Бюджетное общеобразовательное учреждение г. Омска

«Средняя общеобразовательная школа №132»

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ

ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

технической направленности «Кибербезопасность и защита данных в цифровой среде»

на 2024-2026 учебный год

Программа разработана для обучающихся 10-13 лет

Срок реализации: 2 года

Составитель: Пфафенрот Гузаль Джалаловна,

педагог дополнительного образования

Омск - 2024

* 1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Программа «Кибербезопасность и защита данных в цифровой среде» разработана в соответствии с требованиями нормативных документов:

* + - Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020);
    - Федеральный закон от 29.12.2012 г. № 273-ФЗ (ред. от 31.07.2020) «Об образовании в Российской Федерации»;
    - Федеральный закон РФ от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребёнка в Российской Федерации»;
    - Паспорт национального проекта «Образование» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24.12.2018 № 16);
    - Стратегия развития воспитания в РФ на период до 2025 года (распоряжение Правительства РФ от 29 мая 2015 г. № 996-р);
    - Государственная программа Российской Федерации «Развитие образования» (утв. постановлением Правительства РФ от 26.12.2017 № 1642 (ред. от 15.03.2021) «Об утверждении государственной программы Российской Федерации «Развитие образования»;
    - Паспорт федерального проекта «Успех каждого ребёнка» (утверждён на заседании проектного комитета по национальному проекту «Образование» 07 декабря 2018г., протокол

№ 3);

* + - Концепция развития дополнительного образования детей до 2030 года, утверждена распоряжением Правительства РФ от 31 марта 2022 г. № 678-р;
    - Приказ Министерства просвещения Российской Федерации от 09.11.2018 № 196

«Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;

* + - Приказ Министерства образования и науки Российской Федерации от 03.09.2019 №

467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей»;

* Приказ Министерства образования и науки Российской Федерации от 23.08.2017 г. № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;
* Приказ Министерства просвещения Российской Федерации от 13.03.2019 «114 «Об утверждении показателей, характеризующих общие критерии оценки качества условий осуществления образовательной деятельности организациями, осуществляющими образовательную деятельность по основным общеобразовательным программам, образовательным программам среднего профессионального образования, основным программам профессионального обучения, дополнительным общеобразовательным программам»;
* Приказ министерства образования и науки Российской Федерации и министерства просвещения Российской Федерации от 05.08.2020 г. № 882/391 «Об организации и осуществлении образовательной деятельности по сетевой форме реализации образовательных программ»;
* Профессиональный стандарт «Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)» (ред. от 16.06.2019 г.) (приказ Министерства труда и социальной защиты РФ от 18.10.2013 № 544н, с изм., внесёнными приказом Министерства труда и соцзащиты РФ от 25.12.2014 № 1115н и от 05.04.2016 № 422н);
* Профессиональный стандарт «Педагог дополнительного образования детей и взрослых» (приказ Министерства труда и социальной защиты РФ от 05.05.2018 № 298н «Об утверждении профессионального стандарта «Педагог дополнительного образования детей и взрослых»);
* Постановление Главного государственного санитарного врача РФ от 28.09.2020 года

№ 28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодёжи»;

* Постановление Главного государственного санитарного врача РФ от 28.01.2021 № 2

«Об утверждении санитарных правил и норм СанПиН 1.2.3685- 21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания»;

* Методические рекомендации по реализации адаптированных дополнительных общеобразовательных программ, способствующих социально-психологической реабилитации, профессиональному самоопределению детей с ограниченными возможностями здоровья, включая детей-инвалидов, с учётом их особых образовательных потребностей. (Письмо Министерства образования науки РФ № ВК-641/09 от 26.03.2016);
* Примерная программа воспитания. Утверждена на заседании Федерального учебно- методического объединения по общему образованию 02.06.2020г.;
* Методические рекомендации по созданию и функционированию центров цифрового образования «IT-куб» (утв. распоряжением Министерства просвещения Российской Федерации от 10.11.2021 № ТВ-1984/04).
* Устав БОУ «Средняя общеобразовательная школа №132» утверждённый администрацией города Омска №162 от 15.12.2014 г.

Содержание программы «Кибербезопасность и защита данных в цифровой среде» научит обучающиеся эффективно искать достоверную информацию в сети Интернет и её анализировать, безопасно и рационально использовать личные и персональные данные, распознавать угрозы в Интернет-ресурсах и противодействовать им. Кроме того, обучающиеся научатся обнаруживать признаки опасного социального контента в социальных сетях.

**Уровень общеобразовательной программы**: начальный

**Направленность программы:** техническая

# Актуальность программы

Сегодня трудно представить современного человека в мире без цифровых технологий. Мобильная связь, Интернет — эти и многие другие понятия уже прочно вплелись в

общественную и культурную жизнь. За последние четверть века цифровизация охватила все сферы человеческой деятельности и трансформировала их. Информация становится доступнее, и, как следствие, образование и самообразование, а также способы самореализации выходят на качественно иной уровень. Основная среда для использования цифровых технологий — глобальная сеть. В свою очередь, доступность современных цифровых технологий формирует повышенную активность преступников и правонарушителей в этой сфере.

Подростки 10-13 лет ведут переписки в социальных сетях, на форумах и в чатах, где приходится сталкиваться с виртуальными конфликтами. Такие конфликты, из банальных оскорблений могут переходить в нешуточные угрозы, которые имеют затяжной характер. Кроме этого, подростки подвержены стать жертвой кибербуллинга, кибергруминга, фишинга, троллинга. Атака таких видов угроз может быть очень болезненной и внезапной. Так как электронные сообщения очень сложно контролировать и фильтровать, жертва получает их неожиданно, что приводит к сильному психологическому воздействию. Киберпреступники могут воздействовать на жертву семь дней в неделю, 24 часа в сутки, не оставляя пространства и времени, в котором подросток мог бы чувствовать себя защищенным.

# Новизна программы

Заключается в том, что полученные знания и навыки, которые приобретут обучающиеся, помогут им в будущем защитить свои персональные данные, распознать опасный контент в цифровой среде и применять информационные технологии в учебной и познавательной деятельности, и в повседневной жизни.

# Отличительные особенности программы

Занятия по программе создают условия по освоению теоретических основ кибербезопасности в цифровой среде, получить представления о персональных данных и возможности безопасной работы с ними, получить практические навыки по защите от сетевых угроз и киберпреступников.

# Адресат программы

Программа ориентирована на обучающихся возрастной категории от 10 – 13 лет.

Подростки 10 - 13 лет начинают самостоятельно осваивать виртуальное пространство, посещают сайты, общаются в чатах. И хотя подростки в этом возрасте все ещё сильно зависимы от своих родителей, они уже стремятся получить некоторую свободу действий, они уже наслышаны о том, какая информация существует в Интернете. И совершенно нормально, что они хотят всё это увидеть, услышать, прочесть. Ребята начинают интересоваться миром вокруг них и отношения с друзьями становятся по-настоящему важными.

# Объем и срок освоения программы

Объём программы - 288 часа в год.

Программа рассчитана на 2 года обучения.

**Форма обучения:** очная.

# Режим занятий, периодичность и продолжительность занятий

Занятия проводятся два раза в неделю продолжительностью 2 академических часа (1 академический час равен 40 минутам). Перерыв между учебными занятиями 10-15 минут.

**Количество обучающихся в одной группе** 10-15 человек.

* 1. ЦЕЛИ И ЗАДАЧИ ПРОГРАММЫ

**Цель:** формирование у обучающихся умения применять правила кибербезопасности в цифровой среде по защите своих персональных данных.

# Задачи программы:

**Обучающие:**

* формирование навыков безопасного и рационального использования личных и персональных данных в цифровой среде;
* формирование навыков распознавания угрозы в Интернет-ресурсах и противодействия им;
* развивать умения и навыки при работе с пакетом прикладных программ для обработки информации LibreOffice **(**создание и редактирование текстового документа, создание эффективной презентации, создание простейших таблиц в табличном редакторе).

# Развивающие:

− развить познавательную и творческую активность в безопасном использовании информационных и коммуникационных технологий по защите персональных данных;

− развивать умение представлять результаты своей работы окружающим, аргументировать свою позицию;

− развить умения анализировать и систематизировать имеющуюся информацию;

# Воспитательные:

− воспитывать сознательное и бережное отношение к вопросам собственной информационной безопасности;

− развивать устойчивый интерес к правилам здоровье сберегающего и безопасного поведения.

* 1. СОДЕРЖАНИЕ ПРОГРАММЫ

Учебный план

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Название раздела** | **Количество часов** | | |
| **Всего** | **Из них** | |
| **Теория** | **Практика** |
| 1 | Введение в образовательную программу | 8 | 4 | 4 |
| 2 | Раздел 1. Изучение пакета прикладных программ для обработки информации в  LibreOffice. | 48 | 12 | 36 |
| 3 | Раздел 2. Безопасность общения в цифровой  среде. | 80 | 24 | 56 |
| 4 | Раздел 3. Кибербезопасность цифровых данных. | 72 | 24 | 48 |
| 5 | Раздел 4. Безопасность информации в сети | 32 | 12 | 20 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Интернет. |  |  |  |
| 6 | Буклет безопасности. | 40 | 8 | 32 |
| 7 | Итоговое занятие | 8 | - | 8 |
|  | **Итого** | **288** | **84** | **204** |

Содержание программы

# Введение в образовательную программу (8 часов)

Задачи:

1. Познакомить с техникой безопасности в кабинете информатики.
2. Повторить в игровой форме основные названия устройств компьютера.

Введение в образовательную программу «Кибербезопасность и защита данных в цифровой среде». Инструктаж по технике безопасности при работе с оборудованием в аудитории и на рабочем месте обучающегося. Проведение предварительной аттестации для определения уровня владения ПК в форме беседы, игры.

# Раздел 1. Изучение пакета прикладных программ для обработки информации LibreOffice (48 часов)

Задачи:

1. Познакомить с понятием «программа», «презентация», «текстовый документ»,

«электронная таблица».

1. Изучить программу текстового документа [LibreOffice Writer](https://pingvinus.ru/program/libreoffice-writer) и её возможности (редактирование строк текста; использование различных шрифтов символов; копирование и перенос части текста с одного места на другое или из одного документа в другой; контекстный поиск и замену частей текста; задание произвольных междустрочных промежутков; автоматический перенос слов на новую строку; нумерацию страниц; выравнивание краев абзаца; создание таблиц и построение диаграмм)
2. Изучить программу создания презентаций LibreOffice Impress и её возможности (использование готовых шаблонов, макетов, тем; создание слайдов, добавление текстовых, графических, звуковых и видео блоков на слайд, настраивание эффектов показа слайдов).
3. Изучить программу табличного редактора [LibreOffice Calc](https://pingvinus.ru/program/libreoffice-calc) и её возможности (создание простейших таблиц, использование различных шрифтов, и построение диаграмм).

*Теория:* Знакомство и работа с прикладными программами для обработки информации. Знакомство с текстовым редактором. Работа с клавиатурой в текстовом редакторе. Изучение программ создания презентаций и их возможностями. Правила составления презентации. Работа в программе с электронными таблицами, построение диаграмм.

*Практика:* Работа с прикладными программами для обработки информации (текстовые редакторы, создание презентаций, работа с электронными таблицами и диаграммами).

Практическая работа: «Создание редактирование документа. Параметры документа».

Практическая работа: «Создание эффективной презентации». Практическая работа: «Создание и редактирование таблиц».

# Раздел 2. Безопасность общения в цифровой среде (80 часов)

Задачи:

1. Познакомить детей с техникой безопасности в сети Интернет.
2. Научить защищать свои персональные данные.
3. Познакомить с видами угроз при личном и сетевом общении.
4. Изучить определения «Кибербуллинг», «Фишинг», «Кибергруминг», «Троллинг».
5. Изучить популярные варианты распространения фишинга.
6. Научить защититься от фишеров, кибербуллинга, кибергруминга, троллинга в социальных сетях и мессенджерах.

*Теория:* Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети. Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей. Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта. Приватность и конфиденциальность в мессенджерах. Персональные данные. Публикация личной информации. Возможные причины кибербуллинга, кибергруминга и как его избежать. Как помочь жертве кибербуллинга, кибергруминга, троллинг. Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

*Практика:*

Практическая работа: «Имечко». Игра: «Письмо другу».

Практическая работа: «Настройки конфиденциальности в социальных сетях». Игра: «Определи вид сетевой угрозы».

Практическая работа «Как не стать жертвой».

Практическая работа «Фишеры в социальных сетях и мессенджерах».

# Раздел 3. Кибербезопасность цифровых данных (72 часа )

Задачи:

1. Изучить понятия «кибербезопасность», «вредоносные программы»,

«киберпреступники».

1. Изучить виды вирусов и методы защиты от сетевых угроз.
2. Научиться защищать мобильные устройства от несанкционированного доступа.

*Теория:* Наиболее распространенные кибератаки. Вредоносные программы. Методы защиты от вредоносных программ. Киберпреступники – кто они или от кого следует защищаться в сети Интернет. Личная безопасность. Безопасность мобильных устройств. Киберслучаи (выявление нарушения кибербезопасности, устранение нарушения кибербезопасности).

*Практика:*

Практическая работа: Создание презентации: «Какие бывают вирусы»

Практическая работа: «Знакомство или как не стать жертвой киберпреступника». Практическая работа: «Выявление нарушения кибербезопасности».

Викторина: «Запрещенная информация в сети Интернет». Игра «Я в безопасности».

Игра «Мне всё по плечу».

# Раздел 4. Безопасность информации в сети Интернет (32 часов)

Задачи:

1. Научить систематизировать получаемую информацию в процессе поиска.
2. Изучить особенности и стиль ведения личных и публичных аккаунтов.
3. Научить анализировать и оценивать достоверность информации.

*Теория:*

Приемы социальной инженерии. Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов. Уязвимость Wi-Fi-соединений. Публичные и непубличные сети.

*Практика:*

Практическая работа: «Правила безопасности при виртуальных контактах». Практическая работа: «Фейковые новости. Поддельные страницы».

Практическая работа: «Правила совершения онлайн покупок». Практическая работа: «Правила работы в публичных сетях».

# Буклет безопасности (40 часов)

Задачи:

1. Изучить инструкцию по созданию буклета.
2. Научить отбирать информацию на безопасных сайтах.
3. Научить определять актуальность и достоверность информации.

*Теория:* Алгоритм создания буклета. Поиск информации для создания буклета.

*Практика:* Поиск информации, поиск безопасных сайтов, подбор достоверной и актуальной информации, подготовка работ для участия в различных конкурсах и мероприятиях.

# Итоговое занятие (8 часов)

Презентация буклета безопасности.

# ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ

Результативность и способы оценки программы построены на основе компетентностного подхода.

# Предметные результаты:

*Обучающиеся будут знать:*

* технику безопасности при работе за компьютером и в сети Интернет;
* как защитить свои персональные данные в сети Интернет;
* правила безопасного знакомства в сетевом интернет – пространстве;
* правила совершения онлайн покупок;
* риски Wi-Fi-соединений в общественных местах;
* стиль ведения личных и публичных аккаунтов;
* наиболее распространенные кибератаки;
* назначение социальных сетей и мессенджеров;
* виды угроз при личном и сетевом общения (кибербуллинг, фишинг, кибергруминг, троллинг).
* как защитить себя и как помочь жертве кибербуллинга, кибергруминга, троллинг, фишинга.
* виды угроз и антивирусные программы по их выявлению.

*Обучающиеся будут уметь:*

* соблюдать технику безопасности при работе за компьютером и в сети Интернет;
* определять виды сетевой угрозы (кибербуллинг, фишинг, кибергруминг, троллинг).
* защищать мобильные устройства от несанкционированного доступа;
* определять фейковые новости и поддельные страницы;
* распознавать небезопасный сайт в сети Интернет;
* защищать персональные данные, используя надежные пароли;
* выявлять нарушения кибербезопасности;
* работать с пакетом прикладных программ LibreOffice **(**создание и редактирование текстового документа, создание эффективной презентации, создание простейших таблиц в табличном редакторе).

# Метапредметные результаты:

* развитие способностей к оцениванию своих результатов;
* развитие умения анализировать и систематизировать имеющуюся информацию;
* развитие познавательной и творческой активности в безопасном использовании информационных и коммуникационных технологий.
* умение работать в группе, слушать высказывание товарищей, отстаивать свою точку зрения.

# Личностные результаты:

* развитие бережного отношения к вопросам собственной информационной безопасности;
* способность следовать намеченному плану;
* развитие самостоятельности.

1. КОМПЛЕКС ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИХ УСЛОВИЙ
   1. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Период обучения 72 недель, 4 часа в неделю. Всего занятий – 144

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п занятия** | **Тема занятия** | **Форма занятия** | **Количество часов** | **Форма контроля** |
| **Введение в образовательную программу (8 часа)** | | | | |
| **1** | Правила поведения в компьютерном классе.  Игра «Компьютер – не | вводное задание | 8 | Опрос, игра |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | игрушка!» |  |  |  |
| **Раздел 1. Изучение пакета прикладных программ для обработки информации**  **LibreOffice (48 часов)** | | | | |
| **1** | Знакомство с текстовым редактором.  Практическая работа  «Создание редактирование документа. Параметры документа» | Лекция, практикум | 16 | КЗ |
| **2** | Изучение программы  создания презентаций иих возможности.  Практическая работа  «Создание эффективной презентации» | Лекция, практикум | 16 | КЗ |
| **3** | Работа в программе с  электронными таблицами Практическая работа  «Создание и  редактирование таблиц» | Лекция, практикум | 16 | КЗ |
| **Раздел 2. Безопасность общения в цифровой среде (80 часов)** | | | | |
| **1** | Общение в социальных сетях и мессенджерах Практическая работа  «Имечко» | Беседа, игра | 16 | КЗ |
| **2** | Профиль пользователя. Правила добавления друзей в социальных сетях.  Игра «Письмо другу» | Беседа, игра | 16 | КЗ |
| **3** | Пароли для аккаунтов социальных сетей.  Безопасный вход в аккаунты | Беседа | 8 | КЗ |
| **5** | Персональные данные. Практическая работа  «Настройки  конфиденциальности в социальных сетях» | Беседа, практическая  работа | 8 | КЗ |
| **7** | Публикация информации в социальных сетях  Игра «Определи вид сетевой угрозы» | Лекция, игра | 8 | КЗ |
| **8** | Кибербуллинг, Кибергруминг  Практическая работа «Как не стать жертвой» | Беседа, практическая  работа | 8 | КЗ |
| **9** | Публичные аккаунты | Лекция,  практикум | 8 | КЗ |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **10** | Фишинг, троллинг  Практическая работа  «Фишеры в социальных сетях и мессенджерах» | Беседа, практическая  работа | 8 | КЗ |
| **Раздел 3. Кибербезопасность цифровых данных (72 часов)** | | | | |
| **1** | Кибербезопасность, распространенные кибератаки в сети Интернет.  Викторина «Запрещенная информация в сети Интернет» | Лекция, викторина | 8 | КЗ |
| **2** | Вредоносные программы.  Методы защиты от  вредоносных программ Игра «Я в безопасности» | Лекция, игра | 8 | КЗ |
|  | Практическая работа Создание презентации:  «Какие бывают вирусы» | Практикум | 16 | КЗ |
| **3** | Киберпреступники – кто они или от кого следует защищаться в сети Интернет.  Практическая работа  «Знакомство или как не стать жертвой  киберпреступника» | Лекция, практикум | 16 | КЗ |
| **4** | Личная безопасность. Безопасность мобильных устройств.  Игра «Мне всё по плечу» | Лекция, практикум,  игра | 8 | КЗ |
| **5** | Киберслучаи.  Практическая работа  «Выявление нарушения кибербезопасности» | Лекция, практикум | 8 | КЗ |
| **Раздел 4. Безопасность информации в сети Интернет (32 часов)** | | | | |
| **1** | Социальная инженерия: распознать и избежать. Практическая работа  «Правила безопасности при виртуальных контактах» | Лекция, практикум | 8 | КЗ |
| **2** | Ложная информация в Интернете  Практическая работа  «Фейковые новости. Поддельные страницы» | Лекция, практикум | 8 | КЗ |
| **3** | Безопасность при  использовании платежных карт в Интернете | Лекция, практикум | 8 | КЗ |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Практическая работа  «Правила совершения онлайн покупок» |  |  |  |
| **4** | Беспроводная технология связи.  Практическая работа  «Правила работы в публичных сетях» | Лекция, практикум | 8 | КЗ |
| **Буклет безопасности (40 часов)** | | | | |
| **1** | Разработка буклета  «Кибербезопасность и Кибергигиена» | Лекция, практикум | 40 | КЗ, ПР |
| **Итоговое занятие (8 часов)** | | | | |
| **1** | Итоговое занятие | Защита  проектов | 8 | П |
|  |  | **Итого:** | **288 часов** |  |

Календарный учебный график заполнен с помощью условных обозначений: КЗ – комбинированные занятия, сочетающие элементы теории и практики; П – проверочное занятие;

ПР – проектная работа (работа над кейсами).

* 1. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Материально-техническое обеспечение программы:

Компьютерное оборудование:

* + - Стационарные персональные компьютеры (системный блок, монитор, клавиатура USB, мышь USB) с доступом в интернет - 12 шт.(ноутбуки)
    - Браузер «Google Chrome», «Mozilla Firefox» или «Яндекс Браузер».
    - Пакет офисных программ «LibreOffice**»**
    - Принтер цветной.
    - Интерактивная доска, проектор.

# Кадровое обеспечение

* + - 1. Требования к кадровому обеспечению деятельности Центра «IT-куб» определяются образовательной организацией самостоятельно с учетом действующего трудового законодательства.
      2. Образовательную деятельность по дополнительным общеобразовательным программам на базе Центра «IT-куб» осуществляют педагоги дополнительного образования. В соответствии с пунктом 4 статьи 46 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» к занятию педагогической деятельностью по дополнительным общеобразовательным программам допускаются лица, обучающиеся по образовательным программам высшего образования по специальностям и направлениям подготовки, соответствующим направленности дополнительных общеобразовательных программ, и успешно прошедшие промежуточную аттестацию не менее чем за два года

обучения. Соответствие образовательной программы высшего образования направленности дополнительной общеобразовательной программы определяется образовательной организацией.

* 1. ФОРМЫ АТТЕСТАЦИИ

Формы оценки уровня достижений обучающегося

# Для контроля и самоконтроля за эффективностью обучения применяются методы:

− предварительные (наблюдение, опрос);

− текущие (наблюдение);

− итоговые (викторины, игры).

# Формы фиксации образовательных результатов

Для фиксации образовательных результатов в рамках курса используется сборник рисунков обучающихся.

# Формы предъявления и демонстрации образовательных результатов:

− демонстрация буклета безопасности. Подведение итогов конкурса Формы подведения итогов реализации программы

− педагогическое наблюдение;

−педагогический анализ выполнения обучающимися учебных заданий;

− активность обучающихся на занятиях.

* 1. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

|  |  |  |  |
| --- | --- | --- | --- |
| **Оцениваемый результат** | **Высокий уровень** | **Средний уровень** | **Недостаточный уровень** |
| Правила работы за компьютером и в сети Интернет | Хорошо знает и не нарушает правила работы за  компьютером и технику  безопасности | Знает правила  работы с  компьютером и ТБ, но иногда нарушает их | Требует  постоянного внимания со стороны педагога |
| Пакет прикладных программ LibreOffice | Умеет создавать и редактировать текстовый документ, создавать  презентацию, создавать  простейшие таблицы в  табличном редакторе. | Умеет создавать и редактировать текстовый документ, создавать  презентацию, создавать  простейшие таблицы в  табличном  редакторе, но с помощью педагога | Не умеет создавать и редактировать текстовый документ, не умеет создавать презентацию, не умеет создавать простейшие таблицы в  табличном редакторе. |
| Защита  персональных данных | Хорошо знает, как защищать  персональные  данные, используя | Знает, как защищать персональные  данные, используя надежные пароли, | Не умеет защищать персональные  данные, используя надежные пароли, не |

|  |  |  |  |
| --- | --- | --- | --- |
|  | надежные пароли, знает какую информацию о себе нельзя выставлять в сеть Интернет. | но затрудняется какую информацию о себе нельзя выставлять в сеть Интернет. | знает какую информацию о себе нельзя выставлять в сеть Интернет. |
| Сайты в сети Интернет | Ребенок умеет ориентироваться на сайтах, может определять  фейковые новости и поддельные страницы | Ребенок умеет ориентироваться на сайтах, но  затрудняется определять  фейковые новости и  поддельные страницы | Ребенок  практически не ориентируется на сайтах и не может определять  фейковые новости и  поддельные страницы |
| Презентация буклета безопасности  обучающихся,  выставка. Итоги  конкурса буклета безопасности. | Может рассказать, алгоритм буклета безопасности  защиты своих персональных  данных. Может оценивать свои  достижения и достижение  товарищей. | Может рассказать, алгоритм буклета безопасности  защиты своих персональных  данных Может оценивать свои  достижения и достижение  товарищей, но только с помощью педагога | Не может рассказать алгоритм буклета безопасности  защиты своих персональных  данных, не может оценивать свои  достижения и достижение  товарищей. |

Механизм оценки уровня освоения компетенции на определенном этапе ее формирования строится на основе критериев и использует шкалу из 5 уровне:

* + - Нулевой уровень (1 балл)
    - Низкий уровень (2 балла)
    - Средний уровень (3 балла)
    - Высокий уровень (4 балла)
    - Очень высокий уровень (5 баллов)

Точкой входа к формированию карты компетенций обучающихся служит диагностическая анкета (Приложение 1).

* 1. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

*По источнику передачи и восприятия информации:*

* словесный: рассказ, беседа, лекция;
* наглядный: опыт, иллюстрация, дидактический, наглядный материал,образцы;
* практический: показ, постановка опытов.

*По характеру деятельности:*

* объяснительно-иллюстративный (рассказ, показ, лекция, фильм,карточки и т.п.);
* репродуктивный (воспроизведение, действие по алгоритму);
* проблемный (постановка проблемных вопросов, созданиепроблемных ситуаций);
* исследовательский метод (опыты, лабораторные, эксперименты,опытническая

работа);

* проектный метод (разработка проектов, моделирование ситуаций, создание творческих работ);
* метод игры (игры дидактические, развивающие, ролевые, деловые)

3. СПИСОК ЛИТЕРАТУРЫ

# Список литературы для педагога:

1. Белоус А., Солодуха В. Кибероружие и кибербезопасность. О сложных вещах простыми словами. – М.: Инфа-Инженерия, – 2022, Цифровая книга.
2. Диогенес Ю. Озкайя Э. Кибербезопасность. Стратегии атак и обороны. – М.: ДМК- Пресс, – 2020, 326 с.
3. Бабаш А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2019. – 432 c.
4. 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.
5. 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.
6. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. – М.: ЮНИТИДАНА, 2016. – 239 c.
7. 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.
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.x](http://www.xn--d1abkefqip0a2f.xn--/)n[--](http://www.xn--d1abkefqip0a2f.xn--/) p1ai/index.php/glava-1-osnovy-kiberbezopasnosti-tseli-i-zadachi-kursa
10. Стрельцов A.A. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. – Минск, 2005. – 304 c.
11. Сусоров И.А. Перспективные технологии обеспечения кибербезопасности// Студенческий: электрон. научн. журн. 2019. № 22(66)
12. 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.
13. ​

# Список литературы для обучающихся

1. Алигулиев Р. М. Вопросы защиты детей школьного возраста от интернет- зависимости [Текст] / Р.М. Алигулиев, Р.Ш. Махмудова, Р. Ш. Махмудов. // Дистанционное и виртуальное обучение, Москва, 2011. – № 5. – С. 97–107.
2. Климонтова Г. Н. Защита информации для современных школьников [Текст] / Г.Н. Климонтова// Воспитательная работа в школе. – 2013. – № 8. – С. 74–81.
3. Никольская К. Значение персональных данных в век информационных технологий// Вестник УрФО. Безопасность в информационной сфере. 2012. № 2 (4). С. 45-47.

Приложение 1

ДИАГНОСТИЧЕСКАЯ АНКЕТА

**№ группы:** **Дата:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | ФИО  обучающегося | Полнота и достоверность информации  (по шкалеот 0 до 5 баллов) | Умение представлять информацию  (четкое, грамотное изложение материала)  (по шкале от 0до 5 баллов) | Оригинальность предоставляемого продукта  (эстетика, шрифт, рисунок)  (по шкале от 0 до 5 баллов) | Итоги конкурса  «Буклет безопасности»  (по шкале от 0 до 5 баллов) |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 |  |  |  |  |  |
| 10 |  |  |  |  |  |
| 11 |  |  |  |  |  |
| 12 |  |  |  |  |  |