

**государственное бюджетное общеобразовательное учреждение Самарской области
средняя общеобразовательная школа №11 им. Героя Советского Союза
Аипова Махмута Ильячевича городского округа Октябрьск Самарской области**

Рассмотрена на
заседании методического
объединения учителей
Протокол № 1
от «21»августа 2020 г.

Проверена
Заместитель директора по УВР
_____ Л.С. Райник
«24» августа 2020 г.

Утверждена
Приказом № 278-о/д
от «24»августа 2020г.
Директор школы
_____ О.А. Дунова

**РАБОЧАЯ ПРОГРАММА КУРСА ВНЕУРОЧНОЙ ДЕЯТЕЛЬНОСТИ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
(9 КЛАСС)**

Рабочая программа курса внеурочной деятельности «Информационная безопасность» на уровне основного общего образования составлена с учетом:

- требований Федерального государственного образовательного стандарта основного общего образования (утвержден Приказом Министерства образования и науки Российской Федерации от 17 декабря 2010 г. N 1897 (с изменениями и дополнениями));
- в соответствии с основной образовательной программой основного общего образования ГБОУ СОШ № 11 г.о Октябрьск;
- на основании программы по внеурочной деятельности «Информационная безопасность, или на расстоянии одного вируса» 7-9 классы. Наместникова М. С.; Просвещение;
- на основании плана внеурочной деятельности ГБОУ СОШ № 11 г.о. Октябрьск.

В учебном плане ГБОУ СОШ №11 г.о. Октябрьск на изучение курса «Информационная безопасность» отводится по 1 часу в неделю в 9 классе, что составляет 34 часа в год. Из них 22 часа – учебных занятий, 9 часов – подготовка и защита учебных проектов, 3 часа – повторение.

1. Результаты освоения курса внеурочной деятельности

Личностные:

- осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
- готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
- освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
- сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные:

Регулятивные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- идентифицировать собственные проблемы и определять главную проблему;
- выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
- ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- составлять план решения проблемы (выполнения проекта, проведения исследования);
- описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;

- находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
- работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
- принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- выделять явление из общего ряда других явлений;
- определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;
- строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
- излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
- критически оценивать содержание и форму текста;
- определять необходимые ключевые поисковые слова и запросы.

Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- строить позитивные отношения в процессе учебной и познавательной деятельности;
- критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
- договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
- делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его.
- целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
- выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;
- использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
- использовать информацию с учетом этических и правовых норм;
- создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Предметные:

Выпускник научится:

- анализировать доменные имена компьютеров и адреса документов в интернете;
- безопасно использовать средства коммуникации,
- безопасно вести и применять способы самозащиты при попытке мошенничества,
- безопасно использовать ресурсы интернета.

Выпускник овладеет:

–приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Выпускник получит возможность овладеть:

–основами соблюдения норм информационной этики и права;

–основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;

–использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

2. Содержание курса внеурочной деятельности с указанием форм организации и видов деятельности

Раздел 1 «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах.

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете.

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Пароли для аккаунтов социальных сетей.

Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты.

Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях.

Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях.

Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг.

Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга

Тема 8. Публичные аккаунты.

Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг.

Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Выполнение и защита индивидуальных и групповых проектов.

Раздел 2 «Безопасность устройств»

Тема 1. Что такое вредоносный код.

Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода.

Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ.

Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств.

Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Выполнение и защита индивидуальных и групповых проектов.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать.

Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете.

Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете.

Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи.

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 5. Резервное копирование данных.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности.

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности. Выполнение и защита индивидуальных и групповых проектов.

Повторение. Волонтерская практика. 3 часа.

Основными видами деятельности являются: проекты, презентации, беседы.

3. Тематическое планирование

№ п/п	Раздел (Тема)	Кол-во часов	Оборудование
	Безопасность общения	13	нетбук
1	Общение в социальных сетях и мессенджерах	1	нетбук

2	С кем безопасно общаться в интернет	1	нетбук
3	Пароли для аккаунтов социальных сетей	1	нетбук
4	Безопасный вход в аккаунты	1	Нетбук
5	Настройки конфиденциальности в социальных сетях	1	
6	Публикация информации в социальных сетях	1	
7	Кибербуллинг	1	нетбук
8	Публичные аккаунты	1	нетбук
9	Фишинг	1	нетбук
10	Фишинг	1	нетбук
11	Выполнение и защита индивидуальных и групповых проектов	1	нетбук
12	Выполнение и защита индивидуальных и групповых проектов	1	нетбук
13	Выполнение и защита индивидуальных и групповых проектов	1	нетбук
	Безопасность устройств	8	нетбук
14	Что такое вредоносный код	1	нетбук
15	Распространение вредоносного кода	1	нетбук
16	Методы защиты от вредоносных программ	1	нетбук
17	Методы защиты от вредоносных программ	1	нетбук
18	Распространение вредоносного кода для мобильных устройств	1	нетбук
19	Выполнение и защита индивидуальных и групповых проектов	1	нетбук
20	Выполнение и защита индивидуальных и групповых проектов	1	нетбук
21	Выполнение и защита индивидуальных и групповых проектов	1	нетбук
	Безопасность информации	10	нетбук
22	Социальная инженерия: распознать и избежать	1	нетбук
23	Ложная информация в Интернете	1	нетбук
24	Безопасность при использовании платежных карт в Интернете	1	нетбук
25	Беспроводная технология связи	1	нетбук
26	Резервное копирование данных	1	нетбук
27	Основы государственной политики в области формирования культуры информационной безопасности	1	нетбук

28	Основы государственной политики в области формирования культуры информационной безопасности	1	нетбук
29	Выполнение и защита индивидуальных и групповых проектов	1	нетбук
30	Выполнение и защита индивидуальных и групповых проектов	1	нетбук
31	Выполнение и защита индивидуальных и групповых проектов	1	нетбук
	Повторение. Волонтерская практика.	3	нетбук
32	Волонтерская практика	1	нетбук
33	Волонтерская практика	1	нетбук
34	Волонтерская практика	1	нетбук
Итого:		34	