой системы. Файловые таблицы. Права доступа

Резервное копирование и восстановление данных. Восстановление ОС. Аппаратные и программные средства

Чем отличаются методы защиты операционной системы, программного обеспечения и данных

Признаки заражения компьютерных программ. Где можно обнаружить подозрительные процессы

ОС и их возможности в борьбе с вирусами (Windows. Linux)

Разновидности вирусов. Черви, трояны, скрипты и др. Шпионские программы. Шифровальщики. Хакерские утилиты. Сетевые атаки

Защитное ПО. Антивирусные программы. Межсетевые экраны. Брандмауэры  
Антивирусная защита ПК, сети и мобильных пользователей

Наиболее известные антивирусные программы. Kaspersky Internet Security. Dr.Web Security Space. ESET NOD32 Smart Security. Бесплатные программы-сканеры

Настройка антивирусного ПО

Коммерческое и бесплатное антивирусное ПО

### **Модуль 5. Сетевой этикет. Психология и сеть (2 часов).**

Значение сетевого этикета

### **Модуль 6. Правовые аспекты защиты киберпространства (5 часа).**

Ответственность за киберпреступления.

Конституционное право на поиск, получение и распространение информации. Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию" (действует с 1 сентября 2012 года)

Информационное законодательство РФ. Закон РФ "Об информации, информационных технологиях и о защите информации"

Уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ (ст. 237 УК РФ)

Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО (FreeWare, Free, Free GPL, Adware), условно-бесплатное ПО (Trial, Shareware, Demo)

### **Модуль 7. Государственная политика в области кибербезопасности (4 часа).**

Кибервойска

Защита киберпространства как одна из задач вооруженных сил

Информационная война. Информационное оружие

Патриотизм и интернет

### **Формы организации внеурочной деятельности:**

- познавательная беседа;
- изучение терминов;
- интерактивная игра;
- проектная деятельность;
- лекции.

**Виды внеурочной деятельности:**

- ответы на вопросы;
- разгадывание ребусов;
- разгадывание кроссвордов;
- защита проекта;
- итоговое тестирование.

**ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ**

№ п/п	Наименование темы, занятия	Количество часов, отводимых на освоение темы	Теория	Практика
1	Вводное занятие	1	1	
2	Борьба с использованием Интернета в террористических, сепаратистских и экстремистских целях	1	1	
3	Интернет как оружие массового поражения	1	1	
4	Опасная информация в сети	1	1	
5	Социальные последствия безответственного поведения в интернете	1	0,5	0,5
6	Угрозы для IOS-устройств. Угрозы для Android-устройств	1	0,5	0,5
7	ПК и ЗОЖ.	1	1	
8	Организация рабочего места	1		1
9	Классификация интернет-зависимостей	1		1
10	Классификация интернет-зависимостей	1		1
11	Основные меры кибербезопасности	1		1
12	Аппаратная защита ПО и сети	1		1
13	Защита ПК на этапе загрузки. Параметры безопасности ПК.	1		1

14	Защита файловой системы	1		1
15	Резервное копирование и восстановление данных	1		1
16	Признаки заражения компьютерных программ	1	1	
17	ОС и их возможности в борьбе с вирусами	1		1
18	Разновидности вирусов	1	0,5	0,5
19	Защитное ПО. Антивирусные программы	1	1	
20	Наиболее известные антивирусные программы.	1		1
21	Настройка антивирусного ПО	1		1
22	Коммерческое и бесплатное антивирусное ПО	1	0,5	0,5
23	Значение сетевого этикета	1	1	
24	Значение сетевого этикета	1		1
25	Ответственность за киберпреступления	1		1
26	Конституционное право на поиск, получение и распространение информации.	1		1
27	Информационное законодательство РФ.	1		1
28	Уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ	1	1	
39	Правовая охрана программ для ЭВМ и БД.	1	0,5	0,5
30	Кибервойска	1	0,5	0,5
31	Защита киберпространства как одна из задач вооруженных сил	1		1

32	Информационная война. Информационное оружие	1	0,5	0,5
33	Патриотизм и интернет	1	0,5	0,5
34	Зачетное занятие. Круглый стол	1		1
	Итого	33	13	20