бюджетное общеобразовательное учреждение

Сокольского муниципального округа

«Основная общеобразовательная школа № 10»

|  |  |
| --- | --- |
| Согласованана заседании педагогическим советомПротокол № 1 от 28 августа 2024 | УтвержденаДиректор БОУ СМО «ООШ № 10»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Н.Н. ВолковаПриказ № 138 от 28 августа 2024 г. |

Дополнительная общеобразовательная

общеразвивающая программа

**«*Информационная безопасность*»**

Техническая направленность

Возраст обучающихся: 13 -16 лет

Срок реализации программы: 2 года (68 часов)

Год обучения: первый 34 часа

Уровень программы-ознакомительный

Год обучения: второй 34 часа

Уровень программы-базовый

Составитель:

Шамайкова Алёна Андреевна

педагог дополнительного образования

г. Сокол

**Пояснительная записка**

Дополнительная общеобразовательная общеразвивающая программа технической направленности **«*Информационная безопасность*»** составлена в соответствии следующих нормативных документов:

* Федеральный закон РФ «Об образовании в Российской Федерации» от 29 декабря 2012 г. No 273-ФЗ (с последующими изменениями)
* Стратегия развития воспитания в Российской Федерации до 2025 года (утверждена распоряжением Правительства РФ от 29 мая 2015 г.No 996-р.
* Указ Президента Российской Федерации от 21 июля 2020 года No 474 «О национальных целях развития Российской Федерации на период до 2030 года».
* Паспорт федерального проекта «Успех каждого ребенка» (утвержден протоколом заседания проектного комитета по национальному проекту «Образование» от 07 декабря 2018 г. No 3 (с изменениями).
* Указ Президента Российской Федерации от 29 мая 2017 года No 240 «Об объявлении В Российской Федерации Десятилетия детства».
* Распоряжение Правительства Российской Федерации от 23 января 2021 года No 122 – р «Об утверждении плана основных мероприятий, проводимых в рамках Десятилетия детства» период до 2027 года.
* «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам» (приказ Министерства просвещения РФ от 22 июля 2022 г. No 629).
* «Об утверждении Целевой модели развития региональных систем дополнительного образования детей». Приказ Министерства просвещения РФ от 3 ноября2019 г. No 467.
* «О внесении изменений в Порядок организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам», утвержденного приказом Министерства просвещения РФ от 9 ноября 2018 года No 196» (приказ Министерства просвещения РФ от 30 сентября 2020 г.No 533).
* «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно- эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи» (постановление Главного государственного санитарного врача РФ от 28 сентября 2020 г.No 28).
* «Порядок организации и осуществления образовательной деятельности по дополнительным общеобразовательным программа», утвержден приказом Министерства просвещения РФ No 629 от 27.07.2022.
* «Методические рекомендации по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы)» Письмо Министерства образования и науки РФ от 18.11.2015 г.» 09-3242

**Направленность образовательной программы**

Программа «Информационная безопасность» имеет техническую направленность.

**Актуальность программы** в том, что она помогает овладеть современными технологиями для адаптации в обществе и реализации в полной мере своего творческого потенциала.

**Педагогическая целесообразность** заключается в том, что данная программа через подобранные формы, методы и средства обучения позволит обучающимся проявить самостоятельность и даст возможность для самовыражения.

**Отличительные особенности***.* Программа дает возможность закрепить ряд результатов обучения, предусмотренных программами учебного предмета «Информатика» и «Основы безопасности жизнедеятельности»

**Новизна программы** Развитие информационного общества предполагает внедрение информационных технологий во все сферы жизни, но это означает и появление новых угроз безопасности – от утечек информации до кибертерроризма. В связи с этим большое значение приобретает проблема «культуры безопасного поведения в киберпространстве».

**Цель программы:** сформировать активную позицию школьников в получении знаний и умений выявлять информационную угрозу, определять степень ее опасности, предвидеть последствия информационной угрозы и противостоять им.

**Основные задачи:**

1. Образовательные:
	* Дать представление о современном информационном обществе, информационной безопасности личности и государства
	* Дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств
	* Познакомить со способами защиты от противоправных посягательств в сети Интернет, защиты личных данных
2. Развивающие:
	* Сформировать навыки ответственного поведения в современной информационно-телекоммуникационной среде
	* Сформировать общекультурные навыки работы с информацией (умений грамотно пользоваться источниками информации, правильно организовывать информационный процесс)
	* Сформировать навыки по профилактике и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и интернетом
	* Сформировать умение применять на практике полученные знания
	* Развить универсальные учебные действия (планирование, прогнозирование, контроль, коррекция, оценка и т. п.).
3. Воспитательные:
	* Способствовать формированию нравственных норм и ценностей в поведении и сознании
	* Развивать рефлексивную деятельность
	* Формировать готовность и способность к саморазвитию и самоопределению на основе мотивации к познанию, творчеству, труду.

**Сроки реализации программы**

Программа «Информационная безопасность» рассчитана на 2 года обучения, всего 68 часов

год обучения - 34 часа, стартовый уровень.

1. год обучения – 34 часа, базовый уровень.

**Наполняемость групп:** 12 - 15 человек

Набор детей в объединение осуществляется независимо от их способностей и умений. В возрасте от 13 до 16 лет.

**Режим занятий:** 1 раз в неделю по 40 минут

**Форма обучения** очная.

Формы очных учебных занятий:

* тематические (изучение или повторение одной учебной темы);
* комплексные или интегрированные (изучение одной учебной темы с использованием 2—3 видов деятельности);
* игровые (изучение учебного материала в процессе игры);
* итоговые или контрольные (проверка уровня подготовки детей);

В основе обучения лежат групповые занятия. Теоретические знания по всем разделам программы даются на самых первых занятиях, а затем закрепляются в практической работе.

**Планируемы результаты освоения программы**

**Предметные результаты:**

*Научатся:*

* 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;

*Получат возможность овладеть:*

* приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет- сервисов и т.п;
* основами самоконтроля, соблюдения норм информационной этики и права;
* навыками самостоятельного принятия решения и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности в сети интернет;

**Метапредметные результаты:**

*Межпредметные понятия.*

В ходе изучения учебного курса обучающиеся усовершенствуют опыт проектной деятельности и навыки работы с информацией, в том числе в текстовом, табличном виде, виде диаграмм и пр.

*Регулятивные универсальные учебные действия*

В результате освоения учебного курса обучающийся сможет:

* формулировать учебные задачи как шаги достижения поставленной цели деятельности;
* наблюдать и анализировать собственную учебную и познавательную деятельность и деятельность других обучающихся;
* соотносить реальные и планируемые результаты индивидуальной образовательной деятельности и делать выводы;
* принимать решение в учебной ситуации и нести за него ответственность.

*Познавательные универсальные учебные действия*

В результате освоения учебного курса обучающийся сможет:

* строить рассуждение на основе сравнения предметов и явлений, выделяя при этом общие признаки;
* объяснять явления, процессы, связи и отношения, выявляемые в ходе познавательной и исследовательской деятельности (приводить объяснение с изменением формы представления; объяснять, детализируя или обобщая; объяснять с заданной точки зрения);
* делать вывод на основе критического анализа разных точек зрения, подтверждать вывод собственной аргументацией или самостоятельно полученными данными;

*Коммуникативные универсальные учебные действия*

В результате освоения учебного курса, обучающийся сможет:

* определять свои действия и действия партнера, которые способствовали или препятствовали продуктивной коммуникации;
* корректно и аргументированно отстаивать свою точку зрения, в дискуссии уметь выдвигать контраргументы, перефразировать свою мысль (владение механизмом эквивалентных замен);
* критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
* организовывать учебное взаимодействие в группе (определять общие цели, распределять роли, договариваться друг с другом и т. д.);
* выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;

**Личностные**

* 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 ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

**Содержание программы**

**Учебно-тематический план первого года обучения Безопасность общения**

|  |  |  |
| --- | --- | --- |
| №п/п | Название темы | Количество часов |
| Всего | Теория | Практика |
| 1 | Общение в социальных сетях и мессенджерах | 4 | 2 | 2 |
| 2 | С кем безопасно общаться винтернете | 3 | 1 | 2 |
| 3 | Пароли для аккаунтовсоциальных сетей | 5 | 3 | 2 |
| 4 | Безопасный вход в аккаунты | 3 | 1 | 2 |
| 5 | Настройки конфиденциальностив социальных сетях | 2 | 1 | 1 |
| 6 | Публикация информации всоциальных сетях | 2 | 1 | 1 |
| 7 | Кибербуллинг | 4 | 2 | 2 |
| 8 | Публичные аккаунты | 2 | 1 | 1 |
| 9 | Фишинг | 4 | 2 | 2 |
| 10 | Выполнение и защита индивидуальных и групповыхпроектов | 5 | 2 | 3 |
|  | Итого: | 34 | 16 | 18 |

**Содержание программы первого года обучения**

**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**

Правила добавления друзей в социальных сетях. Профиль пользователя.

Анонимные социальные сети.

**Тема 3. Пароли для аккаунтов социальных сетей**

Сложные пароли. Онлайн генераторы паролей. Правилахранения 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 конфидициальность 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.

**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.

**Тема 10. Выполнение и защита индивидуальных и групповых проектов**

Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. Цели, задачи, SMART. Защита проекта.

**Учебно-тематический план 2-го года обучения Безопасность информации и устройств**

|  |  |  |
| --- | --- | --- |
| №п/п | Название темы | Количество часов |
| Всего | Теория | Практика |
| 1 | Что такое вредоносный код | 3 | 1 | 2 |
| 2 | Распространение вредоносного кода | 4 | 2 | 2 |
| 3 | Методы защиты от вредоносныхпрограмм | 3 | 1 | 2 |
| 4 | Распространение вредоносного кода длямобильных устройств | 2 | 1 | 1 |
| 5 | Выполнение и защита индивидуальныхи групповых проектов | 3 | 1 | 2 |
| 6 | Социальная инженерия: распознать иизбежать | 4 | 2 | 2 |
| 7 | Ложная информация в Интернете | 3 | 1 | 2 |
| 8 | Безопасность при использованииплатежных карт в Интернете | 3 | 1 | 2 |
| 9 | Беспроводная технология связи | 2 | 1 | 1 |
| 10 | Резервное копирование данных | 2 | 1 | 1 |
| 11 | Выполнение и защита индивидуальныхи групповых проектов | 5 | 2 | 3 |
|  | Итого | 34 | 14 | 20 |

**Содержание программы второго года обучения**

 **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.

**Тема 5. Выполнение и защита индивидуальных и групповых проектов**

Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. Цели, задачи,SMART. Защита проекта.

**Тема 6. Социальная инженерия: распознать и избежать**

Приемы социальной инженерии. Правила безопасности в виртуальных контактах.

**Тема 7. Ложная информация в Интернете**

Фейковые новости. Поддельные страницы.

**Тема 8. Безопасность при использовании платежных карт в Интернете**

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

**Тема 9. Беспроводная технология связи**

Уязвимости Wi-Fi-соединений. Публичные и непубличные сети.

Правила работы в публичных сетях.

**Тема 10. Резервное копирование данных**

Безопасность личной информации. Создание резервных копий на различных устройствах.

**Тема 11. Выполнение и защита индивидуальных и групповых проектов**

Проектная деятельность. Этапы выполнения проекта. Выбор темы проекта. Цели,

задачи, SMART. Защита проекта.

**Мониторинг образовательных результатов**

В основу критериев оценки внеурочной деятельности обучающихся положены объективность и единый подход. Контроль и оценка умений и навыков осуществляется при достижении базового уровня (выпускник овладел опорной системой знаний на уровне осознанного овладения учебными действиями). Контроль умений и навыков проводится в конце года. В качестве итоговой работы учащиеся должны предоставить индивидуальный проект.

**Требования к содержанию итоговых проектно-исследовательских работ**

**Критерии содержания текста проектно-исследовательской работы**

* + 1. Во введении сформулирована актуальность (личностная и социальная значимость) выбранной проблемы. Тема может быть переформулирована, но при этом четко определена, в необходимости исследования есть аргументы.
		2. Правильно составлен научный аппарат работы: точность формулировки проблемы, четкость и конкретность в постановке цели и задач, определении объекта и предмета исследования, выдвижении гипотезы. Гипотеза сформулирована корректно и соответствуют теме работы
		3. Есть планирование проектно-исследовательской деятельности, корректировка ее в зависимости от результатов, получаемых на разных этапах развития проекта. Дана характеристика каждого этапа реализации проекта, сформулированы задачи, которые решаются на каждом этапе, в случае коллективного проекта – распределены и выполнены задачи каждым участником, анализ ресурсного обеспечения проекта проведен корректно
		4. Используется и осмысляется междисциплинарный подход к исследованию и проектированию и на базовом уровне школьной программы, и на уровне освоения дополнительных библиографических источников
		5. Определѐн объѐм собственных данных и сопоставлено собственное проектное решение с аналоговыми по проблеме. Дан анализ источников и аналогов с точки зрения значимости для собственной проектно- исследовательской работы, выявлена его новизна, библиография и интернет ресурсы грамотно оформлены
		6. Соблюдены нормы научного стиля изложения и оформления работы. Текст работы должен демонстрировать уровень владения научным стилем изложения.
		7. Есть оценка результативности проекта, соотнесение с поставленными задачами. Проведена оценка социокультурных и образовательных последствий проекта на индивидуальном и общественном уровнях.

**Критерии презентации проектно-исследовательской работы (устного выступления)**

1. Демонстрация коммуникативных навыков при защите работы. Владение риторическими умениями, раскрытие автором содержание работы, достаточная осведомленность в терминологической системе проблемы, отсутствие стилистических и речевых ошибок, соблюдение регламента.
2. Умение чѐтко отвечать на вопросы после презентации работы.
3. Умение создать качественную презентацию. Демонстрация умения использовать IT-технологии и создавать слайд презентацию на соответствующем его возрасту уровне.
4. Умение оформлять качественный презентационный буклет на соответствующем его возрасту уровне.
5. Творческий подход к созданию продукта, оригинальность, наглядность, иллюстративность. Предоставлен качественный творческий продукт (макет, программный продукт, стенд, статья, наглядное пособие, литературное произведение, видеоролик, мультфильм и т.д.).
6. Умение установить отношения коллаборации с участниками проекта, наметить пути создания сетевого продукта. Способность намечать пути сотрудничества на уровне взаимодействия с членами кружка или секции, проявление в ходе презентации коммуникабельности, благодарности и уважения по отношению к руководителю, консультантам, умение четко обозначить пути создания сетевого продукта.
7. Ярко выраженный интерес к научному поиску, самостоятельность в выборе проблемы, пути ее исследования и проектного решения.

**Организационно-педагогические условия Методы, применяемые в обучении:**

-учебно-познавательной деятельности (наглядность,практические упражнения, словесный рассказ);

* наглядность (методические пособия, иллюстрации);
* мотивации (творческие задания, поддержание инициативы);

-творческой коммуникации(совместная творческая деятельность, коллективное освоения материала);

* частично-поисковый метод направлен на развитие познавательной активности и самостоятельности. Он заключается в выполнении небольших заданий, решение которых требует самостоятельной активности (работа со схемами, привлечение воображения и памяти).

**Обучение строится на следующих дидактических принципах:**

1. Принцип научности (т.е. нужно учить тому, что достигнуто людьми в историческом общественном развитии).
2. Принцип доступности (необходимо учитывать возможности детей и возрастные особенности при выборе темы).
3. Принцип сознательности (дети должны заинтересованно, обдуманно, а не механически усваивать знания и умения). Если будет соблюдаться принцип доступности, то даже очень маленькие дети способны обучаться сознательно.
4. Принцип систематичности и последовательности (процесс обучения должен быть построен таким образом, чтобы деятельность связывалась со всеми сторонами воспитательной работы и овладением новыми умениями, и навыками опираясь на то, что уже усвоено).

**Методическое обеспечение программы**

1. Методические рекомендации и планы занятий. 2.Учебные пособия:

* энциклопедии для детей школьного возраста,
* научно-популярные издания и публикации,
* видеоматериалы.

3. Дидактический материал Наглядные пособия:

* образцы работ по каждой новой теме. Раздаточные материалы:
* карточки,
* бланки тестов.

**Кадровое обеспечение:**

Педагог дополнительного образования БОУ СМО «ООШ № 10».

**Материально техническое обеспечение**

- Ноутбук AquariusCMPNS685UR11, страна происхождения товара – Российская Федерация;

- проектор и экран для возможности транслировать информацию для группы учащихся;

- аудио обеспечение компьютера (проводные или беспроводные колонки);

- Мышь (Box).

- рабочее место преподавателя;

- рабочие места по количеству обучающихся;

- наглядные пособия (таблицы, схемы и т.д.).

**Список информационных источников Литература для детей и родителей**

**1.** Наместникова М. С. Информационная безопасность, или на

расстоянии одного вируса. 7 – 9 класы. Учебное пособие Материалы авторской мастерской Босовой Л.Л. (metodist.lbz.ru/)

**Интернет-ресурсы для детей и родителей**

1. <http://fcior.edu.ru/> - Федеральный центр информационно- образовательных ресурсов
2. <http://www.edu.ru/>- Федеральные образовательные ресурсы
3. http:// [www.adinf.ru](http://www.adinf.ru/) – Web-сайт разработчиков антивируса ADinf.
4. http:// [www.dials.ru](http://www.dials.ru/) – сервер антивирусной лаборатории.
5. http:// [www.symantec.ru](http://www.symantec.ru/) – Российское интернет-представительство компании Symantec, производящей антивирусный пакет Norton AntiVirus.

**Дополнительные источники:**

1. Бабаш А.В. Информационная безопасность: Лабораторный практикум

/ А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019 – 432 c

1. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014 – 182 с.
2. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017 – 384 c.
3. Дети в информационном обществе <http://detionline.com/journal/about>
4. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИДАНА, 2016 – 239 c.
5. Запечников С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: ГЛТ, 2018 – 558 c.
6. Защита детей by Kaspersky // <https://kids.kaspersky.ru/>

8. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017 – 64 c.

9. Основы кибербезопасности. // https://www.xn-- d1abkefqip0a2f.xnp1ai/index.php/glava-1- osnovy-kiberbezopasnosti-tseli-i- zadachi-kurs

10. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова,Е.Ю. Зотова. – М.: Фонд Развития Интернет, 2013 – 144 с