

АДМИНИСТРАЦИЯ ВАГАЙСКОГО МУНИЦИПАЛЬНОГО РАЙОНА
МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО
ОБРАЗОВАНИЯ
«ВАГАЙСКИЙ ЦЕНТР СПОРТА И ТВОРЧЕСТВА»
МАУДО «ВЦСТ»

ул. Подгорная, 11 с.Вагай ,Вагайский район, Тюменская область, 626240 тел.(факс)
(34539) 23-2-72
dopobrazovanie_vagai@mail.ru

Рассмотрено на заседании
педагогического совета
протокол № 1
«01» июня 2023 г.



**Дополнительная общеобразовательная общеразвивающая программа
социально -гуманитарной направленности
«Киберпатруль»**

Форма обучения: очная, с применение дистанционных образовательных технологий

Возраст обучающихся: 11-13 лет
Срок реализации программы: 1 год
Количество учебных недель в год: 36
Всего академических часов в год: 72
Количество часов в неделю: 2

Автор-составитель:

Первухина Мария Сергеевна,
методист МАУДО «ВЦСТ»

СОДЕРЖАНИЕ

ПАСПОРТ ПРОГРАММЫ.....	3
1.КОМПЛЕКС ОСНОВНЫХ ХАРАКТЕРИСТИК ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ.....	6
1.1 Пояснительная записка.....	6
1.2 Цель и задачи программы.....	11
1.3 Планируемые результаты.....	12
2.КОМПЛЕКС ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИХ УСЛОВИЙ.....	12
2.1 Учебный план.....	12
2.2 Содержание учебного плана.....	14
2.3 Календарный учебный график.....	17
2.4 Календарно – тематическое планирование.....	17
2.5 Материально-техническое обеспечение.....	21
2.6 Условия реализации программы.....	22
2.7 Формы аттестации и оценочные материалы.....	23
2.8 Методические материалы для очной формы обучения и очной с применением ДОТ...27	27
2.9 Система воспитательной работы.....	28
3. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	34
Приложение 1.....	36
Приложение 2.....	39
Приложение 3.....	40
Приложение 4.....	41
Приложение 5.....	42
Приложение 6.....	46
Приложение 7.....	49

ПАСПОРТ ПРОГРАММЫ

Наименование образовательной программы	Дополнительная общеобразовательная общеразвивающая программа социально-гуманитарной направленности «Киберпатруль»
Тематическое направление программы	Информационная безопасность
Направленность	Социально-гуманитарная
Тип программы	Общеразвивающая
Вид программы	Краткосрочная программа реализуется в очной форме с применением дистанционных образовательных технологий
Актуальность, новизна программы, отличительные особенности	<p>Актуальность общеобразовательной общеразвивающей программы заключается в том, что исследование проблемы безопасности детей в сети Интернет последние годы является особенно остро, в связи с бурным развитием IT-технологий и со свободным использованием детьми и подростками современных информационно - коммуникационных технологий (Интернет, сотовая (мобильная) связь).</p> <p>Новизна дополнительной общеобразовательной общеразвивающей программы «Киберпатруль» состоит в том, у школьников, формируются навыки и умения безопасного и целесообразного поведения при работе в сети интернет, умения соблюдать нормы информационной этики и права. Обучающимся даётся представление о возможностях, которые предоставляют современные средства и методы обеспечения информационной безопасности, причём не ставится цель изучения технических тонкостей реализации различных инструментов. Лабораторные занятия по дисциплине «Киберпатруль» предусматривают выполнение практических заданий на персональных компьютерах с использованием пакетов прикладных программ, а также групповые занятия, где дети учатся работать в команде. Лабораторный практикум даёт опыт исследовательской работы, учит основам проектирования систем защиты информации, знакомит с методами защиты информации.</p>
Цель	Освоение обучающимися базовых принципов безопасного поведения в сети интернет и безопасности личного информационного пространства.
Задачи	<p><u>Образовательные:</u></p> <ol style="list-style-type: none"> 1.Способствовать формированию знаний о безопасном поведении при работе с информацией в сети Интернет; 2.Формировать умения соблюдать нормы информационной этики; 3.Формировать умения безопасной работы с информацией, анализировать и обобщать полученную информацию. <p><u>Развивающие:</u></p> <ol style="list-style-type: none"> 1.Развивать компьютерную грамотность и информационную культуру личности; 2.Развивать умение анализировать и систематизировать

	<p>имеющуюся информацию;</p> <p>3. Развивать познавательную и творческую активность в безопасном использовании информационных технологий.</p> <p><u>Воспитательные:</u></p> <p>1. Способствовать выработке сознательного и бережного отношения к вопросам собственной информационной безопасности;</p> <p>2. Способствовать формированию и развитию нравственных, этических, качеств личности;</p> <p>3. Стимулировать поведение и деятельность, направленные на соблюдение информационной безопасности.</p>
Планируемые результаты	<p><u>Предметные:</u></p> <p>1. Сформированы знания о безопасном поведении при работе с компьютерными программами, информацией в сети интернет;</p> <p>2. Сформированы умения соблюдать нормы информационной этики;</p> <p>3. Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.</p> <p><u>Метапредметные:</u></p> <p>1. Развиваются компьютерная грамотность и информационная культура личности в использовании информационных и коммуникационных технологий;</p> <p>2. Развиваются умения анализировать и систематизировать имеющуюся информацию;</p> <p>3. Развиваются познавательная и творческая активность в безопасном использовании информационных и коммуникационных технологий.</p> <p><u>Личностные:</u></p> <p>1. Вырабатывается сознательное и бережное отношение к вопросам собственной информационной безопасности;</p> <p>2. Формируются и развиваются нравственные, этические, патриотические качества личности;</p> <p>3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.</p>
Способы определения результативности программы / формы контроля	<p>Для отслеживания результативности образовательного процесса используются следующие виды контроля:</p> <ol style="list-style-type: none"> 1. Предварительный контроль; 2. Текущий контроль; 3. Промежуточный контроль; 4. Итоговый контроль.
Целевая аудитория программы	<p>Программа предназначена для детей с основной группой здоровья, а также для категории детей с ОВЗ и инвалидностью, детей, находящихся в социально-опасном положении, детей, состоящих в Региональной базе талантливых детей, детей состоящих на различных видах учета в КДН, ПДН и т.д.</p>
Возрастная категория	11-13 лет
Число детей, обучающихся в группе	10-20 человек
Справка о состоянии здоровья	Не требуется
Форма обучения и реализации	Очная, с применением дистанционных образовательных технологий.
Форма организации образовательного процесса	Групповые занятия с индивидуальным подходом

Период реализации программы	Программа рассчитана на 36 недель, 72 академических часа
Режим занятий	1 (один) раз в неделю по два академических часа (один час 45 минут). 72 академических часа
Полное и краткое официальное название образовательной организации	Муниципальное автономное учреждение дополнительное образование «Вагайский центр спорта и творчества» (МАУ ДО «ВЦСТ»)
Почтовый адрес, телефон с указанием кода населенного пункта, электронный адрес организации	Россия, Тюменская область, Вагайский район, с.Вагай, улица Подгорная, 11. 626240. +7 (345) 392-32-72 dopobrazovanie_vagai@mail.ru
Ф.И.О. руководителя организации, контактная информация	Тунгулин Михаил Юрьевич, +7 (345) 392-32-72
Авторы-разработчики программы (Ф.И.О полностью и должность); контактные телефоны, электронный адрес	Первухина Мария Сергеевна, методист МАУ ДО «ВЦСТ» +7-950-482-95-20 korobotova@list.ru
Сведения о квалификации педагога	Реализацию дополнительной общеобразовательной общеразвивающей программы могут осуществлять педагог, имеющий высшее педагогическое образование, обладающие достаточными теоретическими знаниями и опытом практической деятельности в области информатики и программирования.
Организаторы и партнеры программы	- Отдел полиции № 1 МО МВД России «Тобольский» (дислокация с. Вагай); - ПАО «Сбербанк»; - МФЦ Мои документы.
Место реализации	МАОУ «Вагайская средняя общеобразовательная школа» МАОУ «Черноковская средняя общеобразовательная школа»; МАОУ «Шестовская средняя общеобразовательная школа» МАОУ «Шишкинская средняя общеобразовательная школа»; МАОУ «Куларовская средняя общеобразовательная школа»; МАОУ «Зареченская средняя общеобразовательная школа»; МАОУ «Тукузская средняя общеобразовательная школа»; МАОУ «Осиноская средняя общеобразовательная школа»; МАОУ «Казанская средняя общеобразовательная школа»; МАОУ «Дубровинская средняя общеобразовательная школа» МАОУ «Ушаковская средняя общеобразовательная школа».
Особая информация и примечания	http://vagay-dop.ru/ - сайт учреждения МАУ ДО «ВЦСТ» https://vk.com/public145218097 - социальная сеть «ВКонтакте»

1.КОМПЛЕКС ОСНОВНЫХ ХАРАКТЕРИСТИК ДОПОЛНИТЕЛЬНОЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ОБЩЕРАЗВИВАЮЩЕЙ ПРОГРАММЫ «КИБЕРПАТРУЛЬ»

1.1.Пояснительная записка

Предлагаемая дополнительная общеобразовательная общеразвивающая программа «Киберпатруль» имеет социально-гуманитарную направленность и предназначена для реализации на базах школ Вагайского района для дополнительного образования детей.

Обучение проводится в очной форме с применением дистанционных образовательных технологий.

Дополнительная общеобразовательная общеразвивающая программа «Киберпатруль» разработана в соответствии с нормативно-правовыми документами:

- Федеральным Законом Российской Федерации от 29.12.2012 № 273 «Об образовании в Российской Федерации»;

- Федеральный закон от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»;

- Распоряжение Правительства Российской Федерации от 29 мая 2015 г. № 996-р «Об утверждении Стратегии развития воспитания в Российской Федерации на период до 2025 года»;

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

- Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральный закон от 27.07.2006 №152 «О персональных данных»;

- Постановление Главного государственного санитарного врача Российской Федерации от 28.09.2020 № 28 "Об утверждении санитарных правил СП 2.4. 3648-20 "Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи".

- Распоряжением Минпросвещения России от 18.05.2020 № Р-44 «Об утверждении методических рекомендаций для внедрения в основные образовательные программы современных цифровых технологий».

- Распоряжение Правительства РФ от 28 апреля 2023 г. № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации»;

- Распоряжение Правительства Российской Федерации от 31 марта 2022 г. № 678-р «Об утверждении Концепции развития дополнительного образования детей до 2030 г. и плана мероприятий по ее реализации»;

- Приказ Министерства просвещения Российской Федерации от 27.07.2022 № 629 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам"

- Приказом Минпросвещения Российской Федерации от 03.09.2019 № 467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей»;

- Приказом Минобрнауки России от 23 августа 2017 года № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность,

электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;

- Письмом Минобрнауки России от 18.11.2015 №09-3242. «Методические рекомендации по проектированию дополнительных общеразвивающих программ»;

Проблема обеспечения информационной безопасности детей в информационно-телекоммуникационных сетях становится все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей.

В современных условиях развития общества компьютер стал для ребенка и «другом» и «помощником» и даже «воспитателем», «учителем». Всеобщая информатизация и доступный, высокоскоростной Интернет уравнил жителей больших городов и малых деревень в возможности получить качественное образование и стал неотъемлемой частью нашей повседневной жизни.

Использование компьютерных технологий и Интернета в образовательных учреждениях и дома расширяет информационное образовательное пространство обучающего и позволяет повысить эффективность обучения.

Доступ учащихся к информационным ресурсам сети Интернет дает возможность школьникам пользоваться основным и дополнительным учебным материалом, необходимым для обучения в школе, выполнять домашние задания, самостоятельно обучаться. Благодаря таким ресурсам у школьников появляется возможность узнавать о проводимых олимпиадах, конкурсах, и принимать в них активное участие.

Использование компьютера и интернета в работе с детьми и в работе школы достаточно обширно:

- написание рефератов;
- создание мультимедийных презентаций;
- использование электронной почты;
- поиск в сети нужной информации;
- создание собственных школьных веб-страниц;
- рассылка и/или съем материалов (нормативных документов, информации о семинарах и конкурсах и т.п.);
- обмен опытом;
- ответы на типичные вопросы;
- получение ("скачивание") небольших обучающих программ по разным предметам;
- совместные проекты школьников (и учителей) разных школ.

Однако, использование Интернета в образовательной деятельности таит в себе много опасностей, существует ряд аспектов, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих проблемы в поведении у психически неустойчивых школьников, представляющих для детей угрозу.

В связи с этим в настоящее время необходимо особое внимание уделять воспитанию у детей *компьютерной грамотности и культуры информационной безопасности* при работе с компьютером в сети Интернет вне школы с участием родителей. Для этого следует проводить непрерывную образовательно-просветительскую работу с детьми, формировать у обучающихся ответственное и критическое отношение к источникам информации, правовую культуру в сфере защиты от негативной информации и противоправных действий средствами коммуникаций, в том числе внимательно относиться к использованию детьми личных устройств мобильной связи, домашнего

компьютера с Интернетом, телевизора, подключенного к Интернету, использовать дома программные средства защиты от доступа детей к негативной информации или информации по возрастным признакам (возраст+). Научить школьника правильно ориентироваться в большом количестве ресурсов в сети Интернет — важная задача для вовлечения детей в современную цифровую образовательную среду, отвлечения их от бесполезного контента и игр, бесцельной траты времени в социальных сетях и сервисах мобильной связи.

«Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медиаграмотности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Мы же хотим, чтобы ребята стали полноценными гражданами своей страны – теми, кто может анализировать и критически относиться к информационной продукции. Они должны знать, какие опасности подстерегают их в сети и каких избежать» (Павел Астахов, Уполномоченный при Президенте Российской Федерации по правам ребенка).

Направленность программы. Данная программа имеет социально-гуманитарную направленность, личностно-ориентированная, личностно-значимая образовательная деятельность.

Актуальность общеобразовательной общеразвивающей программы заключается в том, что исследование проблемы безопасности детей в сети Интернет последние годы является особенно остро, в связи с бурным развитием IT-технологий и со свободным использованием детьми и подростками современных информационно - коммуникационных технологий (Интернет, сотовая (мобильная) связь).

Современные дети - первое поколение, чье взросление происходит на фоне стремительно развивающихся информационно-коммуникационных технологий. В своих привычках, ценностях и поведении в сети "Интернет" эта группа принципиально отличается от представителей более старшей аудитории (18 - 45 лет). Их основными интересами являются общение в социальных сетях, просмотр видео и онлайн-игры.

Вместе с тем указанная аудитория является крайне уязвимой с точки зрения информационной безопасности. В связи с высокой степенью анонимности интернет-пространства и возможностью выстраивания общения с использованием нескольких профилей и псевдонимов риск проявления асоциальных форм поведения в цифровой среде увеличивается.

Педагогическая целесообразность. Деятельностный подход, который применяется на занятиях, позволяет максимально продуктивно усваивать материал путём смены способов организации работы. Тем самым педагог стимулирует познавательные интересы учащихся и развивает их практические навыки. У детей воспитываются ответственность за свою работу, аккуратность, взаимовыручка.

В программу включены, как индивидуальная работа, так и коллективные практические занятия, развивающие коммуникативные навыки и способность работать в команде. Практические занятия помогают развивать у обучающихся внимание,

концентрацию на своих действиях в сети интернет, умение обеспечивать информационную безопасность свою и своих близких.

Часть учебного времени отведена на проектную деятельность – совместную учебно-познавательную, творческую деятельность, имеющую общую цель, согласованные методы, способы деятельности, направленные на достижение общего результата. Тематика каждого из созданных обучающимися проектов будет направлена на сохранение информационной безопасности в направлениях изучаемых разделов. Непременным условием проектной деятельности является наличие заранее выработанных представлений о ее конечном продукте и, как следствие этого, этапах проектирования и реализации проекта, включая его осмысление и рефлексии результатов деятельности.

Новизна дополнительной общеобразовательной общеразвивающей программы «Киберпатруль» состоит в том, у школьников, формируются навыки и умения безопасного и целесообразного поведения при работе в сети интернет, умения соблюдать нормы информационной этики и права. Обучающимся дается представление о возможностях, которые предоставляют современные средства и методы обеспечения информационной безопасности, причём не ставится цель изучения технических тонкостей реализации различных инструментов. Лабораторные занятия по дисциплине «Киберпатруль» предусматривают выполнение практических заданий на персональных компьютерах с использованием пакетов прикладных программ, а также групповые занятия, где дети учатся работать в команде. Лабораторный практикум даёт опыт исследовательской работы, учит основам проектирования систем защиты информации, знакомит с методами защиты информации.

Программой предусмотрено использование современных учебных материалов, в число которых входят цифровые образовательные ресурсы: мультимедийные презентации, интерактивные обучающие уроки, видео-уроки, занимательные и развивающие игры, викторины, кроссворды по основным разделам курса внеурочной деятельности, тренировочные и проверочные материалы для организации фронтальной и индивидуальной работы, материально - техническая база мобильного класса. Практические работы в содержании программы возможно использовать в качестве вариативных, индивидуальных практических заданий разного уровня углубленности, доступности и степени сложности, исходя из диагностики и стартовых возможностей каждого из участников рассматриваемой программы.

Для анализа результатов деятельности учащихся используются современные оценочные средства. В процессе реализации дополнительной общеобразовательной общеразвивающей программы «Киберпатруль» выделено несколько форм контроля на понимание материала и умение применять знания на практике: тесты на образовательных платформах, рефлексия в ходе занятий, выполнение теоретических и практических упражнений, написание сообщений, проектов. При этом используются следующие методы обучения: объяснение, учебная демонстрация, практические работы, консультации, анкетирование, чтение и анализ научно-популярных статей. На учебном занятии обучающиеся заполняют рефлексивные листы, которые дают возможность педагогу вносить коррективы в содержание учебного материала курса, а обучающемуся отслеживать успешность прохождения курса. На итоговом занятии обучающиеся и педагог подводят результаты по освоению всего курса в целом. В качестве зачетной итоговой работы может быть выставка буклетов, выступления обучающихся по

актуальным вопросам информационной безопасности с собственными мультимедийными презентациями на ученических мероприятиях, создание видео.

Самостоятельная работа выполняется обучающимися в форме проектной деятельности, может быть индивидуальной, парной и групповой. Выполнение проектов требует от учащихся широкого поиска, структурирования и анализа дополнительной информации по теме. Для одаренных детей предусмотрены дополнительные задания в каждом разделе учебного плана, выполняя которые, дети смогут совершенствовать свои навыки и выполнять задания высокого уровня сложности. Такие задания приведены в приложении «Практикумы» (Приложение 4).

Особенности организации образовательного процесса

Адресат программы: дети 11-13 лет.

Срок освоения программы: программа рассчитана на 1 (один) год обучения.

Форма обучения и виды занятий: форма обучения – очная, очная с применением дистанционных технологий.

Программа реализуется на базе школ Вагайского района.

При **очной форме** освоения программа реализуется в группах обучающихся 11-13 лет. Состав группы – постоянный.

Минимальная наполняемость группы – 10 человека;

Максимальная наполняемость группы 20 человек.

Режим и особенности организации занятий: Занятия проводятся 1 (один) раз в неделю по 2 (два) академических часа, 8 занятий и 8 часов в месяц. Продолжительность академического часа – 45 минут. Общее количество часов по программе. Во время занятий предусмотрены **перерывы по 10-15 минут для разминки и отдыха глаз, 15 минут после занятий необходимы для приведения рабочего места в порядок.**

В случае реализации программы с использованием дистанционных технологий образовательный процесс организуется в форме видеоуроков или презентаций, которые педагог предварительно готовит в соответствии с темой. Обучающие материалы отправляются обучающимся любым удобным для них способом. При необходимости педагогом проводятся индивидуальные консультации с обучающимися с использованием приложения Viber. Контроль выполнения заданий фиксируется посредством фотоотчетов, видеоотчетов, размещаемых детьми и (или родителями) по итогам занятия в группе Viber. Общение с родителями и детьми ведётся в группе Viber. Количество занятий в неделю – согласно уровню обучения.

При очной форме обучения с применением дистанционных образовательных технологий согласно документам «Сан.Пин.2.4.3647-20» и «Приказу Минобрнауки России от 23 августа 2017г. №816» занятия проводятся в дистанционном формате. Продолжительность академического часа - 30 минут. Между занятиями предполагается 10 – минутный перерыв. Также необходимо соблюдать длительности дистанционного занятия, исходя из возрастной категории обучающихся. Необходимо соблюдать длительность непрерывной работы за компьютером для обучающихся:

1-х классов — 10 мин,

2-5-х классов — 15 мин,

6-7-х классов — 20 мин,

8-9-х классов — 25 мин,

10-11-х классов — 30 мин.

Распределение времени дистанционного занятия: ознакомление с инструкцией от 2 до 5 минут; работа педагога над темой, теоретическая часть до 20 минут; выполнение индивидуальных заданий до 10 минут; обсуждение результатов занятия до 10 минут

Занятия будут организованы индивидуально. Между занятиями родителям нужно организовать для ребенка 10 минутный перерыв, во время которого помочь ребенку выполнить несложные упражнения – физминутку, обсудить прошедшее занятие, выполняемые задания. Также предусмотрены публикации фотоотчетов и видеотчетов, прошедших проверку педагогом в группе объединения в социальной сети.

Преобладающие формы организации процесса при реализации программы «Киберпатруль»: чтение и анализ литературы по компьютерной грамотности и информационной безопасности, видео-уроки, беседы, практические и индивидуальные работы. В качестве итоговых занятий проводятся опрос или тестирование. После прохождения контрольного тестирования, школьники делятся на мини-группы и создают групповой творческий проект и презентуют его. В программе используются различные виды педагогических технологий: группового обучения, проблемного обучения и технология проектной деятельности.

При обучении по данной программе используются следующие методы:

- Мини-лекции;
- Презентации;
- Самостоятельные работы;
- Игры;
- Видеоуроки;
- Практическая работа;
- Коллективные и индивидуальные исследования;
- Творческие проекты;
- Открытые уроки.

Программа может быть реализована с применением дистанционных образовательных технологий, то есть информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Перечень электронных образовательных ресурсов: образовательная платформа, социальная сеть, мессенджеры и т.д.

1.2. Цель и задачи программы.

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

Данная цель реализуется в следующих **задачах:**

Образовательные:

- 1.Способствовать формированию знаний о безопасном поведении при работе с информацией в сети Интернет;
- 2.Формировать умения соблюдать нормы информационной этики;

3.Формировать умения безопасной работы с информацией, анализировать и обобщать полученную информацию.

Развивающие:

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

Воспитательные:

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

1.3 Планируемые результаты программы

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.

2.КОМПЛЕКС ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИХ УСЛОВИЙ

2.1. Учебный план

№ п/п	Название раздела, Темы	Количество учебных часов			Формы контроля
		Всего	Теория	Практика	
1.	Введение. Знакомство с ДООП «Кибер-патруль»	8	4	4	Опрос Текущий контроль. Прохождение тестирования. Групповая работа. Индивидуальная работа.
1.1	Вводное занятие. Техника безопасности в кабинете информатики. Техника безопасности при работе с компьютером.	2	1	1	
1.2	Воздействие электронных устройств на организм. Как правильно сидеть за компьютером.	2	1	1	
1.3	История электронно-вычислительной техники. Использование электронных устройств при неблагоприятных условиях.	2	1	1	
1.4	Устройство компьютера (внутреннее и внешнее). Уход за компьютером.	2	1	1	
2.	Интернет	20	10	10	Текущий контроль. Беседа. Индивидуальная работа. Групповая работа. Игра. Прохождение теста.
2.1	Что такое интернет: значение в жизни человека, возможности. Переход по вредоносным ссылкам.	2	1	1	
2.2	Что такое пароль и их значение.	2	1	1	
2.3	Электронная почта. Создание почтового электронного ящика. Получение и отправка писем.	2	1	1	
2.4	Защита персональных данных и зачем она нужна.	2	1	1	
2.5	Социальные сервисы и сети, регистрация и работа в сетях	2	1	1	
2.6	Облачные хранилища	2	1	1	
2.7	Компьютерная грамотность в сети интернет	2	1	1	
2.8	Польза и опасности мобильной связи	2	1	1	
2.9	Интернет – зависимость. Интернет, как наркотик.	2	1	1	
2.10	Игровая зависимость	2	1	1	
3.	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы.	10	4	4	Опрос. Контрольные вопросы. Прохождение тестирования. Индивидуальная работа.
3.1	Вредоносный код	2	1	1	
3.2	Что такое вирусы. Виды вирусов.	2	1	1	
3.3	Антивирусная защита. Источники и причины заражения.	2	1	1	
3.4	Установка и функционирование антивирусных программ	2	1	1	
3.5	Защита детей в социальных сетях. Двухфакторная аутентификация в социальной сети.	2	1	1	
4.	Мошеннические действия в Интернете. Киберпреступления.	12	6	6	Беседа. Круглый стол. Групповая работа. Опрос.
4.1	Киберпреступления – что это? Виды интернет-мошенничества (письма, реклама, охота за личными данными и т.д.). Защита личных данных в сети интернет.	2	1	1	
4.2	Виртуальные друзья – кто они?	2	1	1	
4.3	Мобильные мошенники. Странные звонки по мобильному телефону.	2	1	1	
4.4	Безопасные онлайн платежи.	2	1	1	
4.5	Безопасность при использовании платежных карт в Интернете	2	1	1	
4.6.	Правовые основы обеспечения информационной безопасности	2	1	1	
5.	Сетевой этикет. Психология и сеть.	12	5,5	6,5	Беседа. Групповая работа. Индивидуальная работа. Опрос.
5.1	Что такое «нетикет» и почему он появился? Правила общения в интернете. Основы сетевого этикета.	2	1	1	

5.2	Переписка в сети. Этикет при переписке.	2	1	1	Викторина. Творческая работа.
5.3	Что такое форум? Зачем существуют модерация.	2	1	1	
5.4	Общение в сети и его последствия. Агрессия в сети.	2	1	1	
5.5	Психологическое влияние через Интернет. Грифинг, кибер-буллинг, кибермоббинг, троллинг, буллицид.	2	0,5	1,5	
5.6	Безопасное и ответственное поведение в социальных сетях.	2	1	1	
6.	Итоговое занятие	10		10	
6.1.	Контрольная работа	2		2	Контрольный тест
6.2	Создание творческого проекта «Мои правила безопасной работы в сети Интернет».	4		4	Наблюдение. ПВР
6.3	Презентация творческого проекта «Мои правила безопасной работы в сети Интернет».	4		4	Видео мастер-класс, видеопрезентация. Проведение открытого занятия для родителей.
	ИТОГО	72	30,5	41,5	

2.2. Содержание учебного плана

1. Введение. Знакомство с ДООП «Киберпатруль». (8 ч.)

Теория: Правила поведения в компьютерном классе, а также инструктаж на случай внезапных пожаров. Техника безопасности при работе с компьютером. Знакомство с дополнительной общеобразовательной общеразвивающей программой «Киберпатруль», с его целями и задачами, порядком и планом работы на учебный год. Рассмотреть какие заболевания могут вызвать компьютеры, планшеты, мобильные телефоны. Как воздействуют различные мониторы на зрение. Сколько времени, можно проводить за электронными устройствами. Комплекс упражнений при работе за компьютером. Обучающиеся должны знать об истории появления компьютера и Интернета. Использование электронных устройств, когда на улице гроза, дождь, снег. Устройство основные и дополнительные. Устройство ввода информации. Устройства вывода информации. Организация и основные характеристики памяти компьютера.

Практика: Прохождение тестирования на образовательной платформе РЭШ по теме «Техника безопасности при работе с компьютером. Ссылка на прохождение: <https://resh.edu.ru/subject/lesson/3066/train/#188582>. Составление памятки «Профилактика здоровья при работе с компьютером». Работа в группах. Составление памятки при использовании электронных устройств при неблагоприятных условиях. Работа в группах. Составление интерактивного кроссворда на образовательной платформе OnlineTestPad и отгадывание у одноклассников.

Форма контроля: Наблюдение, опрос. Текущий контроль

2. Интернет (18ч.)

Теория: Дать понятие: «Что такое интернет?». Значение в жизни человека, возможности. История создания сети интернет. Браузеры. Правила безопасной работы в сети интернет. Поиск информации в интернете. Переход по вредоносным ссылкам. Что

такое пароль и для чего они нужны? Не надежные и надежные пароли. Где хранят пароли? Алгоритм создания надежного пароля. История электронной почты. Создание почтового электронного ящика. Получение и отправка писем. Нежелательные письма (спам). Что такое персональные данные. Что относится к персональным данным. Классификация специальные и биометрические персональные данные. Последствия несоблюдения правил защиты персональных данных. Как защитить свои персональные данные? Понятие социальных сервисов и сетей. История создания социальных сетей. Наиболее распространенные социальные сети и сервисы. Достоинства и недостатки социальных сетей. Почему не рекомендуется открыто публиковать в социальной сети личную информацию? Чем это может грозить? Опасности социальных сетей и сервисов. Понятие облачного хранилища. Виды облачных услуг. Безопасны ли облачные сервисы. Возможности облачного сервиса. Какие данные можно хранить в облаке. Плюсы и минусы облачных хранилищ. Что такое компьютерная грамотность Интернет, телефон и космос. История создания радиотелефона. Действия мобильного телефона. Чем опасны мобильные телефоны. Как они влияют на здоровье. Польза мобильного телефона. Понятие «Интернет-зависимости». Симптомы «интернет-зависимости». Факторы, способствующие распространению интернет-зависимости. Последствия интернет-зависимости. Профилактика. Виды психических нарушений как следствие интернет-зависимости. Развлечения в Интернете. Виды развлечений. Понятие игровой зависимости. Полезные и вредные игры. Признаки игровой зависимости.

Практика: Индивидуальная работа по карточкам «Поиск информации в сети». Групповая работа с карточками, сравнительная таблица надежных и ненадежных паролей. Индивидуальная работа. Регистрация своего почтового ящика. Отправка писем другу (между одноклассниками). Работа по карточкам. Разбор ситуации по вопросам защиты персональных данных и пути ее решения. Написать мини доклад (сочинение) про любимый мессенджер, которым пользуетесь постоянно на тему: «Почему мне нравится «жить» в социальной сети?». Создание облачного хранилища и работа в нём. Оформление информационного стенда по ИБ. Работа в группах. Составление памятки, как пользоваться правильно мобильным телефоном, чтобы уменьшить его вред. Подготовка командной ролевой игры «Лечение болезни 21 века». Прохождение тестирования и анкетирования на интернет-зависимость учащихся. Материалы анкетирования. <https://infourok.ru/prakticheskaya-rabota-po-ikt-issledovanie-internetzavisimosti-2731215.html>.

Подготовить сообщение «Популярные развлечения в сети Интернет».

Форма контроля: Наблюдение, опрос. Текущий контроль. Представление выполненной работы, посредством видеопрезентации. Выполнение задания для самостоятельного решения.

Дополнительное задание: обучающиеся, которые выполнили задание быстрее, выполняют (по желанию) дополнительные задания, указанные в рабочем листе ученика, в разделе «Практикум».

3. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы (8ч.)

Теория. Что такое вредоносный код. Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов. Способы доставки вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Понятие компьютерных вирусов. История

возникновения вирусов. Виды компьютерных вирусов. Цели компьютерных вирусов. Как распространяются вирусы. Что такое антивирусная защита. Классификация компьютерных вирусов. Признаки заражения компьютера. Источники и причины заражения. Как лечить компьютер. Популярные антивирусные программы. Плюсы и минусы популярных антивирусов. Установка и функционирование антивирусных программ. Защита детей в социальных сетях. Какие угрозы встречаются наиболее часто во всемирной паутине. Угрозы, подстерегающие детей в интернете. ПО для родителей. Ограничение времени нахождения в сети. Рекомендации посещения интернета. Понятие двухфакторной аутентификации.

Практика. Способы выявления вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах. Подготовка сообщения: «Удивительные факты о компьютерных вирусах». Прохождение тестирования на платформе OnlineTestPad. Ссылка для прохождения: <https://onlinetestpad.com/ru/test/50642-kompyuternye-virusy-i-antivirusnye-programmy>. Составление инструктажа по установке антивирусных программ. Написание эссе на тему: «Зачем нужен родительский контроль сети интернет?» .

4.Мошеннические действия в Интернете. Киберпреступления.

Теория. Дать понятие киберпреступления. Виды интернет-мошенничества (письма, реклама, охота за личными данными, легкий заработок в интернете, пирамиды, подозрительные звонки на мобильный телефон и т.д.), опасности мобильной связи. Защита личных данных. Расширить знания о «виртуальном мире» и «реальном мире». Негативные стороны виртуальной жизни. Опасности общения в Сети. Что делать, если вам предлагают перейти по сомнительным ссылкам и пишут незнакомые люди. Основные безопасные правила поведения в Сети. Что такое мобильное мошенничество. Сообщения о заражении мобильного телефона вредоносной программой. Виды телефонного мошенничества. Телефонный вишинг. SMS-фишинг. Как не попасть на мобильное мошенничество. Как не столкнуться с мобильным мошенничеством. Куда жаловаться на телефонных мошенников. Как использовать электронный кошелек или банковскую карту, чтобы не стать жертвой обмана. Основные типы мошенничества и способы их защиты. Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов. Законодательство в информационной сфере. Виды защищаемой информации. Государственная тайна как особый вид защищаемой информации; система защиты государственной тайны; правовой режим защиты государственной тайны.

Практика. Круглый стол «Как не стать жертвой сетевых (мобильных) шуток и розыгрышей». Групповая работа создание информационного буклета, нарисовать плакат «Мобильные мошенники». Создание онлайн кошелька и его настройки. Квест «Покупка в интернет-магазине». (Приложение б). Подготовить доклад на тему: «Конфиденциальная информация».

Форма контроля: Наблюдение, опрос. Текущий контроль. Представление выполненной работы, посредством видеопрезентации. Выполнение задания для самостоятельного решения.

Дополнительное задание: обучающиеся, которые выполнили задание быстрее, выполняют (по желанию) дополнительные задания, указанные в рабочем листе ученика, в

разделе «Практикум».

5.Сетевой этикет. Психология и сеть. (12ч.)

Теория. Понятие нетикет и почему он появился. Категории нетикета. Правила общения в интернете. Основы сетевого этикета. Особенности общения в интернете. Стиль общения. Оформление электронного письма. Размер электронного письма. Электронная подпись. Смайлики. Что такое форум? Для чего они нужны. Функции форумов. Структура форумов. Основные термины для пользования форумами. Понятие модерации, ее цель и задачи. Термины «Агрессия и агрессивность». Особенности агрессивного поведения в Интернете. Как реагировать на агрессию в сети. Понятия грифинг, кибер-буллинг, кибермоббинг, троллинг, буллицид. Откуда появились эти понятия. Виды и формы кибербуллинга. Профилактика интернет-насилия. Правила в интернете и ответственность за собственное поведение. Понятие клевета, фейк, оскорбление. Какую ответственность понесут за клевету, фейк и оскорбление в интернет-ресурсах. Защита личных данных в Интернете. Настройки конфиденциальности в социальных сетях.

Практика. Разработка памятки на тему «Правила общения в сети Интернет». Написать электронное письмо деловому партнеру в текстовом редакторе. Прохождение викторины «Что я знаю о форумах? Нарисовать рисунок «Моя киберагрессия». Изучение научной статьи. Создание буклета или нарисовать рисунки «Остановите кибербуллинг: что делать, если вас травят в интернете». Размещение рисунков на сайте учреждения и в социальных сетях. Интерактивная викторина «Что я знаю о безопасном и ответственном поведении в социальных сетях».

Форма контроля: Наблюдение, опрос. Текущий контроль. Представление выполненной работы, посредством видеопрезентации. Выполнение задания для самостоятельного решения.

Дополнительное задание: обучающиеся, которые выполнили задание быстрее, выполняют (по желанию) дополнительные задания, указанные в рабочем листе ученика, в разделе «Практикум».

6.Итоговое занятие (10ч.)

Теория. Тестовая проверочная работа.

Практика. Создание творческого проекта «Мои правила безопасной работы в сети Интернет». Презентация готового творческого проекта.

2.3. Календарный учебный график

дополнительной общеобразовательной общеразвивающей программы
«Киберпатруль»

Наименование группы / год обучения*	Срок учебного года (продолжительность обучения)	Кол-во занятий в неделю, продолж. одного занятия (мин)	Наименование дисциплины (модуля)	Всего ак. ч. в год	Кол-во ак. ч. в неделю
1 год	с 1 сентября по 31 мая (36 уч. недель)	2 занятия по 45 мин (1 ак.ч.)	«Киберпатруль»	72	2

2.4.Календарно- тематическое планирование

Дата	Тема занятия	Форма проведения занятия		Количество учебных часов		Форма контроля	
		очное	с применением ДОТ	теория	практика	очное	ДОТ
1.Введение. Знакомство с ДООП «Кибер-патруль»				4	4	Наблюдение, опрос. ТК.	Опрос
	Вводное занятие. Техника безопасности в кабинете информатики. Техника безопасности при работе с компьютером.	КЗо	КЗдо	1	1		
	Воздействие электронных устройств на организм. Как правильно сидеть за компьютером	КЗо	КЗдо	1	1	ПР, опрос	Опрос, ПВР
	История электронно-вычислительной техники. Использование электронных устройств при неблагоприятных условиях	КЗо	Видеоурок/ презентация. Индивидуальные исследования. ПР	1	1	ПР	Опрос .ПВР
	Устройство компьютера (внутреннее и внешнее). Уход за компьютером.	КЗо		1	1	ПР	Опрос, ПВР
2. Интернет				10	10		
	Что такое интернет: значение в жизни человека, возможности	КЗо	Видеоурок/ презентация. Индивидуальные исследования. ПР	1	1	ПР	Опрос, ПВР
	Пароль	КЗо		1	1	ПР	Опрос, ПВР
	Электронная почта	КЗо		1	1	ПР	Опрос, ПВР
	Защита персональных данных и зачем она нужна	КЗо		1	1	ПР	Опрос, ПВР
	Социальные сервисы и сети, регистрация и работа в сетях	КЗо		1	1	ПР	Опрос, ПВР
	Облачные хранилища	КЗо		1	1	ПР	Опрос, ПВР
	Компьютерная грамотность в сети Интернет	КЗо		1	1	ПР	Опрос, ПВР

	Польза и опасности мобильной связи	КЗо		1	1	ПР	Опрос, ПВР
	Интернет-зависимость. Интернет, как наркотик	КЗо		1	1	ПР	Опрос, ПВР
	Игровая зависимость	КЗо		1	1	ПР	Опрос, ПВР
3. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы				4	4		
	Понятие компьютерных вирусов. История возникновения вирусов. Виды компьютерных вирусов. Цели компьютерных вирусов. Как распространяются вирусы	КЗо	Видеоурок/ презентация. ПР.	1	1	Наблюдение, опрос. СР.	Опрос, ПВР. СР.
	Что такое антивирусная защита. Как лечить компьютер	КЗо		1	1	Наблюдение, опрос, ТК.	Опрос. СР. ПВР.
	Установка и функционирование антивирусных программ.	КЗо		1	1	Наблюдение, опрос, ТК.	Опрос. СР
	Защита детей в социальных сетях (занятие можно провести совместно с родителями). Двухфакторная аутентификация в социальной сети.	КЗо		1	1	Наблюдение, ТК.	Опрос. СР
4. Мошеннические действия в Интернете. Киберпреступления				6	6		
	Киберпреступления – что это? Виды интернет-мошенничества (письма, реклама, охота за личными данными и т.д.). Защита личных данных в сети интернет.	КЗо	Видеоурок/ презентация. Индивидуальные исследования. ПР	1	1	Наблюдение. Опрос.	Опрос. СР.
	Виртуальные друзья – кто они? Незнакомцы в интернете.	КЗо		1	1	Наблюдение. Опрос. СР.ТК.	Опрос. СР
	Мобильные мошенники. Странные звонки по мобильному телефону	КЗо		1	1	Наблюдение. Опрос. СР.ТК.	Опрос. СР.
	Безопасные онлайн платежи.	КЗо		1	1	Наблюдение. Опрос. СР.ТК.	Опрос. СР.
	Безопасность при использовании платежных карт в Интернете	КЗо		1	1	Наблюдение. Опрос. СР.ТК.	Опрос. СР.

						р-класс. Открытый урок	класс.
Итого		72		29,5	40,5		

Примечание:

Комбинированное занятие для очной формы обучения (КЗо)– мини-лекции, просмотр видеоматериалов/презентаций по теме, выполнение практического задания, изучение рабочего листа ученика, коллективное исследование по теме.

Комбинированное занятие для очной формы обучения с применением дистанционных технологий (КЗдо) – просмотр видеоматериалов/презентаций по теме с конспектированием, выполнение практического задания.

Самостоятельная работа (СР), практическая работа (ПР), текущий контроль (ТК), представление выполненной работы (ПВР).

2.5. Материально-техническое обеспечение

Программа реализуется на базе школ Вагайского района:

- МАОУ «Вагайская средняя общеобразовательная школа»
- МАОУ «Черноковская средняя общеобразовательная школа»;
- МАОУ «Шестовская средняя общеобразовательная школа»
- МАОУ «Шишкинская средняя общеобразовательная школа»;
- МАОУ «Куларовская средняя общеобразовательная школа»;
- МАОУ «Зареченская средняя общеобразовательная школа»;
- МАОУ «Тукузская средняя общеобразовательная школа»;
- МАОУ «Осиноская средняя общеобразовательная школа»;
- МАОУ «Казанская средняя общеобразовательная школа»;
- МАОУ «Дубровинская средняя общеобразовательная школа»
- МАОУ «Ушаковская средняя общеобразовательная школа».

Технические средства обучения (аудио-видео),

1. Компьютерная техника (Монитор, системный блок, мышь компьютерная, клавиатура, колонки);
2. Периферийное оборудование (видеопроектор, экран);
3. Канцелярские принадлежности;

Каждый обучающийся обеспечивается доступом к методическим пособиям, видеоурокам и др. необходимым материалам. Во время самостоятельной работы обучающиеся могут пользоваться Интернетом с целью изучения дополнительного материала по учебным заданиям. Рабочее место обучающегося при освоении программы с использованием дистанционных технологий должно быть организовано дома и соответствовать необходимым нормативам и требованиям, быть оборудовано компьютером, имеющим доступ к сети Интернет, колонками, рабочей поверхностью,

необходимыми инструментами. Рекомендации по организации домашнего обучения приведены в приложении к Программе.

Информационное и методическое обеспечение: при очной форме обучения с использованием ДОТ предусмотрены следующие формы организации занятий:

- видеуроки, мастер-классы, вебинары и т.д.
 - формы организации самостоятельной работы обучающихся: тесты, домашние задания, самостоятельные работы, практические задания
 - получение обратной связи в виде письменных ответов, фотографий, видеозаписей, презентаций
 - онлайн-консультации, текстовые и аудио рецензии
 - создание педагогом новых и использование имеющихся на образовательных порталах и платформах ресурсов и заданий (текстовых, фото, видео, мультимедийных и др.).
 - дидактические материалы: карточки, плакаты и др.; видео- и аудио - материалы.
- Приложение Viber для общения с учениками и получения выполненных заданий. Так же используется электронная почта.

2.6. Условия реализации программы

Для реализации данной программы необходимо иметь:

1. Помещение (компьютерный класс) соответствующее санитарно – гигиеническим нормам и технике безопасности. Помещение должно хорошо освещаться, возможность периодического проветривания, укомплектовано аптечкой для оказания первой помощи.
2. Столы для учащихся 6-10шт;
3. Стулья 12-20шт;
4. Персональные компьютеры для обучающихся;
5. Акустическая система;
6. Локальная сеть с доступом в Интернет;
7. Проектор и демонстрационный экран, интерактивная доска;
8. Шкафы для хранения наглядных пособий;
9. Дидактический материал: иллюстрации, фотографии, книги, видеопрезентации по темам;
10. Оборудование для педагога: компьютер, проектор, экран, муз.колонки, МФУ

Кадровое обеспечение:

Реализацию дополнительной образовательной общеразвивающей программы могут осуществлять педагог, имеющий высшее педагогическое образование, обладающие достаточными теоретическими знаниями и опытом практической деятельности в области информатики и программирования.

Так же в реализации программы могут участвовать:

- Отдел полиции № 1 МО МВД России «Тобольский» (дислокация с. Вагай);
- ПАО «Сбербанк»;
- МФЦ Мои документы.

Методическое обеспечение: Дополнительная общеразвивающая программа «Киберпатруль» имеет развернутое календарно-тематическое планирование, содержащее детальное разделение учебного времени на теоретическую и практическую части.

Информационное обеспечение: использование собственного презентативного материала, видеоролики.

Учебно-методический комплекс: тематические подборки наглядных материалов (схемы, шаблоны, и др.); подборка литературно-художественного материала (рассказы); занимательный материал (викторины, игры); подборка заданий развивающего и творческого характера по темам; разработки теоретических и практических занятий.

Беседы: «История появления компьютера», «Интернет в жизни человека», «Профессии человек-техника» и др. Презентации по темам. Для реализации задач здоровьесбережения имеется подборка профилактических, развивающих упражнений (для глаз, для рук, для снятия напряжения и профилактики утомления и т.п.), эти упражнения применяются в середине занятия.

2.7. Формы аттестации (контроля) и оценочные материалы

Формы контроля и подведения итогов реализации программы:

Для отслеживания результативности образовательного процесса используются следующие виды контроля:

5. Предварительный контроль;
6. Текущий контроль;
7. Промежуточный контроль;
8. Итоговый контроль.

Предварительный контроль проводится в сентябре с целью выявления первоначального уровня знаний и умений и проводится в форме педагогического наблюдения, а также теста, определяющего интерес детей к изучаемой тематике.

Текущий контроль осуществляется на занятиях в течение всего учебного года для отслеживания уровня освоения учебного материала программы и развития личностных качеств обучающихся. Он проводится в различных формах: педагогическое наблюдение, устного опроса, беседы, анализ на каждом занятии педагогом и учащимися качества выполнения творческих работ и приобретенных навыков общения, по результатам конкурсов, соревнований.

Промежуточный контроль предусмотрен по окончании каждого полугодия с целью выявления уровня освоения программы обучающимися и корректировки процесса обучения. В качестве промежуточного контроля применяются такие его формы как анализ участия каждого обучающегося в конкурсах, выставках и творческой деятельности, проведение тестирований по теме или проблемной беседы.

Итоговый контроль призван показать оценку уровня и качества освоения учащимися дополнительной общеразвивающей программы по завершению каждого года обучения. Проводятся тестирования по темам, защита творческих проектов.

Формы подведения итогов реализации общеобразовательной программы:

- итоговые занятия;
- открытые занятия для родителей;
- мастер-класс.

Учащимся, успешно освоившим дополнительную общеобразовательную общеразвивающую программу и прошедшим итоговую аттестацию, выдаются сертификаты, которые самостоятельно разрабатывает и утверждает образовательная организация, почетные грамоты, призы.

При **очной форме освоения** программы контрольные упражнения выполняются на занятии и непосредственно на занятии оцениваются педагогом.

При освоении программы **с использованием дистанционных технологий** обучающиеся выполняют контрольные упражнения самостоятельно и направляют педагогу видео и (или) фотоотчет через приложение Viber. Правильность выполнения контрольных упражнений педагог оценивает, давая обучающимся информацию о правильности выполнения и при необходимости повторно объясняет материал. Собеседование с родителями после каждого занятия.

Формы отслеживания и фиксации образовательных результатов по окончании учебного года: Журнал посещаемости, аналитическая справка, аналитический материал, материал анкетирования и тестирования, портфолио, дипломы об участии в конкурсах и соревнованиях, фото, отзыв родителей.

Результативность деятельности по программе, также определяется результатами участия в конкурсах, конференциях, соревнованиях, успешном проведении открытых занятий и мастер-классов.

Анализ результатов освоения программы осуществляется следующими способами:

При **очной форме** освоения программы текущий контроль знаний осуществляется в процессе устного опроса, текущий контроль умений и навыков в процессе наблюдения за индивидуальной работой, промежуточный и итоговой контроль умений и навыков осуществляется после изучения тем в формах взаимоконтроля, самоконтроля и выполнения поставленных задач педагогом.

При реализации программы **с использованием дистанционных технологий** текущий контроль знаний, а также умений и навыков осуществляется путем анализа фото и видео информации, полученной от обучающихся, промежуточный и итоговой контроль умений и навыков осуществляется после изучения тем в формах беседы с обучающимся, по видеосвязи с или Viber.

Контроль выполнения занятий фиксируется посредством фото-видео отчетов, размещаемых детьми по итогам занятия в группе Viber. Общение с родителями и детьми ведётся в группе Viber.

Для оценки результативности дополнительной общеобразовательной общеразвивающей программы «Киберпатруль» применяются входящий, текущий, промежуточный и итоговый виды контроля.

Входная диагностика осуществляется при комплектовании группы. Цель - определить исходный уровень знаний учащихся, определить формы и методы работы с учащимися.

Формы оценки – анкетирование, собеседование.

Текущая диагностика осуществляется после изучения отдельных тем, раздела программы. В практической деятельности результативность оценивается качеством выполнения практических работ, поиску и отбору необходимого материала, умению

работать с различными источниками информации. Анализируются положительные и отрицательные стороны работы, корректируются недостатки. Контроль знаний осуществляется с помощью заданий педагога (тесты, кроссворды, викторины); взаимоконтроль, самоконтроль и др. Они активизируют, стимулируют работу учащихся, позволяют более полно проявлять полученные знания, умения, навыки.

Промежуточный контроль осуществляется на последнем этапе изучения программы. Формы оценки: тестирование, кроссворды, викторины.

Итоговый контроль осуществляется в конце учебного года. Формы оценки: прохождение тестирования и защита творческого проекта.

Оценочные материалы

Каждая изученная учащимися тема оценивается педагогом: низкий уровень освоения; средний; высокий.

Мониторинг освоения детьми программного материала

Оцениваемые показатели	Знание основных понятий в следующих разделах:	Практические умения и навыки
Высокий уровень	Обучающийся отлично знает основные понятия и свободно ими оперирует. Обучающийся знает и уверенно отвечает на вопросы по следующим разделам: - базовые понятия кибербезопасности; - правила безопасной работы в сети Интернет; - алгоритм создания надёжного пароля; - как защитить свои персональные данные; - что такое интернет зависимость и игровая зависимость; - антивирусная защита и защитить ПК от вирусов; - как защитить себя в социальных сетях; - мобильные мошенники; - сетевой этикет; - какую ответственность несут за клевету, фейк и оскорбление в интернет-ресурсах.	Обучающийся уверенно и самостоятельно применяет полученные знания: - По защите персональных данных; - Поиск информации в сети; - Создание надёжного пароля; - Защита ПК от вирусов с помощью антивирусных программ; - Правильно общается в сети Интернет; - Ответственен за собственное поведение в сети интернет; - Знает, что нужно делать, с электронными устройствами, когда на улице гроза, дождь, снег.
Средний уровень	Обучающийся хорошо знает основные понятия и оперирует ими без ощутимых затруднений. Обучающийся удовлетворительно знает и с небольшой помощью педагога отвечает на вопросы по следующим разделам: - базовые понятия кибербезопасности; правила безопасной работы в сети Интернет; - алгоритм создания надёжного пароля; - как защитить свои персональные данные;	Обучающийся применяет полученные знания: - По защите персональных данных; - Поиск информации в сети; - Создание надёжного пароля; - Защита ПК от вирусов с помощью антивирусных программ;

	<ul style="list-style-type: none"> - что такое интернет зависимость и игровая зависимость; - антивирусная защита и ащитить ПК от вирусов; - как защитить себя в социальных сетях; - мобильные мошенники; - сетевой этикет; - какую ответственность несут за клевету, фейк и оскорбление в интернет-ресурсах. 	<ul style="list-style-type: none"> - Ответственен за собственное поведение в сети интернет; - Правильно общается в сети Интернет;
Низкий уровень	<p>Обучающийся не уверенно знает основные понятия и не может ими оперировать. Обучающийся не уверенно отвечает на вопросы на вопросы по следующим разделам:</p> <ul style="list-style-type: none"> - базовые понятия кибербезопасности; правила безопасной работы в сети Интернет; - алгоритм создания надёжного пароля; - как защитит свои персональные данные; - что такое интернет зависимость и игровая зависимость; - антивирусная защита и ащитить ПК от вирусов; - как защитит себя в социальных сетях; - мобильные мошенники; - сетевой этикет; - какую ответственность несут за клевету, фейк и оскорбление в интернет-ресурсах. 	<p>Обучающийся применяет полученные знания:</p> <ul style="list-style-type: none"> - По защите персональных данных; - Поиск информации в сети; - Создание надежного пароля; - Защита ПК от вирусов с помощью антивирусных программ; - Ответственен за собственное поведение в сети интернет;

Методы и средства диагностики

Освоения учащимися проектной деятельности	-оценка результатов самостоятельности учащихся при реализации творческих, исследовательских проектов.
Развитие творческого мышления	- наблюдение за достижениями учащихся; -экспертная оценка уровня выполнения этапов проектной деятельности.
Сформированность знаний, умений и навыков	-оценка самостоятельной и коллективной работы; - мастер-классы, открытые уроки.
Развитие эмоциональной сферы учащихся	- оценка презентаций проектов; -педагогическое наблюдение за увлеченностью деятельностью и развитием мотивации на занятиях; -оценка уровня отношения к пройденному материалу; - беседы с родителями;
Развитие личностных исследовательских качеств	- защиты проектов; -наблюдения за отношениями учащихся в коллективе; -беседы с учащимися о будущем и выборе профессии; -наблюдения за личным отношением учащихся к работе в объединении; -анализ презентаций учащихся.

При оценке освоения программы дополнительного образования при очной форме обучения и очной с применением дистанционных технологий используется:

- Индивидуальная карта, которая заполняется педагогом на протяжении освоения программы (Приложение 2);
- Оценочный лист защиты проекта (Приложение 3);
- Тест и контрольные вопросы Итогового занятия (Приложение 4);

2.8. Методические материалы для очной формы обучения и очной с применением дот

Методическое обеспечение дополнительной общеобразовательной общеразвивающей программы «Киберпатруль» включает в себя обеспечение образовательного процесса согласно учебно-тематическому плану различными методическими материалами, это:

- Разработки педагога для обеспечения образовательного процесса: планы, конспекты, сценарии, сборники тестов.
- Разработки педагога для проведения занятий: презентации, видеоролики, таблицы, раздаточный материал, стенды и др.
- Материал для организации контроля усвоения учащимися учебного материала: тесты, анкеты, вопросники, контрольные упражнения, методики, творческие отчеты по программе.

Программа предусматривает использование следующих форм работы:

- *фронтальной* - подача материала всему коллективу учеников;
- *индивидуальной* - самостоятельная работа обучающихся с оказанием педагога помощи школьникам при возникновении затруднения, не уменьшая активности учеников и содействуя выработке навыков самостоятельной работы;
- *групповой* - когда обучающимся предоставляется возможность самостоятельно построить свою деятельность на основе принципа взаимозаменяемости, ощутить помощь со стороны друг друга, учесть возможности каждого на конкретном этапе деятельности. Всё это способствует более быстрому и качественному выполнению заданий. Особым приёмом при организации групповой формы работы является ориентирование детей на создание так называемых мини групп или подгрупп.

Для подготовки материала к занятиям (презентации, задания для самостоятельной работы, творческой работы, теоретический материал) используется различные «Интернет-ресурсы.

Перечень методических пособий:

1. Прохождение тестирований на платформе OnlineTestPad: <https://onlinetestpad.com/>.
2. Учебные материалы по занятиям «Российская электронная школа»: <https://resh.edu.ru/>
3. Справочник «Безопасный Интернет для детей: <https://i-deti.org/> .
4. Справочник «Изучи интернет – управляй им»: https://igra-internet.ru/game_list/.
5. Справочник «Лига безопасного интернета»: <https://ligainternet.ru/>.
6. Справочник по занятиям Инфоурок: <https://infourok.ru> .
7. Справочник «Kaspersky Safe Kids: <https://kids.kaspersky.ru/metodic>.

8. Справочник «Институт воспитания»: <https://институтвоспитания.рф/>.

9. Перечень методических материалов:

1. Видео справочник «Цифровой ликбез»: <https://digital-likbez.datalesson.ru/>.

2. Видеоматериалы: <https://resh.edu.ru/page/cyber-project>.

3. Видеоматериалы: <https://kids.kaspersky.ru/video>.

Основными формами проведения занятий являются теоретические и практические занятия. Так же используются нетрадиционные формы занятий, такие как чаепития, чествование именинников, и т.д., в ходе которых ребята учатся общаться между собой и педагогом, развивают свои коммуникативные способности, развивают дружеские отношения в группе.

Методика проведения занятия очного занятия:

Вступительная часть: познакомить учащихся с темой занятия.

Подготовительная часть: познакомить учащихся с задачами, планом занятия.

Основная часть: Ознакомление, обучение, совершенствование и т. д. в зависимости от поставленной задачи и программного материала. Проведение зарядки для тела и глаз.

Заключительная часть: Закрепление изученного материала. Просмотр работ, обсуждение.

Такая методика занятия применяется в каждом разделе

2.9. Система воспитательной работы

В учреждении МАУ ДО «Вагайский центр спорта и творчества» принята и утверждена «Рабочая программа воспитания».

Организация мероприятий с обучающимися и родителями вне учебного плана

ЦЕЛЬ: Создание условий, способствующих развитию интеллектуальных, творческих, личностных качеств учащихся, их социализации и адаптации в обществе.

Реализация данных направлений **предполагает:**

- Создание благоприятных условий и возможностей для полноценного развития личности, для охраны здоровья и жизни детей;
- Создание условий проявления и мотивации творческой активности воспитанников в различных сферах социально значимой деятельности;
- Развитие системы непрерывного образования; преемственность уровней и ступеней образования; поддержка исследовательской и проектной деятельности;
- Освоение и использование в практической деятельности новых педагогических технологий и методик воспитательной работы;
- Дальнейшее развитие и совершенствование системы дополнительного образования.

Приоритетными направлениями в воспитательной работе являются:

- **Общекультурное направление:** (гражданско-патриотическое воспитание, приобщение детей к культурному наследию, экологическое воспитание);
- **Духовно-нравственное направление:** (нравственно-эстетическое воспитание, семейное воспитание);

- **Здоровьесберегающее направление:** (физическое воспитание и формирование культуры здоровья, безопасность жизнедеятельности);

- **Общеинтеллектуальное направление:** (популяризация научных знаний, проектная деятельность);

- **Социальное направление:** (трудовое).

Приоритетные направления воспитательной работы в 2023 – 2026 учебном году

Направление воспитательной работы	Задачи работы по данному направлению
<p>Общекультурное (<i>гражданско-патриотическое воспитание, приобщение детей к культурному наследию, экологическое воспитание</i>)</p>	<p>Формирование гражданской и правовой направленности личности, активной жизненной позиции; Формирование у воспитанников таких качеств, как долг, ответственность, честь, достоинство, личность. Воспитание любви и уважения к традициям Отечества, Центра спорта и творчества, семьи. Воспитание уважения к правам, свободам и обязанностям человека.</p>
<p>Духовно-нравственное (<i>нравственно-эстетическое воспитание, семейное воспитание</i>)</p>	<p>Приобщение к базовым национальным ценностям российского общества, таким, как патриотизм, социальная солидарность, гражданственность, семья, здоровье, труд и творчество, наука, традиционные религии России, искусство, природа, человечество. Формирование духовно-нравственных качеств личности. Воспитание человека, способного к принятию ответственных решений и к проявлению нравственного поведения в любых жизненных ситуациях. Воспитание нравственной культуры, основанной на самоопределении и самосовершенствовании. Воспитание доброты, чуткости, сострадания, заботы и милосердия. Создание единой воспитывающей среды, в которой развивается личность ребенка, приобщение родителей к целенаправленному процессу воспитательной работы образовательного учреждения. Включение родителей в разнообразные сферы жизнедеятельности образовательного учреждения. Повышение психолого – педагогической культуры родителей.</p>
<p>Здоровьесберегающее направление: <i>(физическое воспитание и формирование культуры здоровья, безопасность жизнедеятельности)</i></p>	<p>Формирование и развитие знаний, установок, личностных ориентиров и норм здорового и безопасного образа жизни с целью сохранения, и укрепления физического, психологического и социального здоровья обучающихся как одной из ценностных составляющих личности обучающегося. Формирование у учащихся сознательного и ответственного отношения к личной безопасности и безопасности окружающих, усвоение ими знаний и умений распознавать и оценивать опасные ситуации, определять способы защиты от них, оказывать само- и взаимопомощь. Способствовать преодолению у воспитанников вредных привычек средствами физической культуры и занятием спортом.</p>

<p>Общеинтеллектуальное направление: <i>(популяризация научных знаний, проектная деятельность)</i></p>	<p>Активная практическая и мыслительная деятельность. Формирование потребности к изучению, создание положительной эмоциональной атмосферы обучения, способствующей оптимальному напряжению умственных и физических сил учащихся. Формирование интереса к исследовательской и проектной деятельности, научной работе. Выявление и развитие природных задатков и способностей обучающихся. Реализация познавательных интересов ребенка и его потребности в самосовершенствовании, самореализации и саморазвитии.</p>
<p>Социальное направление: <i>(воспитание трудолюбия, сознательного, творческого отношения к образованию, труду в жизни, подготовка к сознательному выбору профессии)</i></p>	<p>Формирование готовности обучающихся к выбору направления своей профессиональной деятельности в соответствии с личными интересами, индивидуальными особенностями и способностями, с учетом потребностей рынка труда. Формирование экологической культуры. Формирование общественных мотивов трудовой деятельности как наиболее ценных и значимых, устойчивых убеждений в необходимости труда на пользу обществу. Воспитание личности с активной жизненной позицией, готовой к принятию ответственности за свои решения и полученный результат, стремящейся к самосовершенствованию, саморазвитию и самовыражению.</p>
<p>Профилактика правонарушений, социально-опасных явлений</p>	<p>Совершенствование правовой культуры и правосознания обучающихся, привитие осознанного стремления к правомерному поведению. Организация работы по предупреждению и профилактике асоциального поведения обучающихся. Организация мероприятий по профилактике правонарушений, табакокурения, наркомании, токсикомании, алкоголизма.</p>

Календарный план воспитательной работы

Направление воспитательной работы	Мероприятие
СЕНТЯБРЬ	
Общекультурное	День открытых дверей
	Ведение группы объединения в социальной сети
	Создание родительских и детских чатов
Духовно-нравственное	Беседа «Правила внутреннего распорядка. Правила поведения в МАУ ДО «ВЦСТ»»
	Акция, посвященная Дню солидарности в борьбе с терроризмом
	Родительское собрание
Здоровьесберегающее	Подготовка ко Дню пожилого человека. Акция «К людям с добром!»
	<p>Месячник здоровья: БДД. Вручение Памяток водителям</p>

	«Правилам движения в Ваших руках». Просмотр видеоматериалов. Пожарная безопасность. Обзор стенда «Правила поведения при пожаре». Антитеррористическая безопасность. Профилактическая беседа «Терроризм – зло против человечества»
Общеинтеллектуальное	Видео-мастер-класс ко Дню знаний
Профилактика правонарушений, социально-опасных явлений	Оформление и поддержание в актуальном состоянии уголка правовых знаний.
ОКТЯБРЬ	
Общекультурное	Ведение группы объединения в социальной сети Онлайн марафон поздравлений «С Днем учителя»
Духовно-нравственное	Единый урок информационной безопасности. Всероссийский урок безопасности в сети Интернет. Родительское собрание «Как помочь раскрыть талант у ребенка» Воспитательный час «Мир добрыми глазами», к Международному Дню "Белая трость", дню солидарности с людьми плохо видящими и слепыми
Здоровьесберегающее	Посещение спортивного районного мероприятия
Социальное	Единый урок по теме «Мир профессий»
Профилактика правонарушений, социально-опасных явлений	Беседа «Профилактика злоупотребления алкоголя и наркотических средств» Оформление и поддержание в актуальном состоянии уголка правовых знаний.
НОЯБРЬ	
Общекультурное	Мероприятие, посвященное Дню народного единства. Ведение группы объединения в социальной сети
Духовно-нравственное	Акция «Открытка для мамы» Видео-поздравление для мам в социальных сетях
Здоровьесберегающее	Выпуск листовок о мерах личной профилактики ОРВИ и гриппа Посещение мероприятия Центра спорта и творчества «Открытие катка»
Социальное	Профоринтационная игра «Я в мире профессий»
Профилактика правонарушений, социально-опасных явлений	Профилактика безнадзорности «Я не хочу домой» Оформление и поддержание в актуальном состоянии уголка правовых знаний.
ДЕКАБРЬ	
Общекультурное	Ведение группы объединения в социальной сети Единый урок «Мы – Россияне!», посвященный Дню Конституции РФ. Посещение районного мероприятия, посвященного Дню добровольца (волонтера)
Духовно-нравственное	Инструктаж перед каникулами на темы: «БДД в зимний период», «Осторожно, гололед!», «Светоотражающие элементы и удерживающие устройства», Принять участие в благотворительной акции «Дари добро!» ко Дню инвалида. Викторина по ПДД, с целью выявления уровня знаний обучающихся. Акция, посвященная Всемирному дню борьбы со СПИДом Оформление кабинета к Новому году
Здоровьесберегающее	Познавательная игра «Мы за здоровый образ жизни»
Общеинтеллектуальное	Тематический видео-мастер-класс к Новому году

Профилактика правонарушений, социально-опасных явлений	Оформление и поддержание в актуальном состоянии уголка правовых знаний.
ЯНВАРЬ	
Общекультурное	Ведение группы объединения в социальной сети Квест – игра «Блокада Ленинграда»
Духовно-нравственное	Викторина по ПДД, с целью выявления уровня знаний обучающихся.
Здоровьесберегающее	Практикум – тренинг по теме «Дорога и мы» Районное мероприятие Всероссийская массовая лыжная гонка «Лыжня России»
Общеинтеллектуальное	Интеллектуальный марафон «Хочу все знать»
Профилактика правонарушений, социально-опасных явлений	Родительское собрание «Профилактика правонарушений, алкоголизма и наркомании. Действие новых законов в системе профилактики». Профилактическая беседа «Профилактика и предупреждение алкоголизма и наркотической зависимости» Оформление и поддержание в актуальном состоянии уголка правовых знаний.
ФЕВРАЛЬ	
Общекультурное	Беседа «Дню Защитника Отечества посвящается..» Ведение группы объединения в социальной сети Квест - игра «Сталинградская битва» Фотовыставка, посвященная Дню Защитника Отечества
Духовно-нравственное	Воспитательный час «Мы за кибербезопасность»
Здоровьесберегающее	Посещение районного мероприятия «Военизированная эстафета»
Профилактика правонарушений, социально-опасных явлений	Родительское собрание «Профилактика самовольных уходов н/летних из семьи» Оформление и поддержание в актуальном состоянии уголка правовых знаний.
МАРТ	
Общекультурное	Ведение группы объединения в социальной сети Праздник мам, бабушек «Встреча поколений». Выставка подарков «Дорогим любимым».
Духовно-нравственное	Видеопоздравление к Международному женскому дню Акция «Открытка к 8 марта» Помощь волонтерскому объединению в организации поздравления к 8 марта
Здоровьесберегающее	Посещение мероприятия «Проводы зимы»
Профилактика правонарушений, социально-опасных явлений	Просмотр видеофильмов по проблемам алкоголизма Оформление и поддержание в актуальном состоянии уголка правовых знаний.
АПРЕЛЬ	
Общекультурное	Ведение группы объединения в социальной сети Акция «Письмо солдату»
Духовно-нравственное	Акция «Весенняя неделя добра» Родительское собрание «Как родителям помочь раскрыть талант у ребенка»
Здоровьесберегающее	Экологический марафон
Общеинтеллектуальное	Районный конкурс «Горизонты открытий»

Профилактика правонарушений, социально-опасных явлений	Просмотр видеофильмов по проблемам наркомании и табакокурения
	Оформление и поддержание в актуальном состоянии уголка правовых знаний.
МАЙ	
Общекультурное	Ведение группы объединения в социальной сети
	Беседа «Мы помним!»
	Акция «Георгиевская ленточка»
	Акция «Бессмертный полк»
	Акция «Окна Победы»
Духовно-нравственное	Игровая программа «Возможности - ограничены, способности – безграничны»
	Акция «Раскрась жизнь яркими красками!»
Здоровьесберегающее	Профилактическая беседа «Летние каникулы»
	Спортивная эстафета на свежем воздухе
Общеинтеллектуальное	Выявление и поддержка одаренных и талантливых детей
	Участие в районном мероприятии «Отчетный концерт»
Социальное	Деловая игра по профессиональному самоопределению «Мой выбор»
	Анкетирование родителей об удовлетворенности образовательными услугами
Профилактика правонарушений, социально-опасных явлений	Оформление и поддержание в актуальном состоянии уголка правовых знаний.

СПИСОК ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ

Нормативные правовые акты:

1. Федеральный Закон Российской Федерации от 29.12.2012 № 273 «Об образовании в Российской Федерации»;
2. Федеральный закон Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
3. Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
4. Федеральный закон от 27.07.2006 №152 «О персональных данных»;
5. Распоряжение Правительства РФ от 28 апреля 2023 г. № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации».
6. Распоряжение Правительства Российской Федерации от 31 марта 2022 г. № 678-р «Об утверждении Концепции развития дополнительного образования детей до 2030 г. и плана мероприятий по ее реализации».
7. Распоряжение Минпросвещения России от 18.05.2020 № Р-44 «Об утверждении методических рекомендаций для внедрения в основные образовательные программы современных цифровых технологий».
8. Приказ Минпросвещения России от 02 декабря 2019 г. № 649 «Об утверждении Целевой модели цифровой образовательной среды».
9. Приказ Минпросвещения Российской Федерации от 03.09.2019 № 467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей»;
10. Приказ Минобрнауки России от 23 августа 2017 года № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;
11. Письмо Минобрнауки России от 18.11.2015 №09-3242. «Методические рекомендации по проектированию дополнительных общеразвивающих программ»;
12. СанПин 2.4.3648-20: «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи» от 28.09.2020 г.

Специальная литература:

1. Бiryukov A.A. Информационная безопасность защита и нападение 2 е издание: Издательство: ДМК-Пресс., 2017, 434 с.
2. Бiryukov A.A. Информационная безопасность защита и нападение: Издательство: ДМК-Пресс., 2018, 474 с.
3. Колесниченко Денис. Анонимность и безопасность в интернете. От чайника к пользователю. Самоучитель Издательство: БХВ-Петербург, 2018, 240с.
4. Мазаник Сергей. Безопасность компьютера. Защита от сбоев, вирусов и неисправностей: издательство: ЭКСМО, 2019, 256 с.
5. Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасность сетей: Издательство: М.: НОУ "Интуит", 2020,571 с.

6. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студ. Учрежд.высш.проф. образования / В. В.Платонов. — М.: Издательский центр «Академия», 2018, 336 с.
7. Проскурин В.Г Защита в операционных системах: Издательство: Горячая линия-Телеком, 2019, 192 с.
8. Савченко Е. Кто, как и зачем следит за вами через интернет: Москва - Третий Рим, 2019, 100 с.
9. Яковлев В.А.Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2018, 320 с.
10. Основы кибербезопасности: учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М.: Дрофа, 2019. — 238, [1] с. — (Российский учебник).
11. Баранова Е.К., Бабаш А.В. Основы информационной безопасности: учебник / Е.К. Баранова, А.В. Бабаш. — М.: РИОР: ИНФРА-М, 2019. — 202 с. — (Среднее про - фессиональное образование)
12. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы: учеб.пособие для общеобразоват. организаций / М.С. Наместникова. – М.: Просвещение, 2019. – 79 с.: ил. – (Внеурочная деятельность).
13. Цветкова, М.С. Информационная безопасность. Кибербезопасность. 7–9 классы: учебное пособие /М.С. Цветкова, И.Ю. Хлобыстова. — 2-е изд., пересмотр. — М.: БИНОМ. Лаборатория знаний, 2020 — 64 с.: ил.
14. Шаньгин В.Ф. Информационная безопасность и защита информации. / Шаньгин В.Ф. – ДМК-Пресс, 2017 – 702 с.
15. Справочник «Безопасный Интернет для детей: <https://i-deti.org/> .
16. Справочник «Изучи интернет – управляй им»: https://igra-internet.ru/game_list/.
17. Справочник «Лига безопасного интернета»: <https://ligainternet.ru/>.
18. Справочник по занятиям Инфоурок: <https://infourok.ru> .
19. Справочник «Kaspersky Safe Kids: <https://kids.kaspersky.ru/metodic>.
20. Справочник «Институт воспитания»: <https://институтвоспитания.рф/>.
21. Информационный справочник «Персональные данные»: <https://rkn.gov.ru/personal-data/>.

Список литературы для учащихся и их родителей:

- 1.Справочник «Безопасный Интернет для детей: <https://i-deti.org/> .
- 2.Справочник «Изучи интернет – управляй им»: https://igra-internet.ru/game_list/.
- 3.Справочник «Лига безопасного интернета»: <https://ligainternet.ru/>.
- 4.Справочник «Kaspersky Safe Kids: <https://kids.kaspersky.ru/metodic>.
- 5.Справочник «Институт воспитания»: <https://институтвоспитания.рф/>.
- 6.Справочник «Персональные данные Дети»: <http://персональныеданные.дети/>
7. Информационный справочник «Персональные данные»: <https://rkn.gov.ru/personal-data/>.

**ИНСТРУКЦИЯ
ПРИ ПРОВЕДЕНИИ ЗАНЯТИЙ В КОМПЬЮТЕРНОМ КЛАССЕ**

1. Общие требования безопасности

1.1. К работе в компьютерном классе допускаются учащиеся с 1-го класса, прошедшие инструктаж по охране труда, медицинский осмотр, не имеющие противопоказаний по состоянию здоровья и ознакомленные с данной инструкцией.

1.2. Работа учащихся в компьютерном классе разрешается только в присутствии преподавателя (инженера, лаборанта).

1.3. Во время занятий посторонние лица могут находиться в классе только с разрешения преподавателя.

1.4. Во время перемен между уроками проводится обязательное проветривание компьютерного кабинета с обязательным выходом учащихся из класса.

1.5. При работе в компьютерном кабинете возможно воздействие на учащихся следующих опасных и вредных производственных факторов:

- неблагоприятное воздействие на организм человека неонизирующих электромагнитных излучений мониторов;
- неблагоприятное воздействие на зрение визуальных эргономических параметров мониторов, выходящих за пределы оптимального диапазона;
- поражение электрическим током.

1.6. Помните, что каждый учащийся в ответе за состояние своего рабочего места и сохранность размещенного на нем оборудования.

1.7. Компьютерный класс комплектуется медицинской аптечкой с набором необходимых медикаментов и перевязочных средств для оказания первой помощи при травмах или при плохом самочувствии.

1.8. При работе в компьютерном классе необходимо соблюдать правила пожарной безопасности, знать места расположения первичных средств пожаротушения.

1.9. Соблюдение требований настоящей инструкции обязательно для учащихся, работающих в компьютерном классе.

1.10. Пребывание учащихся в помещении кабинета допускается только в присутствии преподавателя.

1.11. Категорически запрещается находиться в компьютерном классе в верхней одежде.

1.12. В компьютерном кабинете запрещено использование мобильных средств связи.

1.13. В процессе работы с видеотерминалами учащиеся должны соблюдать порядок проведения работ, правила личной гигиены, содержать в чистоте рабочее место.

1.14. Учащимся запрещается приносить на занятия острые, режущие, колющие и другие опасные для жизни и безопасности предметы, химические вещества.

1.15. Учащимся запрещается бегать по кабинету или играть в кабинете в подвижные игры, без разрешения педагога подходить к имеющемуся в кабинете оборудованию и пользоваться им, самостоятельно включать компьютеры или запускать компьютерные программы, трогать разъемы соединительных кабелей.

1.16. Учащиеся, допустившие невыполнение или нарушение инструкции по охране труда, привлекаются к ответственности и со всеми учащимися проводится внеплановый инструктаж по охране труда.

2. Требования безопасности перед началом работы. Перед началом работы необходимо:

2.1. Убедиться в отсутствии видимых повреждений на рабочем месте;

2.2. Разместить на столе тетради, учебные пособия так, чтобы они не мешали работе на компьютере.

2.3. Принять правильную рабочую позу.

2.4. Посмотреть на индикатор монитора и системного блока и определить, включён или выключен компьютер. Переместите мышь, если компьютер находится в энергосберегающем состоянии или включить монитор, если он был выключен.

3. Требования безопасности во время работы

3.1. При работе в компьютерном классе учащимся категорически запрещается:

- Находиться в классе в верхней одежде;
- Класть одежду и сумки на столы;
- Бегать, толкать друг друга, громко разговаривать, отвлекать товарищей;
- Находиться в классе с напитками и едой;
- Располагаться сбоку или сзади от включенного монитора;
- Присоединять или отсоединять кабели, трогать разъемы, провода и розетки;
- Передвигать компьютеры и мониторы;
- Открывать системный блок;
- Включать и выключать компьютеры самостоятельно.
- Пытаться самостоятельно устранять неисправности в работе аппаратуры;
- Перекрывать вентиляционные отверстия на системном блоке и мониторе;
- Ударять по клавиатуре, нажимать бесцельно на клавиши;
- Класть книги, тетради и другие вещи на клавиатуру, монитор и системный блок;
- Удалять и перемещать чужие файлы;
- Прикасаться к питающим проводам и устройствам заземления;
- Прикасаться к экрану и тыльной стороне экрана и клавиатуры;
- Работать во влажной одежде и влажными руками;
- Использовать сменные носители информации без предварительной проверки антивирусной программой.
- Приносить и запускать компьютерные игры.

3.2. Находясь в компьютерном классе, учащиеся обязаны:

- Соблюдать тишину и порядок;
- Выполнять требования преподавателя и лаборанта;
- Находясь в сети работать только под своим именем и паролем;
- Соблюдать режим работы (согласно п. 9.4.2. Санитарных правил и норм);

3.3. При появлении рези в глазах, резком ухудшении видимости, невозможности сфокусировать взгляд или навести его на резкость, появления боли в пальцах и кистях рук, усиления сердцебиения немедленно покинуть рабочее место, сообщить о происшедшем преподавателю и обратиться к врачу.

3.3. Работая за компьютером, необходимо соблюдать правила:

- Расстояние от экрана до глаз – 60 – 80 см (расстояние вытянутой руки);
- Вертикально прямая спина;
- Плечи опущены и расслаблены;
- Ноги на полу и не скрещены;
- Локти, запястья и кисти рук на одном уровне;
- Локтевые, тазобедренные, коленные, голеностопные суставы под прямым углом;
- Приветствовать входящих в класс во время урока сидя.

3.4. Длительность работы за компьютером не должно превышать: для учащихся 1-х классов (6 лет) - 10 мин., для учащихся 2-5 классов -15 мин., для учащихся 6-7 классов - 20 мин., для учащихся 8-9 классов - 25 мин., для учащихся 10-11 классов - при двух уроках подряд на первом из них - 30 мин., на втором - 20 мин., после чего сделать перерыв не менее 10 мин. для выполнения специальных упражнений, снимающих зрительное утомление.

4. Требования безопасности в аварийных ситуациях.

4.1. При появлении программных ошибок или сбоях оборудования учащийся должен немедленно обратиться к педагогу.

4.2. При появлении запаха гари, необычного звука немедленно прекратить работу, и сообщить педагогу.

4.3. В случае появления неисправности в работе видеотерминала немедленно следует выключить его и сообщить об этом педагогу (преподавателю).

4.4. При плохом самочувствии, появлении головной боли, головокружении и пр. прекратить работу и сообщить об этом педагогу (преподавателю).

4.5. При возникновении аварийной ситуации необходимо сохранять спокойствие, четко выполнять указания преподавателя и при необходимости эвакуироваться из помещения.

5. Требования безопасности по окончании работы

5.1. После окончания работы завершить все активные программы и корректно выключить компьютер.

5.2. Оставить рабочее место чистым.

5.3. Выходить из кабинета только по указанию педагога.

5.4. Обо всех недостатках, обнаруженных во время работы в компьютерном классе, сообщить преподавателю.

ПРИЛОЖЕНИЕ 2

ИНДИВИДУАЛЬНАЯ КАРТА ОСВОЕНИЯ ПРОГРАММЫ

ФИО учащегося _____ Дата рождения _____
 Объединение _____

Учёт результатов обученности по дополнительной общеобразовательной общеразвивающей программе
 «Киберпатруль»

Показатели		Сроки диагностики	
		1-е полугодие	2-е полугодие
Теоретическая подготовка	соответствие теоретических знаний программным требованиям		
	осмысленность и правильность использования специальной терминологии		
	знание техники безопасности на занятиях		
Практическая подготовка	соответствие практических умений и навыков программным требованиям		
	креативность в выполнении творческих заданий		
	творческие навыки		
	информационная компетентность		
Сформированность базовых компетентностей	коммуникативная компетентность		
	самоорганизация компетентность		
	самообразование компетентность		
	мотивация учебно-познавательной деятельности		
Личностное развитие	сформированность интеллектуальных умений		
	степень обучаемости		
	навыки учебного труда		
	результативность индивидуальных занятий		
	уровень утомляемости		
	целеустремлённость		
	дисциплина и организованность		
	коммуникабельность, степень влияния в коллективе		
	исполнение обязанностей в объединении		

ПРИЛОЖЕНИЕ 3

ОЦЕНОЧНЫЙ ЛИСТ ПО ЗАЩИТЕ ПРОЕКТОВ

«Киберпатруль»

ФИО учащегося _____
 Объединение _____ Группа _____ Год обучения _____

Критерии оценки защиты проекта

Показатели	Степень соответствия		
	Соответствует	В целом соответствует	Не соответствует
	2 балла	1 балл	0 баллов
Умение выделить цель и задачи исследования (работы)			
Умение обосновать актуальность исследования (работы), выделить проблему			
Умение представить содержание работы в соответствии с темой и поставленной целью			
Умение сделать вывод, владение понятийным аппаратом			
Умение следовать алгоритму выступления			
Умение устанавливать контакт с аудиторией			
Умение привлекать иллюстративный материал (фото, видео, аудио материалы, презентации) для облегчения восприятия слушателями логики изложения			
Умение соответствовать регламенту, изложить суть работы в отведенное время			
Умение давать аргументированные ответы на вопросы слушателей			

Сумма баллов по оценке защиты проекта: _____
 (максимальное=18 баллов)

Педагог дополнительного образования: _____

Подпись комиссии:

_____/ _____
 _____/ _____
 _____/ _____

ПРИМЕРЫ РАБОЧЕГО ЛИСТА УЧЕНИКА

Рабочий лист

«КИБЕРБЕЗОПАСНОСТЬ»

Разговоры о важном **Кибербезопасность**

✓ **Рассмотри различные устройства. Обведи те из них, которые можно назвать цифровыми.**

<https://vk.com/public215220961>

Учитель информатики

✓ **В интернет пространстве очень важно защищать свою личную информацию. Какой фильтр нужно выбрать, чтобы дополнительно обезопасить свои публикации от мошенников?**

Видно всем

Видно друзьям

Видно близким друзьям

ЗАЩИТИ ИНФОРМАЦИЮ О СЕБЕ

Не делитесь в социальных сетях личными данными и своими фотографиями

✓ **В интернете мы можем столкнуться с мошенниками. Чтобы выманить наши деньги мошенники оправляют вам ссылки, которые называются «фишинговые ссылки». Что нужно проверить, чтобы не стать жертвой мошенников? Выбери правильные варианты.**

A) посмотри страничку «нового знакомого» - похожа ли она на настоящую;

B) сразу перейти по ссылке;

B) вводи данные карты не проверив адрес сайта;

Г) не вводи данные пока не убедись, что сайт официальный.

✓ **Чтобы защитить свой профиль в социальных сетях от взлома, необходимо использовать разные пароли на всех сервисах. Какой пароль будет более безопасен? Пройди лабиринт, чтобы это выяснить.**

Пароль _____

Как часто нужно менять пароль для безопасности твоего профиля?

✓ **Как распознать обман в интернете?**

Если вам пришло сообщение от незнакомца, то необходимо постараться собрать о нём дополнительную информацию:

1) _____

2) _____

3) _____

Помните! Мошенники всегда будут вас торопить, чтобы у вас не было возможности и времени разобраться в ситуации, чтобы уточнить и проверить полученную информацию.

ЗАЩИТИ ИНФОРМАЦИЮ О СЕБЕ

Не меняй свои персональные данные на сомнительную выгоду

Учитель информатики

КИБЕРБЕЗОПАСНОСТЬ

Рабочий лист

Для каких повседневных задач можно использовать интернет?
Восстанови ответ:

1) У...ЕН...Е 2) О...Щ...Н...Е 3) Т...О...Ч...С...ВО
4) ПРОФЕССИОНАЛЬНАЯ Д...Я...ЕЛЬ...ОСТ...

Соотнеси слово со значением стрелкой

СПТАМ	Травля человека в интернете
СКАМ	Рассылка информации без согласия получателя
ФИШИНГ	Мошенничество с целью выманивания денег
КИБЕРБУЛЛИНГ	Мошенничество с целью доступа к личной информации

Здесь найдёшь полезную информацию по теме безопасности в интернете

СОСТАВЬ СПИСОК ПРАВИЛ БЕЗОПАСНОГО ИНТЕРНЕТА

- _____
- _____
- _____
- _____

воспитательная работа школы <https://vk.com/public215220961>

ИТОГОВЫЙ ТЕСТ

Вопрос №1 Какую информацию нельзя разглашать в Интернете?

- а) свои увлечения
- б) свой псевдоним
- в) домашний адрес +

Вопрос №2 Какие данные из нижеперечисленных можно сообщать по электронной почте?

- а) номера банковских карт твоих родителей
- б) секретные слова (ответы) на специальные секретные вопросы, используемые при идентификации вашего аккаунта
- в) свои имя и фамилию +

Вопрос №3 Что такое СПАМ:

- а) агрессивное поведение на форумах
- б) массовая рассылка рекламы и прочих объявлений +
- в) цепочка непонятных, нелогичных объяснений

Вопрос №4 Что НЕ поможет защитить твою электронную почту от взлома?

- а) создавать разные надежные пароли от своих аккаунтов
- б) не открывать сообщения с незнакомых и подозрительных адресов
- в) сказать свой пароль родителям +

Вопрос №5 В сети вы встретились с дразнилками и оскорблениями, вы:

- а) ответите грубостью
- б) заблокируете этого человека и сообщите родителям +
- в) никому об этом не говорите

Вопрос №6 Когда можно доверять письму от неизвестного отправителя?

- а) отправитель ссылается на твоих друзей
- б) к тебе обращаются по имени
- в) никогда нельзя доверять письму от неизвестного отправителя +

Вопрос №7 Какой из предложенных паролей лучше выбрать для своей электронной почты?

- а) дата рождения
- б) s_7_NR32a +
- в) 123456

Вопрос №8 Тебе на электронную почту пришло письмо от незнакомого человека, представившегося знакомым твоей мамы, в котором он просит пройти по ссылке и проголосовать за его проект. Что ты сделаешь?

- а) пройду по ссылке и посмотрю, что за проект
- б) напишу в ответ письмо и спрошу, откуда он знает мою маму
- в) удалю письмо. Я ничего не знаю об этом сайте и авторе письма. Скорее всего, это спам. +

Вопрос №9 Как можно хранить пароль?

- а) написать на листочке и приклеить на монитор
- б) только в памяти (в своей голове) +
- в) сохранить в браузере

Вопрос №10 Какое правило безопасного поведения в сети Интернет позволит уберечь себя от вирусов?

- а) не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета +
- б) не добавляй незнакомых людей в свои контакты
- в) общаясь в Интернете, будь дружелюбен. Не пиши грубых слов!

Вопрос №11 Как гарантировать 100% защищенность компьютера от заражения вирусами в сети?

- а) установить новое программное обеспечение
- б) таких гарантий нет +
- в) посещать только известные сайты

Вопрос №12 Вам пришло письмо: «Чтобы выиграть миллион в нашей лотерее, вам нужно зарегистрироваться на этом сайте (ссылка на сайт). Регистрация закрывается завтра. Не пропустите!». Что вы сделаете?

- а) зайду на сайт и посмотрю, что за лотерея
- б) напишу в ответ письмо, где попрошу прислать подробности о лотерее
- в) удалю письмо. Я ничего не знаю об этом сайте и авторе письма. Скорее всего, это спам +

Вопрос №13 Что такое Компьютерный вирус?

- а) безобидный червячок
- б) компьютерная программа, нарушающая работу других программ +
- в) компьютерный герой-шпион

Вопрос №14 При установке приложения обработки фотографий на смартфон приложении просит доступ к СМС-сообщениям и телефонной книге. Согласиться или нет?

- а) согласиться, поскольку это безопасно
- б) не согласиться, поскольку это небезопасно +

Вопрос №15 Что не является персональными данными?

- а) фамилия, имя, отчество +
- б) история болезни
- в) дата и место рождения

Тест №2

Вопрос №1 Ваш друг в социальной сети написал следующее сообщение: "у меня горе помоги, реквизиты на стене". Что Вы будете делать?

- а) отправлю деньги другу
- б) уточню, что случилось и нужна ли помощь не через социальную сеть. +
- в) не буду отправлять деньги другу

Вопрос №2 Интернет – это...

- а) всемирная компьютерная сеть, соединяющая вместе тысячи сетей. +
- б) персональный компьютер
- в) браузер

Вопрос №3 Как называется детский Браузер?

- а) Internet Explorer
- б) Гогуль +
- в) Mozilla Firefox

Вопрос №4 Сетевой этикет – это...

- а) правила поведения за столом
- б) правила поведения в обществе
- в) нравственные правила поведения в компьютерных сетях. +

Вопрос №5 Что делать, если вы стали жертвой интернет-травли?

- а) Выкинуть компьютер
- б) Ничего не делать, терпеть
- в) Обратиться в администрацию ресурса с просьбой наказать обидчика +

Вопрос №6 Что такое Антивирусная программа?

- а) комплекс мероприятий, направленных на обеспечение информационной безопасности
- б) любая программа для обнаружения компьютерных вирусов, а также нежелательных программ и восстановления зараженных такими программами файлов +
- в) мошенники в сети Интернет

Вопрос №7 Нужно ли в интернете всем сообщать свою фамилию, имя, адрес, номер школы?

- а) всем виртуальным друзьям нужно рассказать о себе
- б) никогда не сообщать личную информацию +
- в) сообщать только вымышленную информацию

Вопрос №8 Что такое НИК?

- а) вымышленное виртуальное имя +
- б) компьютерная программа
- в) компьютерный герой

Вопрос №9 Виртуальный друг предлагает встретиться, ваши действия?

- а) встретиться с виртуальным другом в торговом центре
- б) сообщить родителям об этом +
- в) встретиться с виртуальным другом в заброшенном, таинственном месте

Вопрос №10 На вашу электронную почту пришло письмо от неизвестного адресата, вы:

- а) сохраните в черновики и откроете позднее
- б) откроете немедленно
- в) некогда не открываете писем от неизвестных адресатов +

Вопрос №11 Сколько времени детям, по мнению специалистов, можно проводить за компьютером?

- а) пока не выиграешь в любимую игрушку
- б) пока не подготовишься к урокам
- в) не более часа в день +

Вопрос №12 Укажи устройство для подключения компьютера к сети:

- а) модем +
- б) монитор
- в) сканер

Вопрос №13 Можно ли отправлять SMS или оставлять свой номер телефона с незнакомого сайта, чтобы получить код доступа к игре или подарку?

- а) никогда не следует отправлять SMS или давать свой номер телефона +
- б) всегда оставлять номер телефона, а SMS слать нельзя
- в) всегда отправлять сообщение и давать номер, чтобы получить код доступа

Вопрос №14 Что такое информация?

- а) – это компьютерная программа, для чтения книг
- б) – это, прежде всего, предоставление каких-либо знаний или фактов о чем-либо +
- в) – это общение в интернете

Вопрос №15 Социальная сеть – это...

- а) место, где можно общаться с друзьями и знакомыми, слушать музыку и смотреть фильмы +
- б) поисковая система
- в) интернет-сервис для поиска материалов для реферата

ПРИМЕР КВЕСТА «ПОКУПКА В «ИНТЕРНЕТ-МАГАЗИНЕ»

Задание №1

Напишите правила потребительской безопасности.

Задание №2. Ситуации.

Ситуация 1. В одном из интернет-магазинов вы увидели, что смартфон, о котором вы давно мечтали, и у вас есть для этого некоторая сумма денег, продается очень дешево. Каковы ваши действия?

Ответ. Правила безопасного поведения в интернет магазинах: Покупая в интернет-магазинах, сохраняйте здоровый скептицизм. Помните: цена не может быть слишком низкой, тем более, если вы рассчитываете приобрести оригинальную продукцию бренда.

Изучите историю магазина в сети, проверьте наличие контактов, выясните, можно ли туда приехать и познакомиться вживую. Читая отзывы, обратите внимание, чтобы они были разными. Заказные отзывы пишут люди, которым приходится делать это много раз в день, поэтому такие тексты будто написаны по шаблону.

Посмотрите, как на отзывы реагируют продавцы. Обратите особое внимание на негативные: если их отработывают, это хороший знак (причем ситуация должна быть конкретная, содержать номер заказа и т.п.).

Ситуация 2. На ваш телефон пришло сообщение от знакомого о срочном переводе ему денег, позже он объяснит зачем ему это надо. Какие будут ваши действия?

Ответ. Правила безопасных платежей:

Если вам в мессенджер пришла просьба от знакомого с просьбой срочно выслать денег, ничего не отправляйте! Сначала перезвоните ему и удостоверьтесь, что аккаунт не был взломан злоумышленниками.

Чтобы никогда не терять деньги на незаметных платежах, не покупать дополнительных услуг по ошибке и точно заплатить за нужные, всегда читайте правила перед тем, как поставить галочку напротив чекбокса «согласен» и перейти к оплате.

Платите безопасно! Классический случай — вас переадресуют на защищенную страницу (адрес начинается с «https://»). Если нет, лучше не рисковать. По правилам эквайринга (*Эквэйринг (от англ. acquire «приобретать, получать») — возможность для торгового предприятия принимать безналичную оплату за товары и услуги пластиковыми картами*) на сайте продавца должна быть информация о том, кто принимает платеж. Прочтите ее и сверьте с тем, что написано на следующей странице.

Заведите отдельную (можно виртуальную) карту для платежей в интернете.

Если для оплаты в интернете вы пользуетесь своей обычной картой, не храните на ней крупные суммы денег.

Подключите в своем банке СМС-информирование о всех операциях по картам и счетам. Так вы сможете быстро заметить, если ваша карта будет скомпрометирована, и заблокировать ее.

Если на смартфоне появилась надпись «Вставьте сим-карту», срочно зайдите в ближайший офис вашего мобильного оператора или позвоните ему с другого телефона и выясните, в чем

проблема. Возможно, кто-то получил дубликат вашей симки и ее нужно срочно заблокировать.

Потеряли телефон, к которому привязана банковская карта? Срочно блокируйте и симку, и карту.

Ситуация 3. На одном из сайтов вам предложили бесплатно поиграть в компьютерную игру, так как игра проходит в тестовом режиме. Что необходимо помнить в такой ситуации?

Ответ. Правила безопасного пользования интернет сервисами и ресурсами:

Для некоторых приложений и сервисов предусмотрен бесплатный тестовый период (например, на 2-3 месяца), после чего вы должны самостоятельно отключить услугу. Если вы этого не сделаете, подписка может быть автоматически продлена и станет платной, а с указанной при регистрации карты начнут списывать деньги.

Мошенники создают сайты, на которых вы якобы можете бесплатно посмотреть, поиграть или скачать приглянувшийся вам фильм, но сначала надо оставить телефон или отправить сообщение на короткий номер. Так с вашего счета могут списать внушительную сумму за СМС, а сам телефон попадет в базу спамеров.

Помните, что бесплатный сыр бывает только в мышеловке. Осторожно, под видом игры ваш компьютер могут заразить вирусами.

Задание №3

Соедините термины и определения..Распечатать на листочках и разрезать, чтобы школьники соединяли карточки.

Термины:

Банковская карта

Виртуальная банковская карта

Фишинг

Мошенничество (финансовое)

Электронный кошелек

Кредитная карта

HTTPS

Определения

- пластиковая карта, которая привязана к одному или нескольким расчётным счетам в банке. Ей можно оплачивать товары и услуги, в том числе онлайн, и снимать наличные деньги в банкоматах и операционных кассах. По сути, это физический символ вашего банковского счёта, который можно потрогать и предъявить.

- специальная карта для покупок и платежей онлайн. Часто она даже не имеет материального носителя: банк сообщает вам только номер, срок действия и код проверки подлинности карты (CVC2/CVV2). Бывает в пластике, но оплачивать покупки офлайн и снимать наличные с её помощью нельзя.

- вид интернет-мошенничества, цель которого – завладеть логинами, паролями и другой конфиденциальной информацией, чтобы получить доступ к деньгам и аккаунтам пользователя.

- совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.
- специальная программа или интернет-сервис, с помощью которых можно хранить электронные деньги и платить ими. По сути, это аналог банковского счёта. Самые известные: «Яндекс.Деньги» и кошелёк платёжной системы QIWI.
- средства, которые автоматически берёте у банка в кредит и обязаны вернуть с процентами.
- расширение протокола НТТР, которое используется для шифрования и безопасного обмена данными между пользователем и сайтом.

Задание №4.

Впишите в пробел значение.

1. Потеряли телефон, к которому привязана банковская карта? Срочно блокируйте и симку, и карту. Её всегда можно разблокировать позже, а деньги будут целее. _____ (Блокировать карты и симки);
2. Чем дольше существует магазин и чем больше о нём положительных отзывов, тем лучше. _____ (Покупать только на сайтах с отличной репутацией)
3. Адрес сайта должен начинаться с «https://», рядом с которым нарисован закрытый замок зелёного цвета. Это значит, что данные передаются в зашифрованном виде и надёжно защищены. _____ (Вводить конфиденциальные данные только на защищённых страницах)
4. . Большинство банков поддерживают технологию верификации 3D-Secure. При совершении операции вам приходит сообщение с кодом подтверждения транзакции, который нужно ввести в специальном окошке на платёжной странице. Поэтому важно сообщать в банк, если у вас украли телефон или вы сменили номер. _____ (Подключить СМС-оповещения.)
5. Выдаётся специально для покупок и платежей онлайн. Часто она даже не имеет материального носителя: банк сообщает вам только номер, срок действия и код проверки подлинности карты (CVC2/CVV2). Бывает в пластике, но оплачивать покупки офлайн и снимать наличные с её помощью нельзя. _____ (Виртуальная банковская карта).
6. Не сообщайте ни банковским служащим, ни работникам интернет-магазинов. Первые и так знают всю необходимую информацию, вторым она совершенно не нужна для проведения платежа. _____ (Данные своей банковской карты).
7. Нельзя расглашать. _____ (Свои персональные данные).

ПРИМЕР ДОСКИ УСПЕВАЕМОСТИ

Дата	Тема занятия	Успеваемость					
		Иванов И.И	Петров П.П.	ФИО ученика	ФИО ученика	ФИО ученика
01.09.22	Вводное занятие. Введение в программу. История развития компьютерных технологий						
06.09.22	Знакомство с программой ДООП						
08.09.22							
...							
...							
...							
...							
...							

Примечание:



- Низкий уровень – изначально прибегает к помощи педагога, затрудняется при ответе на вопросы



- Средний уровень – частично прибегает к помощи педагога и обучающихся, отвечает на вопросы педагога



- Высокий уровень – самостоятельно конструирует и программирует, отвечает на вопросы педагога без трудностей



- Повышенный уровень – выполнено дополнительное задание