МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Министерство образования и науки Смоленской области

Муниципальное образование

"Починковский район" Смоленской области

МБОУ Прудковская СШ

РАССМОТРЕНО

Руководитель ШМО

_____ М.В. Петрова

Протокол № 1
от «30» августа2024 г.

УТВЕРЖДЕНО

Директор школы

_____А. А. Петроченкова

Приказ № 80
от «30» августа. 2024 г.

Рабочая программа
курса внеурочной деятельности «Кибербезопасность»

в 5 классе
на 2024 – 2025 учебный год

Прудки
2024г.

Цель программы: освоение обучающимися базовых принципов безопасного поведения в сети интернет и безопасности личного информационного пространства.

Задачи обучения:

Развивающие:

1. Развивать компьютерную грамотность информационную культуру личности в использовании информационных и коммуникационных технологий;
2. Развивать умение анализировать и систематизировать имеющуюся информацию;
3. Развивать познавательную и творческую активность в безопасном использовании информационных и коммуникационных технологий;

Обучающие:

1. Способствовать формированию знаний о безопасном поведении при работе с компьютерными программами, информацией в сети Интернет;
2. Формировать умения соблюдать нормы информационной этики;
3. Формировать умения безопасной работы с информацией, анализировать и обобщать полученную информацию.

Воспитывающие:

1. Способствовать выработке сознательного и бережного отношения к вопросам собственной информационной безопасности;
2. Способствовать формированию и развитию нравственных, этических, патриотических качеств личности.
3. Стимулировать поведение и деятельность, направленные на соблюдение информационной безопасности.

Направленность программы – техническая.

Программа разработана с учётом требований законов Российской Федерации: «Об образовании в Российской Федерации», «О защите детей от информации, причиняющей вред их здоровью и развитию» и «Санитарно-эпидемиологических требований к условиям и организациям обучения в общеобразовательных учреждениях» и «Санитарно-эпидемиологических требований к устройству, содержанию и организации режима работы общеразвивающих организаций дополнительного образования детей».

Актуальность дополнительной общеразвивающей программы «Информационная безопасность» заключена в достижении метапредметных результатов и предметных умений дисциплины «Информатика» по формированию навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в сети интернет, умений соблюдать нормы информационной этики и права.

Реализация программы позволяет создать условия для развития и информационной защиты детей.

Возраст детей, участвующих в реализации программы.

Программа рассчитана для обучающихся от 7 до 17 лет. Принимаются все желающие, достигшие возраста 7 лет.

Особенности состава обучающихся: неоднородный (смешанный); постоянный.

Уровень программы - стартовый, предполагает использование и реализацию общедоступных и универсальных форм организации материала, минимальную сложность предлагаемого для освоения содержания программы.

Организационно-педагогические условия реализации программы.

Периодичность в неделю	Продолжительность занятия	Кол-во часов в неделю	Кол-во часов в год
2 раза	40 минут	2 часа	68

Форма обучения: очная.

Форма проведения занятий: аудиторная, внеаудиторная.

Расписание занятий составлено с учетом школьного расписания в образовательных учреждениях и свободного времени обучающихся. Продолжительность по времени занятий и перемен - в соответствии с Уставом учреждения.

Форма организации занятий: групповая, индивидуально - групповая, коллективная.

Методы освоения программного материала:

В ходе реализации программы возможно использование различных **методов и приёмов** организации занятий:

- практический (опыты, упражнения);
- наглядный (иллюстрация, демонстрация, наблюдения обучающихся);
- словесный (объяснение, разъяснение, рассказ, беседа, инструктаж, лекция, дискуссия, диспут); работа с книгой (чтение, изучение, реферирование, цитирование, беглый просмотр, конспектирование);
- идеометод (просмотр, обучение, упражнение, контроль).

Планируемые результаты.

Усвоение данной программы обеспечивает достижение следующих результатов:

Год обучения	Результаты освоения программы		
	Личностные	***Метапредметные***	***Предметные***
2024-2025	1. Вырабатывается сознательное и бережное отношение к вопросам собственной и информационной безопасности; 2. Формируются и развиваются нравственные, этические, патриотические качества личности; 3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.	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.	1. Сформированы знания о безопасном поведении при работе с компьютерными программами, информации в сети интернет; 2. Сформированы умения соблюдать нормы информационной этики; 3. Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.

Система оценки результатов освоения программы - педагогическое , тесты, педагогический анализ результатов анкетирования, тестирования, зачётов, взаимозачётов, опросов, выполнение обучающимися диагностических заданий, участие в мероприятиях, защиты проектов, решение задач поискового характера, активности обучающихся на занятиях и т.п. **Материально-техническое обеспечение** реализации дополнительной общеразвивающей программы «Информационная безопасность» включают следующих перечень необходимого оборудования:

1. Кабинет «Точка роста»
2. Компьютер для педагога (ноутбук)
3. Ноутбуки для обучающихся
4. Доступ к сети Интернет

Паспорт программы

Название программы: «Кибербезопасность»

Платформа: Центр образования «Точка роста»

Направление: организация и технология защиты информации, (техническое, социальное)

Вид программы: общеразвивающая

Уровень сложности: базовый

Форма реализации: очная

Возраст обучающихся: 11-12 лет

Срок реализации программы: 1 год (40 учебных недель)

Количество часов: 68

Кол-во часов на учебный год / в неделю: 2

Ожидаемые результаты освоения программы:

сформировать у обучающихся с учетом возрастных особенностей личностные результаты, которые позволят им грамотно ориентироваться в информационном мире с учетом имеющихся в нем угроз, понимать и выполнять правила информационной безопасности и отражать личностные качества в информационной деятельности.

УЧЕБНЫЙ ПЛАН

№ п/п	Тема	Всего часов	Теория	Практика	Формы контроля
1.	**Информация, компьютер и Интернет.**	**8**	**4**	**4**	**тестирование**
1.1.	Компьютер. История создания	2	1	1	Интерактивное занятие
1.2.	Интернет как средство поиска информации	2	1	1	Рефлексивная беседа
1.3.	Полезные и вредные страницы Интернета	2	1	1	Интерактивное занятие
1.4.	Ложные ссылки. Реклама	2	1	1	Интерактивное занятие
2.	**Безопасность общения**	**8**	**4**	**4**	**Творческая работа**
2.1	Общение в социальных сетях и мессенджерах	2	1	1	Тест
2.2.	С кем безопасно общаться в интернете	2	1	1	Интерактивное занятие
2.3	Пароли для аккаунтов социальных сетей	2	1	1	Рефлексивная беседа
2.4.	Безопасный вход в аккаунты	2	1	1	Викторина
3.	**Мир виртуальный и реальный. Интернет зависимость.**	**8**	**4**	**4**	**Творческая работа**
3.1.	Настройки конфиденциальности в социальных сетях.	2	1	1	Тест
3.2.	Публикация информации в социальных сетях	2	1	1	Викторина
3.3.	Кибербуллинг	2	1	1	Тест
3.4.	Фишинг	2	1	1	Тест
4.	**Методы безопасной работы в Интернете**	**8**	**4**	**4**	**Творческая работа**
4.1	Правила хранения паролей.	2	1	1	Викторина
4.2.	Онлайн генераторы паролей	2	1	1	Тест
4.3.	Виды аутентификации	2	1	1	Викторина
4.4.	Настройки безопасности аккаунта	2	1	1	Тест
5.	**Потребительские опасности в**	**9**	**5**	**4**	**Творческая работа**

	Интернете				
5.1.	Электронная торговля - ее опасности.	2	1	1	Тест
5.2.	Виды интернет - мошенничества	3	2	1	Викторина
5.3.	Сколько стоят ошибки в интернете.	2	1	1	Рефлексивная беседа
5.4.	Плагиат	2	1	1	Интерактивное занятие
6.	**Основные правила поведения сетевого взаимодействия**	**8**	**4**	**4**	**Творческая работа**
6.1	Как вести себя в гостях у «сетевых» друзей	2	1	1	Рефлексивная беседа
6.2.	Виды этикета	2	1	1	Творческая работа
6.3.	Общие правила сетевого этикета	2	1	1	Интерактивное занятие
6.4.	Безопасная работа в сети в процессе сетевой коммуникации	2	1	1	Викторина
7.	**Государственная политика в области защиты информации**	**12**	**8**	**4**	**Тестирование**
7.1.	Как государство защищает киберпространство	3	2	1	Интерактивное занятие
7.2.	Авторское право	3	2	1	Рефлексивная беседа
7.3.	Интеллектуальная собственность	3	2	1	Интерактивное занятие
7.4.	Как расследуются преступления в сети	3	2	1	Тест
8.	Итого	61	33	28	

Календарный учебный график

Дата	Тема	Всего часов	Теория	Практика	Формы контроля
Тема 1. Информация, компьютер и Интернет.					
02.09 03.09	Компьютер. История создания	2	1	1	Интерактивное занятие
09.09 10.09	Интернет как средство писка информации	2	1	1	Рефлексивная беседа
16.09 17.09	Полезные и вредные страницы Интернета	2	1	1	Интерактивное занятие
23.09 24.09	Ложные ссылки. Реклама	2	1	1	Интерактивное
Тема 2. Безопасность общения					
30.09 01.10	Общение в социальных сетях и	2	1	1	Тест
07.10 08.10	С кем безопасно общаться в интернете	2	1	1	Интерактивное занятие
14.10 15.10	Пароли для аккаунтов социальных сетей	2	1	1	Рефлексивная беседа
21.10 22.10	Безопасный вход в аккаунты	2	1	1	Викторина
Тема 3. Мир виртуальный и реальный. Интернет зависимость.					
05.11 11.11	Настройки конфиденциальности в социальных сетях.	2	1	1	Тест
12.11 18.11	Публикация информации в социальных сетях	2	1	1	Викторина
19.11 25.11	Кибербуллинг	2	1	1	Тест
26.11 02.12	Фишинг	2	1	1	Тест
Тема 4. Методы безопасной работы в Интернете.					
03.12 09.12	Правила хранения паролей.	2	1	1	Викторина
10.12 16.12	Онлайн генераторы паролей	2	1	1	Тест
17.12 23.12	Виды аутентификации	2	1	1	Викторина
24.12 13.01	Настройки безопасности аккаунта	2	1	1	Тест
Тема 5. Потребительские опасности в Интернете.					
14.01 20.01	Электронная торговля - ее опасности.	2	1	1	Тест
21.01 27.01 28.01	Виды интернет - мошенничества	3	2	1	Викторина
03.02 04.02	Сколько стоят ошибки в интернете.	2	1	1	Рефлексивная беседа

10.02 11.02	Плагиат	2	1	1	Интерактивное занятие
Тема 6. Основные правила поведения сетевого взаимодействия.					
	Как вести себя в гостях у «сетевых» друзей	2	1	1	Рефлексивная беседа
	Виды этикета	2	1	1	Творческая работа
	Общие правила сетевого этикета	2	1	1	Интерактивное занятие
	Безопасная работа в сети в процессе сетевой коммуникации	2	1	1	Викторина
Тема 7. Государственная политика в области в области защиты информации					
	Как государство защищает киберпространство	3	2	1	Интерактивное занятие
	Авторское право	3	2	1	Рефлексивная беседа
	Интеллектуальная собственность	3	2	1	Интерактивное занятие
	Как расследуются преступления в сети	3	2	1	Тест
8.	Итого	61	33	28	

ПЛАНИРУЕМЫЕ РАЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ

В результате освоения данной программы по окончании учебного года обучающиеся:

Будут знать: об истории появления компьютера и Интернета. Правила работы с компьютером. Научиться соблюдать правила работы с файлами. Уметь отличать безопасные сайты и ссылки от вредоносных. Знать технические и программные возможности мобильных устройств. Преимущества мобильной связи и их опасность. Понимать пользу и опасности виртуального общения, социальных сетей. Основные правила работы с ПК, электронными книгами и мобильными устройствами в условиях окружающей среды, основные навыки ухода за ПК, опасности при работе с электрическими приборами. Виды общения в Интернете. Правила безопасной работы при интернет-общении. Уметь пользоваться основными видами программ для общения в сети. Чего не следует делать при сетевом общении. Основные понятия о компьютерных вирусах и контент-фильтрах. Принципы работы интернет - магазинов, понятие «электронные деньги». Дозировано использовать личную информацию в сети интернет. Правила сетевого этикета. Политику государства в области защиты информации.

Будут уметь: Правильно работать за компьютером. Пользоваться браузером для поиска полезной информации. Внимательно прочитывать сообщения о нежелательных страницах, отказываться от их просмотра. Выполнять основные действия с файлами. Копировать файлы, проверять файлы на вирусы. Уметь работать с информацией и электронной почтой. Владеть основными приемами поиска информации в сети Интернет. Соблюдать технику безопасности и гигиену при работе за ПК. Владеть основными приемами навигации в файловой системе. Уметь применять программу. Отличать вредные игры от полезных. Использовать приемы работы с антивирусными программами, запускать программы-антивируса для сканирования компьютера и внешних носителей информации, устанавливать и сканировать антивирусной программой. Детские контент-фильтры. Различать (распознавать) мошеннические действия. Корректно общаться в сети Интернет. Защищать свои информационные данные от внешнего воздействия (интернет и вирусы, вирусы и злоумышленники).

СИСТЕМА ОЦЕНКИ ДОСТИЖЕНИЯ ПЛАНИРЕУМЫХ РЕЗУЛЬТАТОВ.

Согласно Стандарту, система оценки достижения планируемых результатов освоения курса занятий по внеурочной деятельности «Информационная безопасность» состоит из двух основных компонентов:

1. Оценка предметных результатов, которая предусматривает выявление уровня достижения обучающимися планируемых результатов по данному направлению деятельности с учётом предметных знаний, действий с предметным содержанием. По окончании изучения каждой темы проводится обследование уровня усвоения знаний умений и навыков, полученных на занятии в разнообразной форме: интерактивное занятие, викторины, творческая работа и т.д.

2. Оценка метапредметных результатов как сформированности регулятивных, коммуникативных и познавательных универсальных действий может быть отслежена в результате следующих действий:

- Выполнение специально сконструированных диагностических задач, направленных на оценку уровня сформированности конкретного вида универсальных учебных действий;
- Выполнение учебных и учебно-практических задач средствами учебных предметов;
- Выполнение комплексных заданий на межпредметной основе
- Работа по оцениванию метапредметных результатов проводится в виде промежуточной и итоговой аттестации обучающихся.

Низкий уровень: удовлетворительное владение теоретической информацией по темам курса, умение пользоваться литературой при подготовке сообщений, элементарные представления об исследовательской деятельности, пассивное участие в семинарах.

Средний уровень: достаточно хорошее владение теоретической информацией по курсу, умение систематизировать и подбирать необходимую литературу, проводить исследования и опросы, иметь представление о учебно-исследовательской деятельности, участие в конкурсах, организации и проведении мероприятий.

Высокий уровень: свободное владение теоретической информацией по курсу, умение анализировать литературные источники и данные исследований и опросов, выявлять причины, подбирать методы исследования, проводить учебно-исследовательскую деятельность, активно принимать участие в мероприятиях, конкурсах, применять полученную информацию на практике.

СПИСОК ЛИТЕРАТУРЫ

Нормативно-правовые документы:

1. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 г. № 436-ФЗ;

2. Федеральный закон Российской Федерации от 21 июля 2011 г. №2252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»;

3. Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (с изм., внесенными Федеральными законами от 04.06.2014 г. № 145 -ФЗ, от 06.04.2015 г. № 68-ФЗ)

5. Постановление Главного государственного санитарного врача Российской Федерации от 29.12.2010 г. № 189 (ред. от 25.12.2013 г.) «Об утверждении СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях» (Зарегистрировано в Минюсте России 03.03.2011 г. № 19993), (в ред. Изменений № 1, утв. Постановлением Главного государственного санитарного врача Российской Федерации от 29.06.2011 г. № 85, Изменений № 2, утв. Постановлением Главного государственного санитарного врача РоссийскойФедерации от 25.12.2013 г. № 72, Изменений № 3, утв. Постановлением Главного государственного санитарного врача РФ от 24.11.2015 г. № 81)

Основная литература:

1. Бирюков А.А. Информационная безопасность защита и нападение 2- е издание: Издательство: ДМК-Пресс., 2017, 434 с.

2. Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2012, 474 с.

3. Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2012, 240с.

4. Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2014, 256 с.

5. Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасность сетей: Издательство: М.: НОУ "Интуит", 2016,571 с.

6. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студ. Учрежд. высш. проф. образования / В. В.Платонов. — М.: Издательский центр «Академия», 2013, 336 с.

7. Проскурин В.Г Защита в операционных системах: Издательство: Горячая линия-Телеком, 2014, 192 с.

8. Савченко Е. Кто, как и зачем следит за вами через интернет: Москва - Третий Рим, 2012, 100 с.

9. Яковлев В.А. Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2015, 320 с.